Harta, Lukas et al.

Research Report

Regulatory and financial burdens of EU legislation in four Member States – a comparative study. Vol. 4: Burdens arising from Art. 30 and 33 of the General Data Protection Regulation

Provided in Cooperation with:
Foundation for Family Businesses / Stiftung Familienunternehmen

Suggested Citation: Harta, Lukas et al. (2023) : Regulatory and financial burdens of EU legislation in four Member States – a comparative study. Vol. 4: Burdens arising from Art. 30 and 33 of the General Data Protection Regulation, ISBN 978-3-948850-35-7, Foundation for Family Businesses, Munich

This Version is available at:
https://hdl.handle.net/10419/273338

Foundation for
Family Businesses

Regulatory and financial burdens of EU legislation in four Member States – a comparative study

Vol. 4: Burdens arising from Art. 30 and 33 of the General Data Protection Regulation

Publication details

Published by:

Foundation for Family Businesses

Stiftung Familienunternehmen
Prinzregentenstraße 50
80538 Munich
Germany
Phone: +49 (0) 89 / 12 76 400 02
Fax: +49 (0) 89 / 12 76 400 09
E-mail: info@familienunternehmen.de
www.familienunternehmen.de/en

Part A prepared by:

cep
Centres for European Policy Network
FREIBURG | BERLIN | PARIS | ROMA

cep
Kaiser-Joseph-Straße 266
79098 Freiburg im Breisgau
Germany

Dr. Lukas Harta, LL.M.
Dr. Anja Hoffmann
Dr. Matthias Kullas
Prof. Dr. Andrea de Petris

alerion
AVOCATS

Alerion
137 rue de l'Université
75007 Paris
France

Carole Bui
Caroline Leroy-Blanvillain
Corinne Thierache

Part B prepared by:

prognos
Wir geben Orientierung.

Prognos AG
Goethestraße 85
10623 Berlin
Germany

Jan Tiessen
Michael Schaaf
Jan-Felix Czichon

Csil

CSIL
Corso Monforte 15
20122 Milan
Italy

Jessica Catalano
Sara Banfi
Anthony Bovagnet

Cover image: SrdjanPav | iStock

ISBN: 978-3-948850-35-7

Quotation (full acknowledgement):

Stiftung Familienunternehmen (eds.): Regulatory and financial burdens of EU legislation in four Member States – a comparative study, Vol. 4: Regulatory and financial burdens arising from Art. 30 and 33 of the General Data Protection Regulation, prepared by cep, Alerion, Prognos AG and CSIL, Munich 2023, www.familienunternehmen.de/en

Contents

Comparing legislation as well as regulatory and financial burdens in four EU Member States

This study is part of a larger project investigating whether and how European legislation is implemented in selected EU Member States on legislative and administrative levels and what (different) bureaucratic burdens are associated with their fulfilment in comparable family businesses. The project was started in autumn 2020; it covers Austria, France, Germany and Italy and deals with a selected number of European directives and regulations. This part of the project covers the General Data Protection Regulation (GDPR) and focusses on the burdens arising from Art. 30 and 33.

The study contributes to an evidence-based discussion on the reduction of regulatory burdens at European and national levels by comparing the transposition and implementation of European data protection legislation. It focusses on the legal and administrative burdens for private businesses regarding the preparation and maintenance of a record of processing activities according to Art. 30 GDPR and the requirements related to the notification of personal data breaches to the competent supervisory authority according to Art. 33 GDPR. The two articles impose structurally very different requirements: While Art. 30 GDPR causes continuous administrative efforts, Art. 33 GDPR requires short-term measures. The parallel analysis of both requirements provides a meaningful impression of the bureaucratic burdens caused by the GDPR. Part A – the comparison of the legislation – was essentially completed in January 2023, Part B – on the economic assessment of the regulatory burden – was finalised in May 2023.

The study was made possible by numerous family businesses, chambers, consultancies and other experts that agreed to share their experiences concerning the record of processing activities and the notification of personal data breaches with the scientists. We are grateful for their commitment and the time they invested in the interviews. Thank you!

Moreover, we would like to thank the Regulatory Control Council Baden-Württemberg (Normenkontrollrat Baden-Württemberg), who had co-initiated and actively supported the study from 2019 to 2022.

Study: "Regulatory and financial burdens of EU legislation in four Member States – a comparative study, Vol. 1: Regulatory and financial burdens arising from the A1 Certificate"

Study: "Regulatory and financial burdens of EU legislation in four Member States – a comparative study, Vol. 2: Burdens arising from the Posting of Workers Directive"

Study: "Regulatory and financial burdens of EU legislation in four Member States – a comparative study, Vol. 3: Burdens arising from the transparency register of the Anti-Money Laundering Directive"

Summary of main results

Key findings of the legal study (cep and Alerion)

1. Part A of this study compares the regulatory burden related to the compliance with two provisions of the EU General Data Protection Regulation (GDPR) in Austria, France, Germany and Italy. The study focusses on the legal and administrative requirements with regard to
   - the preparation and maintenance of a record of processing activities according to Art. 30 GDPR and
   - the requirements related to the notification of personal data breaches to the competent supervisory authority according to Art. 33 GDPR.
2. Art. 30 GDPR requires controllers and processors of personal data to maintain a record of processing activities (RPA) containing a range of information on the data processed by the company, including
   - the name and contact details of the controller,
   - the purposes of the processing,
   - a description of the categories of data processed and of the categories of affected data subjects,
   - the categories of recipients to whom such data are being disclosed,
   - an indication of whether the data are transferred to a third country and,
   - where possible, the timelines for the deletion of the data as well as a general description of the technical and organisational security measures applied to the data by the company.
3. Since the information listed above must be provided for each "processing activity", the volume of the RPA depends on the understanding of the notion of a "processing activity". However, the term is not defined in the GDPR. While the Austrian and the Italian data protection authorities (DPAs) do not provide any relevant help here, it becomes clear from the guidance given by the French and the German[1] DPAs that not every single processing operation must be included in the RPA, but a certain abstraction can be made. However, the appropriate level of abstraction is not entirely clear.

No definition of "processing activity" in Art. 30 GDPR

4. Overall, the levels of guidance and help given on the websites of the national DPAs on how to draft an RPA differ significantly between the four Member States researched. While

1 Germany has a federal system of data protection supervision. It consists of the DPAs of the Federation (the "Bund") and the 16 federal states (the "Länder"). As far as the data protection supervisory authorities of the federal states are the competent authority, this study is based on the templates and guidance provided by the Landesbeauftragter für Datenschutz und Informationsfreiheit (LfDI) Baden-Württemberg.

the Austrian DPA does not provide a template and gives only very little information on the duties in relation to the drafting of an RPA, the other authorities provide significantly more guidance and help.

5. As the GDPR lists the information to be included in the RPA without detailing it, the official templates provided by the national DPAs differ to a certain extent. For example, other than in Austria (where there is no official template at all) and in Italy, the German and French templates clearly list which exact contact details must be indicated. Although a more comprehensive template seems to create a greater burden, it makes it clearer for the controller what level of granularity of information is required.
6. Some of the Member States researched request additional information to be included in the RPA, which can be regarded as gold plating; however, the extent of gold plating is marginal.
7. The bureaucratic burden with regard to the drafting of an RPA also depends on the availability and user-friendliness of the official templates provided by the competent DPAs.

Exemption for smaller enterprises applies rarely

8. The exemption for smaller enterprises with fewer than 250 employees from the obligation to maintain an RPA in Art. 30 (5) GDPR largely runs dry. As the counter-exceptions are wide, the exemption rarely applies.

Room for simplification and improvement

9. Based on the above, we issue the following recommendations: The bureaucratic burden could be reduced by the provision of improved official templates for an RPA which meet the following criteria:
   - they are harmonised and translated into the respective national language,
   - they combine the advantages of existing templates of national DPAs, e.g. by
     - being clearly structured,
     - being self-explanatory or containing direct links to sources where further information is available,
     - offering checkboxes or, preferably, drop-down menus at least for the most relevant information (like the template of the French DPA),
   - they provide more help for small and medium-sized enterprises on how to create a simplified RPA.
10. Art. 33 GDPR obliges the controller to document personal data breaches and to report specific data breaches to the competent data protection authority. The notification must be made "without undue delay" and, "where feasible", within 72 hours after the controller has "become aware" of the breach.
11. The GDPR defines a "personal data breach" as a security breach which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data which are transmitted, stored or otherwise processed.

12. According to Art. 33 GDPR, the notification shall contain at least

    - a description of the nature of the personal data breach,
    - the name and contact details of the data protection officer or other contact point where more information can be obtained,
    - a description of the likely consequences of the personal data breach and
    - a description of the measures taken or proposed to be taken by the controller to address the personal data breach.

13. In addition, France, Germany[2] and Italy request some information that is not required by the GDPR. For instance, France and Italy ask, inter alia, for security measures taken before the data breach and the data breach's estimated level of severity. We consider these requirements to be gold plating.

gold plating by France, Germany and Italy

14. Interestingly, not all notification forms request every piece of information that Art. 33 GDPR requires. For instance, the German online notification form does not require the name and contact details of the data protection officer.

15. Overall, the information to be included in the notification varies significantly in terms of its level of detail. The Austrian form requests the smallest amount of information, followed by the German, French and Italian form. However, it must also be considered that the Italian form operates mainly with checkboxes as opposed to the open text boxes that the Austrian and German forms use predominantly. Furthermore, while Italy requests more information than the other three Member States, it also provides guidance on some aspects that are not further specified in the other Member States, for example, regarding the measures taken or proposed to be taken by the controller to address the personal data breach.

16. Based on the above, we issue the following recommendations:

    - Member States should refrain from requesting information that is not required by the GDPR and
    - notification forms should be made more user-friendly, e.g. by using checkboxes instead of open text boxes.

prevention of gold plating and user-friendly notification forms recommended

2 For Germany, the notification form of the LfDI Baden-Württemberg was analysed.

Key findings of the assessment of the regulatory burdens (Prognos AG and CSIL)

Approach

1. Part B of this study compares the regulatory burden related to the implementation of Art. 30 and 33 of the **General Data Protection Regulation (GDPR)** in four EU Member States based on the concept of compliance costs. The empirical assessment is informed by a total of 67 in-depth interviews conducted with companies and experts across the four Member States.

Current practice

2. Art. 30 GDPR requires businesses to document all processing activities involving personal data in a record of processing activities (RPA). If a data breach occurs, companies are, according to Art. 33, obliged to notify the supervisory authority within 72 hours. Apart from one exception, all companies surveyed had fully implemented the requirements of Art. 30 and 33.

3. In practice, the exception for small and medium-sized enterprises under Art. 30 (5) cannot be used by businesses, as almost every company handles special categories of data under Art. 9 (1) (e.g. payroll accounting) and is thus obliged to create and maintain an RPA.

4. **The notification process under Art. 33 can be conducted digitally.** In France and Italy, the notification must be submitted to the authority via an electronic form; in Austria via mail or e-mail and in Germany depending on the regulations of the data protection authority of the respective federal state, often as an electronic form, alternatively by e-mail or phone.

5. **The implementation of and compliance with Art. 30 and 33 require substantial efforts on the part of the companies.** No country-specific differences for the imposed burdens have been identified in the comparative study. Instead, the burdens are related to the size of the company and the number of processing activities.

Uncertainties due to insufficiently defined legal terms shape corporate practice

6. **Due to insufficiently defined legal terms, companies rely heavily on official information and templates to comply with Art. 30 GDPR.** As the GDPR does not define what a "processing activity" is, but rather only contains a wide definition of the term "processing", meaning any operation involving personal data, companies across all Member States used templates that were either provided by the authorities, consultants or, in rare cases, by companies themselves.

7. **Especially large and micro-enterprises are affected by the regulations of Art. 30 GDPR.** Micro-enterprises often do not have sufficient resources and/or competencies and are therefore particularly dependent on external service providers, which results in

additional costs. Large companies, on the other hand, often have more complex business models that operate with personal data.

8. The study shows extensive use of external consultancies supplementing the internal efforts. External expertise was necessary to ensure a timely and sufficient level of compliance to prevent sanctions and damage to the companies' brand reputation.

9. **Companies with B2C business models faces substantial burdens due to Art. 30 GDPR** as B2C approaches result in a particularly high number of processing activities.

10. **The maintenance and updating of the RPA represent substantial annual expenses perceived as a distinct burden.** Companies spend annually an average of one hour per processing activity to maintain the included information. There was no country difference identified; thus, compliance costs are dependent on the size of the company and RPA, ranging from 30 to 40 hours for micro- and small enterprises and from 92 to 297 hours for medium-sized and large enterprises. The majority indicated that the RPA is used only for compliance reasons; accordingly, these efforts are perceived as a special burden.

Maintenance and updating of the RPA are not subject to country-specific differences, but generate significant costs

11. **Internal processes and the risk assessment require the most time and effort for companies when reporting data breaches.** The data protection officer must be informed of the data protection incident and conduct a risk assessment to decide whether the incident must be reported to the authority. Risk is also indeterminate, which is why assessment frequently involves significant effort and is perceived as a burden.

12. **The implementation of the notification process is not a specific burden, except in France.** The online form in France imposes a burden because it lacks user orientation and a good user experience (e.g. through intuitive user interface, clear instructions as well as the possibility to store recurring details). For example, it is not possible to save entries for later use or to return to previous pages for adjustments. In Italy and some federal states in Germany, there are also online portals, but these were not mentioned as a burden. Otherwise, the notification is made by e-mail or via predefined forms that must be sent to the authorities. In Austria, the predefined form is mandatory.

Proposals for reducing administrative burdens

13. **More precise definitions of indeterminate legal terms.** Indeterminate legal terms create uncertainty, additional efforts and consultancy costs. The GDPR should be amended by commenting or changed to clearly define the terms used. This would also make it possible to unify and standardise templates for records of processing activities (RPA) for all Member States.

SMEs need legal certainty in the use of the opening clause

14. **Enforcing the opening clause for small and medium-sized enterprises.** The practical implementation of the opening clause for small and medium-sized enterprises would reduce the burden on companies significantly. This requires a clear definition of which data

subject to special protection under Art. 9 (1) GDPR may be processed without the need to create a RPA.

15. **Improved support from official authorities.** Consultancy services as well as best-practice examples, templates and information that are particularly practice-oriented and thus provide immediate value added for affected companies.

16. **Consistent reporting procedure among data protection authorities, considering user-centricity, fluent user experience and automation.** The administrative implementation of Art. 33 should be standardised as an online solution to reduce the time per notification. Reporting via automated and user-friendly online platform saves time, especially if company data can be stored and/or typical cases can be recalled.

Part A: Comparative legal study by cep and Alerion on administrative requirements related to Art. 30 and 33 of the General Data Protection Regulation

Part A prepared by:

cep
Kaiser-Joseph-Straße 266
79098 Freiburg im Breisgau
Germany

Dr. Lukas Harta, LL.M.
Dr. Anja Hoffmann
Dr. Matthias Kullas
Prof. Dr. Andrea de Petris

Alerion
137 rue de l'Université
75007 Paris
France

Carole Bui
Caroline Leroy-Blanvillain
Corinne Thierache

I. Introduction

This study covers two selected sets of obligations under the General Data Protection Regulation[3] (GDPR) and focusses on the legal and administrative requirements for private businesses with regard to the preparation and maintenance of a record of processing activities according to Art. 30 GDPR (Section III) as well as the requirements related to the notification of personal data breaches to the competent supervisory authority according to Art. 33 GDPR (Section IV). For this study, it is assumed that the relevant provisions of the GDPR apply to the respective private business and that the provisions of other specific legal acts do not take precedence instead.[4]

Beforehand, we will provide an overview of some general aspects of the GDPR which are relevant for the understanding of this study (Section II).

II. The General Data Protection Regulation (GDPR)

1. Objectives of the regulation

The General Data Protection Regulation (GDPR) entered into force in 2016 and applies since 25 May 2018 to companies and entities which process personal data as part of their activities. The GDPR aims to protect the fundamental rights and freedoms of the individuals whose personal data are being processed. At the same time, it shall ensure the free movement of personal data.

2. Legal effects

a) Full harmonisation

In principle, the GDPR intends a full harmonisation of the national legislation on the protection of personal data in the EU.[5] Its provisions have an exhaustive and conclusive character to ensure an equivalent level of protection in all Member States. The Member States are therefore, in general, not allowed to introduce new principles relating to the lawfulness of the processing of personal data or impose additional conditions which do not comply with the principles set forth by the GDPR. Nevertheless, the GDPR provides for a significant number of opening clauses which allow the Member States to lay down additional, stricter or derogating national rules in accompanying legislation to the GDPR, leaving them a certain margin of discretion

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJEU L 119, 4 May 2016, p. 1–88.

4 For example, private businesses may also be subject to EU Directive 2002/58/EG on privacy and electronic communications and the respective national laws transposing this directive, in particular if they process personal data for the provision of telecommunications services on a commercial basis. These laws contain more specific provisions which might in some cases take precedence over the provisions in the GDPR. This study covers only the GDPR and does not deal with any more specific laws or the requirements arising therefrom.

5 CJEU, judgment of 28 April 2022, C-319/20 (Meta Platforms), ECLI:EU:C:2022:322, No 57.

with regard to their implementation.[6] This fact can, however, be disregarded for the purposes of this study as neither Art. 30 nor Art. 33 GDPR contain an explicit opening clause.

b) Immediate effect

As a regulation, the GDPR is binding in its entirety and generally and directly applicable in all Member States.[7] Its provisions need not be transposed into the national laws of the Member States. Rather, its provisions generally have immediate effect in the national legal systems without the national authorities being required to adopt measures of application.[8] However, some of the GDPR's provisions require the adoption of measures of application by the Member States.[9] Inter alia, the Member States must – by virtue of law – designate independent national data protection authorities (DPAs) whose task is to enforce the provisions of the GDPR.[10] The DPAs must be equipped with adequate resources;[11] however, the concrete design of these supervisory authorities is essentially left to the Member States.[12] Furthermore, the Member States must provide for an effective system of sanctions for violations of the GDPR.[13] These obligations are supplemented by the Member States' general obligation to implement the provisions of the GDPR. According to Art. 291 TFEU, Member States are obliged to adopt all measures of national law necessary to implement the GDPR as a legally binding EU act. Such national implementation measures may consist in the adoption of legislation or the adaptation of administrative activities to the requirements of the GDPR. This could lead to a different enforcement of the GDPR within the Member States.

3. Regulatory content and relevant definitions

The GDPR applies to the processing of personal data, whether or not by automated means.[14] "Personal data" are any information relating to an "identified or identifiable" natural person (the "data subject").[15] "Processing" means any operation involving personal data, including their collection, storage, use, dissemination and erasure.[16]

---

6 CJEU (fn. 5), No 57.

7 Art. 288 Treaty on the Functioning of the European Union (TFEU).

8 CJEU (fn. 5), No 58.

9 CJEU (fn. 5), No 58 et seq.

10 Art. 51 (1) et seqq., Art. 54 (1) GDPR.

11 Art. 52 (3) GDPR.

12 Nguyen, A., in Gola, DSGVO, 2nd. edition 2018, Art. 51 No 3.

13 Art. 83 GDPR.

14 Art. 2 (1) GDPR. If the processing is not carried out by automated means, the GDPR only applies as far as such data form part of a filing system or are intended to do so.

15 Art. 4 No 1 GDPR.

16 Art. 4 No 2 GDPR.

The regulation applies to the processing of personal data by controllers and processors. A "controller" is a body which determines the purposes and means of the processing of personal data,[17] namely, the why and how of the processing.[18] It is thus the body that decides certain key elements of the processing. A "processor" is a separate entity in relation to the controller;[19] it processes personal data on behalf of the controller,[20] for example, an IT service provider hired by the controller to perform general IT support on its systems which include a vast amount of personal data.[21] The concept of controller and its interaction with the concept of processor play a crucial role in the application of the GDPR because they determine who shall be responsible for compliance with different data protection rules.[22]

The GDPR stipulates several basic principles for the processing of personal data.[23] Personal data must be processed lawfully, transparently and fairly and may only be collected for specified, explicit and legitimate purposes. The processing of personal data must be limited to what is necessary (data minimisation) and may not be processed in a manner that is incompatible with the purposes for which they were originally collected (purpose limitation). Furthermore, personal data must be accurate, kept up to date and may only be stored for the period for which it is needed with regard to the purpose of the processing. In addition, controllers and processors must ensure an adequate security of the data and use technical or organisational measures to protect the data against loss, unlawful processing, destruction or damage.

The GDPR explicitly imposes the responsibility for compliance with the above-mentioned data protection principles on the controller. However, the controller is not only responsible for the compliance with the principles, but must also be able to demonstrate compliance, in particular to the supervisory authorities (principle of accountability) (Art. 5 (2) GDPR).[24] This also means that the controller bears the burden of proof for the lawfulness of data processing. These accountability obligations force controllers to maintain and provide comprehensive documentation.

---

17 Art. 4 No 7 GDPR.

18 EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 7 July 2021, p. 3, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en.

19 EDPB (fn. 18), p. 3.

20 Art. 4 No 8 GDPR.

21 EDPB (fn. 18), p. 27 f. The GDPR also introduces more specific rules on the use of controllers.

22 EDPB (fn. 18), p. 7, No 2.

23 Art. 5 (1) GDPR.

24 Art. 5 (2) GDPR. See also EDPB (fn. 18), Part 1, Sect. 1, No 6, p. 8.

The accountability principle is central within the GDPR.[25] Although Art. 5 (2) GDPR directly assigns the accountability to the controller, some of its provisions on personal data processing are addressed not only to controllers, but also to processors.[26] The GDPR also addresses some more specific accountability obligations to both controllers and processors, inter alia to maintain and provide appropriate documentation upon request. Both controllers and processors can be fined in the case of non-compliance with the obligations of the GDPR that are relevant to them and both are directly accountable towards supervisory authorities by virtue of their obligations.[27]

The accountability principle is also reflected in Art. 30 GDPR, which lays down the controller's and processor's obligations to maintain a record of processing activities with extensive information (see Section III). Art. 30 GDPR is an excellent example for a documentation obligation which the GDPR regulates in further detail.

Furthermore, the accountability principle is the basis for the controller's obligation in Art. 33 (5) GDPR to document all personal data breaches which have occurred during their activities.[28]

4. Possible national divergences in the implementation, application and enforcement of the GDPR

Despite the direct applicability and the fully harmonising effect of the GDPR, possible national divergences with regard to the understanding, application and enforcement of Art. 30 and 33 GDPR may arise in particular from the following facts:

Abstract provisions, indefinite legal terms and regulatory gaps lead to a different implementation and enforcement in the Member States

First, some of the provisions of the GDPR are quite abstract, which is also due to the fully harmonising approach of the GDPR and the complex regulatory subject matter.

Second, the GDPR contains a great number of indefinite legal terms that can be interpreted differently and may thus lead to a different understanding and application of its provisions.

Third, the GDPR leaves open specific points, questions or details or does not regulate them completely. Therefore, the question is to what extent such regulatory gaps or missing details create a certain leeway for the Member States to regulate these missing aspects or otherwise fill or handle these gaps in their national implementation or enforcement practices.

25 EDPB (fn. 18), Part 1, Sect. 1, No 7, p. 8.

26 EDPB (fn. 18), Part 1, Sect. 1, No 3, p. 7.

27 EDPB (fn. 18), Part 1, Sect. 1, No 9, p. 8.

28 Art. 29 Working Party, Working Paper 250 rev. 1, Guidelines on Personal data breach notification under Regulation 2016/679 of 3 October 2017, last revised and adopted on 6 February 2018, hereinafter referred to as "Guidelines WP 250", p. 31, available at https://ec.europa.eu/newsroom/article29/items/612052.

Fourth, the GDPR is enforced at the national level by the national DPAs. Since the GDPR contains numerous indefinite legal terms and does not regulate every point in detail, some national DPAs have published various guidelines, recommendations and short papers on specific GDPR provisions or legal questions to eliminate ambiguities and ensure a uniform interpretation and application of the GDPR.

This leads or may lead to differences in the enforcement of the law and thus also to different bureaucratic burdens, insofar as the European Data Protection Board (EDPB) has not yet issued EU-wide applicable guidelines and recommendations on the respective issue that lead to a uniform line in enforcement.

5. The Guidance of the European Data Protection Board (EDPB)

The EDPB is an independent body established by the GDPR, which is composed of representatives of the Member States' DPAs and the European Data Protection Supervisor and aims to ensure a uniform application of the GDPR in the EU.[29] Its main tasks include the provision of general guidance, including guidelines, recommendations and best practices regarding the GDPR to clarify the law and to promote a common understanding of EU data protection laws.[30] Inter alia, the Board is issuing guidelines on the interpretation of core concepts of the GDPR.[31] The EDPB is the successor of the Art. 29 Working Party, which was the advisory body on data protection and privacy under the former data protection directive.[32] This study takes into account the relevant guidance issued by the EDPB and the national DPAs of the selected Member States.

III. Regulatory burdens arising from the obligation to maintain a record of processing activities according to Art. 30 GDPR

This chapter examines which regulatory burdens arise for private companies from the obligations under Art. 30 GDPR with regard to the preparation and maintenance of a record of processing activities (RPA).

29 Art. 68, 70 (1) GDPR.

30 https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en; Art. 68 (1) GDPR.

31 In addition, the EDPB may also advise the European Commission and issue binding decisions in certain cases to ensure consistency of the activities of national DSAs on cross-border matters (Art. 64, 70 GDPR).

32 Art. 29, 30 Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

1. EU level

a) Legal sources

aa) Art. 30 GDPR

The obligation to maintain an RPA is regulated by Art. 30 GDPR. This article does not contain an explicit opening clause for the Member States.

bb) Guidance from the European Data Protection Board (EDPB)

The former Art. 29 Working Party had issued a position paper[33] on the derogations from the obligation to maintain an RPA, which has been endorsed[34] by the EDPB. This paper encourages national supervisory authorities to provide tools to facilitate the preparation and management of RPAs for SMEs. Beyond this, the EDPB has not issued any further written guidance on Art. 30 GDPR. In particular, the EDPB has so far not provided uniform proposals or templates for the RPA.

b) Subjects of the duty

The persons obliged to comply with the duties under Art. 30 GDPR are the controllers and processors or their representatives.

c) Overview and purpose of the duties under Art. 30 GDPR

Art. 30 GDPR obliges controllers and processors to maintain an RPA under their responsibility. An RPA is a document which is to contain extensive information on the processing operations carried out by the respective company or body with regard to personal data. The obligation to maintain an RPA is one of the documentation requirements which the GDPR regulates in detail. The function of the RPA is to enable the controller or processor themselves and possibly the national DPA to obtain an overview of all the controller's or processor's data processing activities. It additionally serves to enable the controller or processor to prove that their data processing complies with the GDPR. The RPA is thus an instrument of accountability of the controller (Art. 5 (2) GDPR).

d) The notion of a "processing activity"

The GDPR does not define the notion of a "processing activity" beyond the definition of "processing".[35] It also leaves open to what level of detail these "processing activities" must be described.

---

33 Art. 29 Working Party, Position Paper of 19 April 2018 on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR, available at https://ec.europa.eu/newsroom/article29/items/624045.

34 https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en.

35 Cf. Section A. II. 3. above.

e) Information to be included in the record of processing activities (RPA)

According to Art. 30 GDPR, the information to be included in the RPA is partly different for controllers and processors.

aa) Controllers

Controllers must include the following information:[36]

- name and contact details, namely,
  - the name of the controller,
  - the contact details of the controller,
  - the controller's representative, if the controller is obliged to designate a representative in the EU,
  - the name of the controller's data protection officer (if appointed),
  - the joint controller, where the controller determines the purposes and means of the processing jointly with another controller,
- the purposes of the processing,
- a description of the categories of data subjects,
- a description of the categories of personal data,
- the categories of recipients to whom the personal data have been or will be disclosed; this includes recipients in third countries or international organisations,
- any transfers of personal data to a third country or an international organisation, including the identification of that country or organisation,
- "where possible", the envisaged timelines within which the different categories of data must be deleted (erased);
- "where possible", controllers must also include a general description of the technical and organisational data security measures (TOMs) according to Art. 32 (1) GDPR.

bb) Processors

Processors must also maintain a record of all categories of processing activities they carry out on behalf of a controller. They must include the following information:[37]

36 Art. 30 (1) lit. a) – g) GDPR.

37 Art. 33 (2) lit. a) – d) GDPR.

- name and contact details, namely,
  - the name of the processor or processors,
  - the contact details of the processor or processors,
  - the processor's representative, where the processor is obliged to designate a representative in the EU,
  - the name of the processor's data protection officer (if appointed),
  - the name of each controller on whose behalf the processor is acting,
  - the contact details of each controller on whose behalf the processor is acting,
  - the representative of any of the controllers, where the controllers are obliged to designate a representative in the EU,
- the categories of processing carried out on behalf of each controller,
- any transfers of personal data to a third country or an international organisation, including the identification of that country or organisation;[38]
- "where possible", processors must also include a general description of the technical and organisational data security measures (TOMs) according to Art. 32 (1) GDPR.

f) Design of the record of processing activities

aa) Format

The GDPR stipulates that the RPA shall be in writing, including in electronic form. It is, however, unclear which format the respective national DPA may request the RPA; for example, whether the RPA must be provided in writing or electronically or only partially in writing.

bb) Language

The GDPR does not regulate in which language the RPA must be kept or provided to the authority. This may also result in national differences.

g) Exemption from the duty to maintain a record of processing activities

Art. 30 (5) provides for an exemption for small and medium-sized enterprises or organisations (SMEs) from the obligation to maintain an RPA. Companies with fewer than 250 employees shall not be required to maintain an RPA. However, this exception does not apply if the processing involves risks to the rights and freedoms of data subjects, occurs more often than occasionally or includes special sensitive categories of data (health data, for example). If at

38 If the transfer is not otherwise allowed by the GDPR and can only be based on the derogation for the private sector according to the second subparagraph of Art. 49 (1) GDPR, the controller must also document which "suitable safeguards" it has taken with regard to the protection of personal data [Art. 31 (1) lit. e GDPR].

least one of these conditions is fulfilled, the documentation obligation revives irrespective of the company's qualification as an SME.

The Art. 29 Working Party has clarified in its Working Paper[39] endorsed by the EDPB that there are three types of processing to which the derogation does not apply:

- processing that is likely to result in a risk to the rights and freedoms of data subjects,
- processing that is not occasional,
- processing that includes special categories of data or personal data relating to criminal convictions and offences.

It has also clarified that these three types of processing are alternative ("or") and the occurrence of any one of them on their own triggers the obligation to maintain the record of processing activities.

Beyond this, it has clarified that the exemption does not apply even if the processing is likely to result in a normal risk (and not just a high risk).

However, SMEs which conduct one or more of the three critical types of data processing mentioned above must only maintain records of those critical processing activities. For example, a small organisation is likely to regularly process data regarding its employees. As a result, such processing cannot be considered "occasional" and must therefore be included in the record of processing activities. Other processing activities which are, in fact, "occasional", however, do not need to be included in the record of processing activities (unless they can also be attributable to one of the other two types of processing).[40]

According to the EDPB, a data protection activity can only be considered to be "occasional" if it is not carried out regularly and occurs outside the regular course of business or activity of the controller or processor, for example, under random, unknown circumstances and within arbitrary time intervals.[41]

---

39 Art. 29 Working Party, Position Paper of 19 April 2018 (fn. 33), p. 1.

40 Art. 29 Working Party (fn. 33), p. 2.

41 EDPB, Guidelines 2/2018 of 25 May 2018 on the derogations of Art. 49 under Regulation 2016/679, p. 4, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf; Art. 29 Working Party Position Paper of 19 April 2018 (fn. 33), p. 2, referring to former WP 29 Guidelines on Art. 49 of Regulation 2016/679 [WP 262].

The exception from the duty to maintain an RPA is thus relativised and subject to a risk assessment. In addition, important terms in Art. 30 (5) are subject to interpretation (for example, at which point is data processing carried out regularly and thus not "occasionally"), which may lead to different applications of this exception.

h) Making available of the RPA to the supervisory authority

The controller, the processor or their representative is obliged to make the RPA available to the national DPA on request.[42] The purpose of this obligation is to enable the DPA to monitor the processing operations based on these records.[43]

Failure to provide documentation may result in an administrative fine of up to 10 million euros or up to 2 per cent of the company's total worldwide annual turnover of the preceding financial year.[44] In addition, the principle of responsibility can lead to a shift in the burden of proof in the case of complaints and court proceedings and can have a decisive impact on case law.[45]

2. Austria

a) Relevant national legal and other sources

aa) Primary legislation

Legislative competence for data protection law lies with the federal level.[46] Data protection law is laid down in the Data Protection Act (Datenschutzgesetz, DSG).[47] It does not contain specific provisions with regard to the duties under Art. 30 GDPR.[48]

bb) Secondary legislation

In Austrian law, there is no secondary legislation that contains information on the implementation or enforcement of Art. 30 GDPR.

42 Art. 30 (4) GDPR.

43 Recital 82 of the GDPR.

44 Art. 83 (4) lit. a) GDPR.

45 Gola, DS-GVO, Einl. No 64.

46 Art. 10 (1) No 13 of the Federal Constitutional Law, available in a bilingual version translated by the Federal Chancellery at https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1930_1/ERV_1930_1.pdf.

47 The DSG was originally passed in 1999, BGBl. I Nr. 165/1999, adapted to the GDPR in 2018, BGBl. I Nr. 23/2018, and amended last in 2021, BGBl. I Nr. 148/2021. A bilingual version translated by the Federal Chancellery is available at https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.pdf.

48 While § 49 DSG does contain an RPA provision, it is in the context of the implementation of Law Enforcement Directive (EU) 2016/680.

cc) Guidance from Austrian public authorities

The data protection authority, the Datenschutzbehörde (DSB), is an independent federal authority[49] that serves as a national data protection authority according to Art. 51 GDPR.[50] Thus, its competence includes the enforcement of Art. 30 GDPR.

The DSB has issued a guideline on the GDPR (hereinafter referred to as the "DSB guideline").[51] However, it has not issued a template on how to design an RPA. In fact, the DSB guideline explicitly states that it is up to controllers and processors how to design the RPA and that there is no template from the DSB.[52] In addition, the DSB guideline states that notifications to the data processing register (Datenverarbeitungsregister, DVR) that had to be prepared prior to the GDPR may, but do not have to, be used as RPA template.[53]

dd) Selection of relevant national case law

The Federal Administrative Court (Bundesverwaltungsgericht, BVwG), the court that decides about appeals against DSB decisions, has decided on two cases in which the DSB found a violation of Art. 30 GDPR.[54] One of those decisions was appealed to the Supreme Administrative Court (Verwaltungsgerichtshof, VwGH), which upheld the decision.[55] However, Art. 30 was not the focus of either decision.

ee) Other sources

The Austrian Chamber of Commerce (Wirtschaftskammer Österreich, WKO), an association representing most Austrian business since membership is – for most businesses – mandatory, has RPA templates for controllers[56] as well as for processors.[57]

---

49 https://www.dsb.gv.at/.

50 §§ 18, 19 DSG.

51 Leitfaden zur Verordnung (EU) 2016/679, available at https://www.dsb.gv.at/dam/jcr:5fc3b77f-d546-4609-aca0-e34035979549/DSGVO_Leitfaden_2022.pdf.

52 P. 45.

53 DVR notification templates are not available on the DSB website. Templates as of 2004 can be retrieved at https://handlungsplan.net/wp-content/files/Formblatt_1_Angaben_zum_Auftraggeber.pdf, https://handlungsplan.net/wp-content/files/Formblatt_2_Meldung_einer_Datenanwendung.pdf and https://handlungsplan.net/wp-content/files/Formblatt_4_Angaben_zu_ergriffenen_Datensicherheitsmassnahmen.pdf.

54 BVwG, decision of 20 August 2020, W258 2217446-1, available at https://ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20200820_W258_2217446_1_00/BVWGT_20200820_W258_2217446_1_00.pdf, and decision of 26 November 2020, W258 2227269-1, available at https://ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20201126_W258_2227269_1_00/BVWGT_20201126_W258_2227269_1_00.pdf.

55 VwGH, decision of 14 December 2021, Ro 2021/04/0007-4, available at https://ris.bka.gv.at/Dokumente/Vwgh/JWT_2021040007_20211214J00/JWT_2021040007_20211214J00.pdf.

56 Available at https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-Verantwortlicher.docx.

57 Available at https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-Auftragsverarbeite.docx.

b) The notion of a "processing activity"

No definition of "processing activity" in GDPR

The DSB guideline does not define the notion of a "processing activity". Neither does it specify beyond listing the categories of information required how detailed the RPA must be.

c) Information to be included in the RPA

While there is no template from the DSB, according to its guideline, the following information must in any case ("jedenfalls") be included in the RPA:[58]

aa) Controllers

- name and contact details of the controller (according to the WKO template, that includes the postal address, e-mail address and, if applicable,[59] other contact data such as the phone number),
- if applicable: data of
  - a joint controller,
  - the controller's representative,
  - the data protection officer.

  According to the WKO template, that includes the name, postal address, e-mail address and, if applicable,[60] other contact data such as the phone number.
- the purposes of the processing,
- a description of the categories of data subjects (the WKO template names as examples customers, employees and suppliers) and of the categories of personal data (namely, categories of persons and types of data concerned),
- categories of recipients, including recipients in third countries or international organisations,
- if possible: deletion periods, description of technical and organisational measures (according to the WKO template, that includes confidentiality, integrity, availability and resilience, pseudonymisation and encryption, and measures of evaluation).

58 DSB guideline, pp. 44–45.

59 In German: "allenfalls".

60 In German: "allenfalls".

The WKO template also includes:

- information on whether a data protection impact assessment was carried out; if so, when; if not, why not,
- a description of the legal basis for the data processing,
- information on where contracts, declarations of consent and other documents can be found,
- information on whether sensitive data according to Art. 9 GDPR[61] or personal data relating to criminal convictions and offences according to Art. 10 GDPR[62] are processed,
- documentation of guarantees for data transfers to third countries that are not based on Art. 45, 46, 47 or 49 (1) subpara. 1 GDPR.

bb) Processors

The DSB guideline merely mentions that all categories of activities carried out on behalf of the controller must be indicated.[63] It does not mention the other categories of data referred to in Art. 30 (2) GDPR, such as the name and contact details of the processor.

The WKO template lists:

- name and contact data (postal address, e-mail address and, if applicable, further contact data such as the phone number) of the processor(s) and, if applicable, of the processor's data protection officer,
- name and contact data (postal address, e-mail address and, if applicable, further contact data such as the phone number) of the controller(s) and, if applicable, the controller's data protection officer and the controller's representative,
- categories of processing activities carried out on behalf of the specific controller,
- recipients in third countries (categories of recipients resp. recipients in third countries and international organisations, name of the third country, documentation of guarantees for data transfers to third countries that are not based on Art. 45, 46, 47 or 49 (1) subpara. 1 GDPR,
- general descriptions of technical and organisational measures (confidentiality, integrity, availability and resilience, pseudonymisation and encryption, and measures of evaluation).

61 Such as data revealing racial or ethnic origin, political opinion or religious beliefs.

62 Data relating to criminal convictions and offences.

63 DSB guideline, p. 45.

cc) References/Guidance on the possible reduction of the effort involved in the creation of the RPA

In Austria, no such guidance exists.

d) Design of the RPA

aa) Format

The DSB guideline states that the RPA must be in writing.[64] According to Austrian legal literature, this includes electronic formats.[65]

The WKO templates are Microsoft Word files.

bb) Language

The RPA can be maintained in any language. However, if the RPA is made available to the DSB, the document must be made available in German.[66]

e) Actualisation/Update of the RPA

The DSB does not indicate when and how the RPA must be updated or how amendments must be documented. Austrian legal literature states that the RPA must be updated on an ongoing basis, adding new processing activities and deleting processing activities that are no longer up to date.[67]

f) Exemption from the duty to maintain an RPA (Art. 30 (5))

In Austrian legal literature, some authors understand processing to be "occasional" if it is not carried out on a regular basis and does not foreseeably take place repeatedly. In this understanding, activities such as the processing of employee pictures that take place whenever a new employee is hired is not occasional because foreseeably, new employees will be hired in the future.[68]

64 DSB guideline, pp. 44–45.

65 Jahnel, Kommentar zur Datenschutz-Grundverordnung (2020), Art. 30, para. 16; Horn, DS-GVO ante portas: Die Dokumentationspflichten im Verarbeitungsverzeichnis nach Art 30 DS-GVO, jusIT 2017, 106 (112); Bogendorfer in Knyrim (Hrsg.), Der DatKomm, Art. 30 GDPR, para. 45.

66 DSB guideline, p. 44.

67 Jahnel, Kommentar zur Datenschutz-Grundverordnung (2020), Art. 30, para. 20.

68 Jahnel, Kommentar zur Datenschutz-Grundverordnung (2020), Art. 30, para. 13; Gottweis, Das Verzeichnis von Verarbeitungstätigkeiten gem Art 30 DSGVO, in Jahnel (Hrsg.), Jahrbuch Datenschutzrecht 2018, 49 (60).

As for processing that includes special categories of data according to Art. 9[69] or Art. 10 GDPR,[70] the BVwG[71] and the VwGH[72] have ruled that a processing activity also involves such data – in the given case, data revealing political opinion – if the affinity for a particular political party is merely inferred from other characteristics. None of these decisions dealt with Art. 30 GDPR, however. They are relevant merely insofar as they interpret the notion of special categories of data according to Art. 9 GDPR. More specifically, the sanctioned company had carried out anonymous surveys in which it had asked for sociodemographic data such as age, education, income and place of residence as well as interest in election advertising from political parties. Based thereon, it inferred the party affinity of individuals with a given set of sociodemographic data and place of residence. The DSB sanctioned this behaviour, which was upheld by the BVwG and the VwGH. The other case referred to above, related to the same manner of conduct. While the DSB had imposed a fine as well, this fine was quashed by the BVwG, but not for reasons related to the interpretation of Art. 30 GDPR.[73]

As for processing that is likely to result in a risk to the rights and freedoms of data subjects, Austrian commentaries emphasise that since data processing is never completely without risk, the standard must be whether a risk is likely and how large the negative consequences would be.[74]

g) Making available of the RPA to the supervisory authority

As mentioned above, while the RPA may be maintained in any language, the RPA must be made available to the DSB in German.[75]

It is not specified in what form the DSB may request the RPA.

---

69 Such as data revealing racial or ethnic origin, political opinion or religious beliefs.

70 Data relating to criminal convictions and offences.

71 BVwG, decision of 20 August 2020, W258 2217446-1, available at https://ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20200820_W258_2217446_1_00/BVWGT_20200820_W258_2217446_1_00.pdf.

72 VwGH, decision of 14 December 2021, Ro 2021/04/0007, available at https://ris.bka.gv.at/Dokumente/Vwgh/JWT_2021040007_20211214J00/JWT_2021040007_20211214J00.pdf.

73 BVwG, decision of 26 November 2020, W258 2227269-1, available at https://ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20201126_W258_2227269_1_00/BVWGT_20201126_W258_2227269_1_00.pdf.

74 Jahnel, Kommentar zur Datenschutz-Grundverordnung (2020), Art. 30, para. 11; Bogendorfer in Knyrim (Hrsg.), Der DatKomm, Art. 30 GDPR, para. 60.

75 DSB guideline, p. 44.

3. France

a) Relevant national legal and other sources

aa) Primary legislation

In France, Art. 57 of the French Act[76] on data processing, data files and individual liberties (Act No 78–17 of 6 January 1978 as amended lastly by French Decree No 2019–536 dated 29 May 2019[77]) contains information on the implementation and enforcement of Art. 30 GDPR. It provides that the controller and, where appropriate, its representative shall maintain the RPA under the conditions laid down in Art. 30 GDPR.

These articles only provide for the application of Art. 30 GDPR. There is no derogation from this article in French legislation for private companies.[78]

bb) Secondary legislation

There is no secondary legislation on the implementation or enforcement of Art. 30 GDPR in France.

cc) Guidance from French public authorities

In France, the French data protection authority, named "Commission Nationale de l'Informatique et des Libertés" (CNIL) is the only responsible authority for the enforcement of Art. 30 GDPR. The CNIL was created by French Act No 78–17 of 6 January 1978. The CNIL is responsible for ensuring the protection of personal data contained in computer or paper files and respective processing, both public and private.[79] Furthermore, its task is to ensure that information technology remains at the service of citizens and that it does not infringe on human identity, human rights, privacy or individual or public freedoms.

It is responsible for ensuring the protection of personal data contained in computer or paper files and processing, both public and private.

The CNIL is an independent administrative authority, meaning a public organisation that acts on behalf of the French state without being placed under the authority of the French

---

76 Art. 57, French Act No 78–17 of 6 January 1978 on data processing, data files and individual liberties, available in French at https://www.legifrance.gouv.fr/loda/id/LEGISCTA000006095896.

77 See URL in fn. 76 to access the Act in its entirety.

78 Art. 100 of the above-mentioned French Act provides for specificities to be integrated in the RPA. However, this article is not relevant to this study as it concerns public bodies for prevention, investigation, detection or prosecution of criminal offences of the execution of criminal penalties and the free circulation of such data. Art. 100 can thus be widely disregarded for the purpose of the present study. Art. 100 is available in French at https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037817665.

79 Definition available only in French at https://www.cnil.fr/fr/cnil-direct/question/la-cnil-cest-quoi.

government or a French minister. The CNIL has a role of alerting, advising and informing to all audiences but also has a power of controlling and sanctioning.[80]

The CNIL has issued the following documents on Art. 30 GDPR which can be considered as official guidance:

- the CNIL's website is the main source for guidance on Art. 30 GDPR; the CNIL's guidelines and recommendations are indicated on a page dedicated to the RPA,[81]
- a short reference to an RPA in the processor's guidelines published in September 2017;[82]
- the CNIL proposes a basic RPA template[83] identical for controllers and processors designed to meet most common needs in terms of data processing, especially for small companies. The use of this template is recommended, but not mandatory.

dd) Selection of relevant national case law

For the time being, only one national case on the implementation and enforcement of Art. 30 GDPR has been identified:

In a decision rendered on 15 September 2021[84], the CNIL condemned a French company notably for not implementing an RPA or even producing any justification even after receiving the CNIL's notice and refused to apply the exception in Art. 30 (5) GDPR.[85]

ee) Other sources

In France, the CNIL in collaboration with Bpifrance has issued a guidance document. Furthermore, only one minor business association, Medinsoft, has published guidance on this matter.

---

80 More information about the CNIL's missions is available at https://www.cnil.fr/en/cnils-missions.

81 Guidelines from the CNIL with regard to the RPA available only in French at https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement.

82 CNIL, Processor's Guidelines, September 2017, p. 9, only available in French at https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf.

83 The template is available on the CNIL's website at https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement.

84 Deliberation of the restricted formation of the CNIL no. SAN-2021-014, 15 September 2021, concerning the French company *Société nouvelle de l'annuaire français (SNAF)*, available only in French at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044043045.

85 This decision will be discussed below, cf. Part A. III. 3. f).

(1) CNIL and Bpifrance

The CNIL in collaboration with Bpifrance[86] has issued a *"Practical guideline to GDPR awareness for small and medium-sized businesses"* available at the CNIL's website and notably directly under the CNIL's RPA template.[87]

(2) Medinsoft's Guidance

Medinsoft is a business association composed of more than 1,000 companies which constitutes a network for the promotion of the digital industry. The Medinsoft LEGAL'IN TECH commission published on 28 May 2019 a "GDPR White Book" which provides guidelines, notably on the implementation of Art. 30 GDPR, that are predominantly taken from the guidelines mentioned by the CNIL on its website.[88] The RPA template proposed by Medinsoft is the same as the one proposed by the CNIL.

b) The notion of a "processing activity"

The notion of a "processing activity" is not defined by the French legislation beyond the definition of "processing",[89] nor by the CNIL for the implementation of Art. 30 GDPR.

French Data Protection Authority provides examples of "processing activities"

The notion of a "processing activity", in France, refers to the main activities of the company requiring data collection and more generally data processing. The CNIL provides examples of processing activities such as recruitment, payroll management, training, badge and access management, sales statistics and prospect management.[90] The CNIL does not distinguish between the processing activities of small and large companies.

c) Information to be included in the RPA

The RPA must be detailed, at minimum, with each item listed in Art. 30 GDPR.

86 Bpifrance is an investment public bank whose mission is to assist French companies at every stage of their development, providing credit, guarantees, innovation aid and equity capital.

87 CNIL and Bpifrance, Practical guidelines to GDPR awareness for small and medium-sized businesses, pp. 31–33, 17 April 2018, available only in French at https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf.

88 Medinsoft, GDPR White book, 28 May 2019, available only in French at https://medinsoft.com/wp-content/uploads/2019/05/LivreBlanc_LegalInTech.pdf.

89 The CNIL defines on its website *"Processing of personal data"* as *"an operation, or a set of operations, concerning personal data, regardless of the process used (collection, recording, organisation, conservation, adaptation, modification, extraction, consultation, use, communication by transmission or dissemination or any other form of provision, reconciliation)"*. This definition is available only in French on the CNIL's website at https://www.cnil.fr/fr/definition/traitement-de-donnees-personnelles.

90 CNIL and Bpifrance, Practical guidelines to GDPR awareness for small and medium-sized businesses, p. 16, 17 April 2018, ibid.

However, the RPA basic template created by the CNIL[91] contains space for more information. This is the only template available and although it is not mandatory, lawyers recommend including such information in the RPA. Moreover, the template is identical for controllers and processors.

In France, the following information should be included in the RPA:

aa) Controllers[92]

- the name and contact details of the controller and, if applicable, of its representative, if the controller is not established in the European Union (according to the CNIL: name, postal address, e-mail address, ZIP code, city, phone number) (mandatory),
- where applicable, the name and contact details of the controller's data protection officer (according to the CNIL: name, postal address, e-mail address, ZIP code, city, country, phone number, company details if an external data protection officer is concerned) (mandatory where applicable),

For each category of processing activity and according to the information to be inserted in the CNIL's template, the RPA must contain at least the following elements:

- the date of creation and last update of the processing (mandatory according to the CNIL but not provided for by the GDPR),
- the name and the number/reference of the processing (mandatory according to the CNIL but not provided for by the GDPR),
- the date of creation and last update of each register form composing the RPA (mandatory according to the CNIL but not provided for by the GDPR),
- where applicable, the name and contact details of the joint controller of the processing carried out (according to the CNIL: postal address, ZIP code, city, country, phone number, e-mail address) (mandatory where applicable),
- the purposes of the processing, the objective for which the data are collected (mandatory); it is also possible to indicate for a main purpose and sub-purposes,

91 See fn. 83.

92 This list is provided by the CNIL on its website in accordance with its template, see fn. 83.

- the categories of data subjects (according to the CNIL: customer, prospects, employees, internal services (for example, finance department, human resources department etc., providers, candidates) (mandatory); in the CNIL's RPA template, it is possible to fill in a field to provide additional clarification regarding the concerned category; however, no example is given,
- the categories and description of personal data (according to the CNIL, for example, identity, family, economic or financial situation, banking data, connection data, location data, social security identification number) (mandatory),
- a description of the eventual sensitive data concerned[93] by the data processing (mandatory according to the CNIL but not provided for by the GDPR),
- the categories and description of recipients to whom the personal data have been or will be disclosed (according to the CNIL, this includes processors, internal services processing personal data, institutional or commercial partners, recipients from third countries or international organisations (mandatory); in the CNIL's RPA template, it is possible to fill in a field to provide for additional clarification regarding the concerned category (for example, the administrative and financial department can be indicated in the category of internal services processing data),
- any transfers of personal data to a third country or to an international organisation (recipients, country) and, in certain very specific cases, the safeguards provided for such transfers (for example, standard contractual clauses, binding corporate rules, adequate country, code of conduct, certification, Art. 49 GDPR exemption); a reference to the concerned documentation shall be indicated (mandatory),
- to the extent possible, the time limits for the deletion of the various categories of data, namely, the retention periods, or failing that, the criteria for determining them (mandatory to the extent possible), and,
- to the extent possible, a general description of the technical and organisational security measures implemented (according to the CNIL: traceability,[94] software protection, data backup, data encryption, monitoring of users' access, monitoring of processors and other measures to be defined)[95] (mandatory to the extent possible).

---

93 According to Art. 9 GDPR, sensitive data are data revealing racial of ethnic origin, political opinion, religious or philosophical beliefs and trade union membership as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

94 The CNIL does not define "traceability". However, when the CNIL refers to this notion, it is related to audits and logging. See CNIL's Guideline on security of personal data, p. 23, available in French at https://www.cnil.fr/fr/la-cnil-publie-une-nouvelle-version-de-son-guide-de-la-securite-des-donnees-personnelles.

95 These categories of technical and organisational security measures are listed in a drop-down list included in the CNIL RPA's template.

In the CNIL's RPA template, it is possible to fill in a field to provide for additional clarification regarding the concerned measures. However, no example is given.

The CNIL recommends that, to the extent possible, the RPA be enriched with additional information to make it a more comprehensive compliance management tool.[96] For instance, the CNIL recommends adding to the RPA the information the controller must provide to data subjects according to Art. 12 to 14 GDPR (inter alia, the legal basis of the processing, and as the case may be, the legal basis for the transfer of data to third countries, information on the rights that apply to the processing, the existence or non-existence of an automated decision, the origin of the data etc.) to allow the controller or the processor to rely on their RPA to draft the information notices.

The CNIL also recommends recording in the RPA a history of data breaches and a list of all documents related to data transfers outside the European Union (standard contractual clauses, binding corporate rules etc.) and to the sub-processors (sub-processing agreements).

bb) Processors[97]

As mentioned above, there is no separate official RPA template for processors in France. The CNIL only provides for an identical basic template for controllers and processors. This template may also be used and is effectively commonly used by French processors, especially by small and medium-sized companies. However, there is no guidance from the CNIL on how processors should fill in this template.

In accordance with the GDPR, processors must provide the following information in their RPA:

- the name and contact details of the processor and, if applicable, of its representative, if the processor is not established in the European Union (according to the CNIL: name, postal address, e-mail address, ZIP code, city, phone number) (mandatory),
- where applicable, the name and contact details of the processor's data protection officer (according to the CNIL: name, postal address, e-mail address, ZIP code, city, country, phone number, company details if an external data protection officer is concerned) (mandatory where applicable).

96 Guidelines from the CNIL with regard to RPA are available at https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement, cited above.

97 This list is provided by the CNIL on its website in accordance with its template, see fn. 83.

Beyond this, for each category of processing activity performed on behalf of clients, processors must include at least the following elements in the RPA:

- the contact details of each controller on whose behalf the processing activity is carried out and, if applicable, of its representative, if the controller is not established in the European Union (according to the CNIL: name, postal address, e-mail address, ZIP code, city, phone number) (mandatory),
- where applicable, the name and contact details of the controller's data protection officer (mandatory where applicable) (according to the CNIL: name, postal address, e-mail address, ZIP code, city, phone number, company details if an external data protection officer is concerned),
- the contact details of each sub-processor, and, if applicable, of its representative, if the sub-processor is not established in the European Union (according to the CNIL: name, postal address, e-mail address, ZIP code, city, phone number) (mandatory),[98]
- the categories of processing carried out on behalf of each client, namely, the operations actually carried out on their behalf (for example, the category "service of sending prospecting messages"; this may involve the collection of e-mail addresses, the secure sending of messages, the management of unsubscriptions etc.) (mandatory),
- any transfers of personal data to a third country or to an international organisation (recipients, country) and, in the very specific cases mentioned in the second paragraph of Art. 49 (1) GDPR (absence of an adequacy decision under Art. 45 GDPR, absence of the appropriate safeguards provided for in Art. 46 GDPR and inapplicability of the exceptions provided for in the first paragraph of Art. 49 (1) GDPR), the safeguards provided for such transfers must be mentioned; a reference to the concerned documentation shall be indicated (mandatory),
- to the extent possible, a general description of the technical and organisational security measures implemented (according to the CNIL: traceability[99], software protection, data backup, data encryption, monitoring of users' access, monitoring of processors, other measures to be defined) (mandatory to the extent possible).

In the CNIL's RPA template, it is possible to fill in a field to provide for additional clarification regarding the concerned measures. However, no example is given.

---

98 This piece of information is mentioned neither in Art. 30 (2) GDPR nor in the CNIL's RPA template. This information is, however, expressly required by the CNIL in the Processor's Guideline published in September 2017, p. 9, available only in French at https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf.

99 See fn. 94.

The CNIL recommends furthermore that, to the extent possible, the RPA be enriched with additional information to be a more comprehensive compliance management tool.

As there is only one RPA template published by the CNIL for both controllers and processors, the template contains fields to be filled in by controllers, while Art. 30 GDPR does not require processors to provide the requested additional information. Therefore, the following information is not mandatory for processors:

- the date of creation and last update of the processing,
- the name and the number/reference of the processing,
- the date of creation and last update of each register form composing the RPA,
- where applicable, the name and contact details of the joint controller for whom the processing is carried out (according to the CNIL: postal address, ZIP code, city, country, phone number, e-mail address),
- the purposes of the processing, the objective for which the data are collected; it is also possible to indicate a main purpose and sub-purposes,
- the categories of data subjects involved (customers, prospects, employees, internal services, providers, candidates); in the CNIL's RPA template, it is possible to fill in a field to provide additional clarification regarding the concerned category; however, no example is given,
- the categories and description of personal data (for example, identity, banking data, connection data, location data, social security identification number),
- a description of the eventual sensitive data concerned by the data processing (mandatory but not provided for by the GDPR),
- the categories and a description of the recipients to whom the personal data have been or will be disclosed, including processors, internal services processing personal data, institutional or commercial partners, recipients from third countries or international organisations); in the CNIL's RPA template, it is possible to fill in a field to provide additional clarification regarding the concerned category (for example, the administrative and financial department can be indicated in the category of internal services processing data); and,
- to the extent possible, the time limits for the deletion of the various categories of data, namely, the retention periods or, failing that, the criteria for determining them.

According to French lawyers, processors could effectively leave blank the text fields which the GDPR requires only for controllers. Unfortunately, the CNIL does not provide any guidance on this specific aspect. However, even if the information listed above is not mandatory for

controllers, lawyers recommend that processors include in their RPA all information listed in the above-mentioned bullet points which they can easily obtain, including from the controller itself. This is particularly advisable if the processor aims to use the RPA as a more comprehensive management and compliance tool as recommended by the CNIL. French processors may thus use the RPA template to centralise any information regarding the concerned data processing (including information indicated in the RPA template but not required by the GDPR for processors), notably if such information and any updates are easy to obtain.

cc) References/Guidance on the possible reduction of the effort involved in the creation of the RPA

There is no guidance on how companies' efforts for the creation of the RPA can be reduced. Each company must create a complete RPA with all the points above-mentioned. However, according to the CNIL's template, references to other documents can be made.

d) Design of the RPA

aa) Format

In France, the RPA shall be in written form, including in paper or electronic form[100]. The RPA's basic template is an Excel table composed of a general index listing all processing activities and of a form for each processing activity[101].

bb) Language

Art. 1 of the French Toubon Act[102] states that French is the language of education, work, exchanges and public services. However, there is no obligation within the French legislation concerning the RPA and the CNIL has not pro-nounced itself on this point. It is strongly recommended to use French as far as the CNIL should be considered as a public service.

e) Actualisation/Update of the RPA

The RPA must be regularly updated in line with functional and technical developments in data processing. In practice, any change in the conditions of implementation of each processing listed in the RPA (new data collected, extension of the retention period, new recipient of the processing operation etc.) must be included in the RPA. No indication is given by the CNIL concerning the way to document the amendments. However, lawyers recommend archiving

100 Guidelines from the CNIL, available at https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement, cited above.

101 CNIL's RPA template, available at https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement, cited above.

102 French Act No 94–665 of 4 August 1994 on the use of the French language, available only in French at https://www.legifrance.gouv.fr/loda/id/LEGITEXT000005616341/#:~:text=Dans%20la%20d%C3%A9signation%2C%20l'offre,la%20langue%20fran%C3%A7aise%20est%20obligatoire.

any documents relating to the above-mentioned changes in the perspective of operations of control conducted by the CNIL.

The modification must be made directly in the RPA document. The RPA template provided by the CNIL notably requires mentioning the date of update of each form as well as the date of update of each processing.

f) Exemption from the duty to maintain an RPA (Art. 30 (5))

CNIL very restrictive on exemptions

In France, the application of Art. 30 (5) GDPR is quite cautious and thus very limited. If there is any doubt as to whether this exemption applies to a processing operation, the CNIL recommends including the processing activity in the RPA.

In practice, this exemption is limited to very specific cases of processing, implemented on an occasional and non-routine basis, such as a communication campaign for the opening of a new establishment, provided that such processing does not raise any risk to the data subjects.

On its website, the CNIL provides other examples of a processing operated by SMEs which cannot fall under the exemption:[103]

- non-occasional processing: payroll management, customer/prospect and supplier management etc.,
- processing likely to result in a risk to the rights and freedoms of data subjects: geolocation systems, video surveillance etc.,
- processing of sensitive data: health data, offences etc.

In a decision rendered on 15 September 2021,[104] the CNIL refused to apply the exemption in Art. 30 (5) GDPR. The CNIL considered that even though the company only had a single employee (its president), its data processing was not occasional since it constituted the core of its activity. The company should therefore have implemented an RPA.

As the company did not comply with the deadline set in the CNIL's notice, nor subsequently, the CNIL considered that the company had failed to comply with the obligation set out in Art. 30 GDPR.

103 Guidelines from the CNIL, available in French at https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement.

104 See fn. 84.

The CNIL proceeded to condemn the company to a 3,000 euros administrative fine, with regard notably to the breaches constituted by Art. 16, 17, 30 and 31 GDPR, but also to make public, on Légifrance's[105] websites, its deliberation.

g) Making available of the RPA to the supervisory authority

Although the RPA is an internal and evolving document which should above all help the controller or the processor to manage their GDPR compliance, it must nevertheless be able to be communicated to the CNIL upon request.

In particular, the CNIL may use it as part of its mission to control data processing.

Private organisations (not entrusted with a public service mission) are not required to communicate the RPA to the public. Nevertheless, they may, if they consider it appropriate, communicate it to persons who request it.[106]

The CNIL does not impose a particular format. If a written RPA is required, the electronic form seems to be allowed for the submission of the RPA.

4. Germany

a) Relevant national legal and other sources

aa) Primary legislation

Data protection in Germany is primarily governed by the GDPR as directly applicable EU law. There is, however, still a national data protection law in Germany. On the federal level, data protection is regulated by the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG),[107] which, due to the primacy of EU law, only applies to the extent that the GDPR is not directly applicable.[108] The BDSG does not regulate further details concerning the obligations

105 https://www.legifrance.gouv.fr/.

106 Guidelines from the CNIL, available in French at https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement.

107 Federal Data Protection Act of 30 June 2017 (Federal Law Gazette 2017 I, p. 2097), as last amended by Art. 10 of the Act of 23 June 2021 (Federal Law Gazette 2021 I, p. 1858, and 2022 I, p. 1045); English version available at https://www.gesetze-im-internet.de/englisch_bdsg/index.html. The BDSG existed before the entry into force of the GDPR and has been adapted to the latter by the First and Second Act Adapting Data Protection Law to Regulation (EU) 2016/679 and Implementing Directive (EU) 2016/680. The second Act is available at https://dejure.org/ext/b6f2e53d32b96a20c7c710ba4ca86d69 (in German only). The BDSG is subordinate to other, more specific legal provisions on data protection in other Federal Acts (Section 1 (2) BDSG), which will not be further discussed in this study. For example, the substantive rules of the German Telecommunications and Telemedia Data Protection Act (Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)) transposing the ePrivacy Directive 2002/58/EG into German law will not be further addressed here. This directive contains special rules inter alia for the protection of the privacy of users of terminal equipment and is a "lex specialis" to the GDPR (cf. Art. 95 GDPR).

108 This means that the BDSG does not apply where the GDPR directly applies, cf. also Section 1 (5) BDSG.

around the maintenance of an RPA.[109] In addition, due to the federal structure of Germany, its 16 individual federal states have their own state data protection acts which apply in parallel to the BDSG. For example, Baden-Württemberg has enacted the State Data Protection Act of Baden-Württemberg (Landesdatenschutzgesetz, LDSG-BW).[110] However, these acts mainly apply to the processing of personal data by public bodies[111] and not by private companies and can thus be widely disregarded for the purpose of this study.[112]

From the above, it follows that there is no relevant specific German primary legislation governing or clarifying the obligations to maintain an RPA under Art. 30 GDPR. Insofar, solely Art. 30 GDPR applies. There is thus no derogation from Art. 30 GDPR in German legislation.

bb) Secondary legislation

There is no relevant specific German secondary legislation governing or clarifying the obligations to maintain an RPA under Art. 30 GDPR.

cc) Guidance from German public authorities

Data protection supervision in Germany is split between different authorities. Germany has a federal system of data protection supervision, which consists of the data protection supervisory authorities of the Federation (the "Bund") and the 16 federal states (the "Länder").

For companies providing telecommunications or postal services, the competent supervisory authority is the Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI) in Bonn.[113] The BfDI is an autonomous and independent supreme federal authority tasked inter alia with enforcing the GDPR within its competences.[114] However, for all other companies that are not subject to the exclusive jurisdiction of the BfDI – and thus for the majority of companies in the private sector

109 To avoid any misunderstandings, it should be mentioned that the BDSG indeed does contain a provision which regulates the controllers' and processors' duties with regard to the maintenance of a record of processing activities (RPA) in Section 70. However, this provision is an implementing provision which transposes Directive 2016/680 and thus only applies to the processing of personal data by the police and criminal justice authorities.

110 Landesdatenschutzgesetz Baden-Württemberg (LDSG-BW) as of 12 June 2018, GBl. (BW) 2018, p. 173, available at https://www.landesrecht-bw.de/jportal/?quelle=jlink&query=DSG+BW&psml=bsbawueprod.psml&max=true&aiz=true#jlr-DSGBW2018rahmen (in German only).

111 Section 2 (1) LDSG-BW. Parallel to the BDSG which inter alia governs the data processing by public bodies at the federal level, the Länder have insofar made use of the GDPR's opening clauses for data protection in the public area.

112 They might apply exceptionally in certain cases of contract processing between state authorities and companies (not relevant for the purpose of this study). However, the State Data Protection Acts are relevant for companies when it comes to determining the competent data protection authority, see cc) below.

113 Section 29 of the German Telecommunications and Telemedia Data Protection Act of 21 June 2021 (TTDSG), available at https://www.gesetze-im-internet.de/ttdsg/, and Section 9 (1) BDSG.

114 https://www.bfdi.bund.de/EN/DerBfDI/UeberUns/DieBehoerde/diebehoerde_node.html.

– the supervisory authorities of the Länder are competent.[115] If the controller or processor has more than one establishment in Germany, the competent supervisory authority is the authority of the federal state ("Land") in which the controller's or processor's central administration is based (unless another establishment must be considered its main establishment).[116] Therefore, for private entities which have their sole establishment or their central administration (main establishment) in Baden-Württemberg, the competent supervisory authority within the meaning of the GDPR is the data protection commissioner of Baden-Württemberg (Landesbeauftragter für Datenschutz und Informationsfreiheit, LfDI) in Stuttgart (hereinafter referred to as "LfDI Baden-Württemberg").[117]

(1) The German Data Protection Conference (DSK)

The independent data protection supervisory authorities of the Länder and the BfDI have come together in the so-called Data Protection Conference (Datenschutzkonferenz, hereinafter referred to as "DSK").[118] This conference serves to coordinate the work of the German data protection authorities to achieve a uniform application of European and national data protection law and jointly advocating for its further development. The guidance of the DSK applies subject to a different (future) view of the EDPB.

German Data Protection Conference issues guidance and templates

The DSK has issued the following documents on Art. 30 GDPR:

- a guidance document named "Information on the record of processing activities, Art. 30 GDPR" of February 2018[119],
- Short Paper No 1 of 17 December 2018 on the record of processing activities – Art. 30 GDPR[120],

115 According to Section 40 (1) BDSG, the authorities pursuant to the law of the Länder shall monitor the application of data protection legislation by private bodies within the scope of the GDPR. All in all, the state data protection authorities of the Länder are authorised to supervise the data protection law compliance of public bodies of the respective state (Land) and of all non-public bodies whose main establishment is situated in this Land and that are not subject to the exclusive jurisdiction of the BfDI. See also https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Datenschutz/Zust%C3%A4ndigkeit-BfDI.html.

116 Section 40 (2) 1 BDSG, Art. 4 No 16 GDPR.

117 Section 40 (1), (2) BDSG, Art. 4 No 16 GDPR, Section 25 (1) LDSG-BW. Other relevant special provisions which provide for a different competence are not identifiable here. The website of the LfDI Baden-Württemberg is available at https://www.baden-wuerttemberg.datenschutz.de/.

118 The DSK meets twice per year and takes a position on issues relevant to data protection, in particular through resolutions, decisions, guidance, standardisation, statements, press releases and specifications. The website of the DSK is available at https://www.datenschutzkonferenz-online.de/index.html.

119 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO, version dated February 2018, available at https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf (in German only).

120 DSK, Kurzpapier Nr. 1 – Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO, version dated 17 December 2018, available at https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf (in German only).

- a sample template for an RPA for controllers[121] and
- a sample template for an RPA for processors.[122]

(2) The LfDI Baden-Württemberg

As mentioned above,[123] the LfDI Baden-Württemberg is competent to supervise the data protection compliance of private bodies having their sole establishment or their central administration (main establishment) in Baden-Württemberg.

Regarding the RPA, the LfDI Baden-Württemberg refers to the DSK's guidance document "Information on the record of processing activities, Art. 30 GDPR" of February 2018[124] and in general to all DSK Short Papers including Short Paper No 1 on the RPA.[125]

In addition, the LfDI Baden-Württemberg has released:

- a sample template for an RPA named "Work guide RPA and deletion concept – table with examples applicant data" (Excel spreadsheet; hereinafter "Excel template of the LfDI Baden-Württemberg");[126] this template contains sample entries for the processing activity "application procedure" and further includes a documentation of the controller's deletion concept pursuant to its obligation to erase data under Art. 17 (1) GDPR, as well as
- yearly activity reports, some of which also contain a certain guidance with regard to the obligation to maintain a RPA, for example, the activity reports of 2018[127] and 2019,[128]

---

121 PDF file "Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher gem. Art. 30 Abs. 1 DSGVO", available at https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_verantwortliche.pdf or via the Website of the LfDI Baden-Württemberg, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/dsk_muster_vov_verantwortlicher.pdf, which alternatively provides for an RTF file at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/04/Muster_Verarbeitungsverzeichnis_Verantwortlicher.rtf.

122 PDF file "Übersicht von Verarbeitungstätigkeiten Auftragsverarbeiter gemäß Art. 30 Abs. 2 DSGVO", available at https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_auftragsverarbeiter.pdf or via the Website of the LfDI Baden-Württemberg, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/dsk_muster_vov_auftragsverarbeiter.pdf, which alternatively provides for an RTF file at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/04/Muster_Verarbeitungsverzeichnis_Auftragsverarbeiter.rtf.

123 Cf. A. III. 4.(Germany) a) cc).

124 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119).

125 DSK, Kurzpapier Nr. 1 – Verzeichnis von Verarbeitungstätigkeiten (fn. 120).

126 LfDI, sample template for a processing directory pursuant to Art. 30 GDPR with deletion concept pursuant to Art. 17 (1) GDPR (Excel spreadsheet) with sample entries for applicant data. The template is available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/11/211129_Arbeitshilfe_VV_und_Loeschkonzept_Tabelle-mit-Bsp-Bewerberdaten.xlsx.

127 34th activity report (Tätigkeitsbericht) of the LfDI Baden-Württemberg 2018, p. 11, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/LfDI-34.-Datenschutz-T%C3%A4tigkeitsbericht-Internet.pdf.

128 35th activity report (Tätigkeitsbericht) of the LfDI Baden-Württemberg 2019, p. 7, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/01/35.-T%C3%A4tigkeitsbericht-f%C3%BCr-den-Datenschutz-Web.pdf.

- a training video[129] on how to draft an RPA, which also shows a one-page RPA template for an association that can in a slightly adapted form also be used by small craft businesses.

dd) Selection of relevant national case law

There are some court decisions of mostly lower courts that mention or marginally deal with the obligations to maintain an RPA according to Art. 30 GDPR. In most of these cases, Art. 30 was not the focus of the decision and/or the decisions did not result in any relevant findings on the content and design of the RPA.[130] In one decision, the German Federal Labour Court (Bundesarbeitsgericht) dealt marginally with Art. 30 and confirmed that an RPA does not have to contain a list of all specific personal data actually processed.[131] In another decision, the Administrative Court of Wiesbaden[132] refused to apply the exemption in Art. 30 (5) GDPR.[133]

ee) Other sources

In Germany, inter alia, business associations such as the Bitkom e.V. and the German Association for Data Protection and Data Security (Gesellschaft für Datenschutz und Datensicherheit, GDD), the largest German data protection association, have published more detailed guidance for private companies with regard to the obligations under Art. 30 GDPR.

(1) The Bitkom e.V.

The Bitkom e.V., the business association of the German information and telecommunications industry, representing more than 2,600 companies in the digital economy, has published a guide on the RPA.[134] This guide includes examples for an RPA both for controllers and processors.

129 LfDI Baden-Wuerttemberg, training video "Europaweit geltende Regelungen praktisch umgesetzt, Folge 2: Verarbeitungsverzeichnis nach Art. 30 Abs. 1 DS-GVO", July 2020, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/07/Schulung-Verarbeitungsverzeichnis-2020-07.mp4.

130 Therefore, these decisions are not mentioned here.

131 Bundesarbeitsgericht, judgment of 16 December 2021, Court Ref. No 2 AZR 235/21, ECLI:DE:BAG:2021:161221.U.2AZR235.21.0, No 34, available at https://www.bundesarbeitsgericht.de/entscheidung/2-azr-235-21/.

132 Judgment of the Administrative Court of Wiesbaden of 17 January 2022, Court file No 6 K 1164/21.WI, No 109, available at https://openjur.de/u/2391922.html. This decision will be addressed below, cf. A. III. 4. c) aa).

133 This decision will also be addressed below, cf. A. III. 4. f).

134 Bitkom e.V., Das Verarbeitungsverzeichnis, Leitfaden, available at https://www.bitkom.org/Bitkom/Publikationen/Das-Verarbeitungsverzeichnis.html.

(2) The German Association for Data Protection and Data Security

The GDD has published practical assistance guides both for controllers[135] and processors[136] on how to draft and structure an RPA. These guides include[137], inter alia,

- explanatory notes and information on the structure of the respective RPA and the proposed front page and main sheets,
- a sample template[138] for an RPA for controllers, including a model for a front page, the main sheets and an explanatory note, and a proposal for a structure for an RPA for processors,[139] as well as
- a list of hyperlinks to templates for controllers published by other EU data protection authorities.

All above-mentioned templates of the German DPAs and the German business associations are non-binding recommendations.

b) The notion of a "processing activity"

There is no specific official definition of the notion of a "processing activity" in Germany. A description in accordance with Art. 30 GDPR must be prepared for each individual processing activity.[140] It is, however, unclear what a "processing activity" is and to what level of detail these "processing activities" must be described in the RPA.

According to the DSK,[141] a processing activity is generally understood to be a business process at an appropriate level of abstraction. A strict standard must be applied so that each new purpose of the processing constitutes a separate processing activity. Even in the case of only a minor change of purpose, it must be examined whether a pre-existing description

135 GDD-Praxishilfe DS-GVO (Va) Verzeichnis von Verarbeitungstätigkeiten – Verantwortlicher, Version 2.2, July 2022, available at https://www.gdd.de/downloads/praxishilfen/GDDPraxishilfeDSGVOVerzeichnisvonVerarbeitungsttigkeiten.pdf und https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ds-gvo-verzeichnis-von-verarbeitungstaetigkeiten/view.

136 GDD-Praxishilfe DS-GVO (Vb) Verzeichnis von Verarbeitungstätigkeiten – Auftragsverarbeiter, Version 1.0, January 2020, available at https://www.gdd.de/downloads/praxishilfen/GDDPraxishilfe_5bVVTAuftragsverarbeiter.pdf.

137 The detailed information contained in these guides will not be comprehensively addressed in this study.

138 This template is also available as a separate Word file at https://www.gdd.de/downloads/praxishilfen/ph-va-muster-zum-verzeichnis-fuer-verarbeitungstaetigkeiten-vvt.

139 https://www.gdd.de/downloads/praxishilfen/ph-vb-muster-zum-verzeichnis-von-verarbeitungstaetigkeiten-fuer-auftragsverarbeiter; a separate word file is available at https://www.gdd.de/downloads/praxishilfen/ph-vb-muster-zum-verzeichnis-von-verarbeitungstaetigkeiten-fuer-auftragsverarbeiter.

140 34th activity report (Tätigkeitsbericht) of the LfDI Baden-Württemberg 2018 (fn. 127), p. 11, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/LfDI-34.-Datenschutz-T%C3%A4tigkeitsbericht-Internet.pdf.

141 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 1.

of a processing activity must be adapted or whether a completely new description must be prepared.[142]

The LfDI Baden-Württemberg explains in its 34th activity report that a processing activity is generally understood to be a specific, independent business process and agrees that a strict standard must be applied. What specifically constitutes a processing activity depends on the individual company:[143]

Baden-Württemberg's data protection authority requires different granularity of RPA depending on the size of the company

- In a small company with only few employees, for example, the entire personnel administration (including application procedures and payroll) can be regarded as a single processing activity.
- In a medium-sized enterprise, there should be more subdivision; for example, into recruitment, hiring, management of current staff, termination of employment and similar processing activities.
- In a large company, there may be dozens or even hundreds of processing activities in the HR department alone; for example, if there are different application procedures for holiday jobbers, working students, apprentices, middle employees, managers and top managers, the respective information for every single one of these processing activities must be included in the RPA.

The LfDI Baden-Württemberg thus seems to link the volume of a single processing activity to the size of the company and probably to the scope of the processing carried out within such single processing activity as well. However, the GDPR does not link the term "processing activity" to the size of the company.[144] It seems that a "processing activity" can include more than one processing operation. However, neither the GDPR nor the guidance given by the German supervisory authorities provide a clear definition of a "processing activity".[145]

c) Information to be included in the RPA

In Germany, the following information must be included in the RPA:

142 In practice, the sum of the individual descriptions of the processing activities will often form the RPA, see below III. 4. c) aa) and DSK, Kurzpapier Nr. 1 – Verzeichnis von Verarbeitungstätigkeiten (fn. 120), p. 2.

143 34th activity report of the LfDI Baden-Württemberg 2018 (fn. 127), pp. 11 et seq.

144 Piltz, C., Was ist eine „Verarbeitungstätigkeit" im Sinne der DSGVO?, 18 March 2019, available at https://www.delegedata.de/2019/03/was-ist-eine-verarbeitungstaetigkeit-im-sinne-der-dsgvo/.

145 Piltz, C., ibid.

aa) Controllers

According to the DSK template and the guidance given by the DSK, the controllers' RPA must contain all the information listed exhaustively in Art. 30 (1) 2 lit. a–g GDPR, namely,

- the name and contact details of the controller (name, postal address, e-mail address, phone number (mandatory), internet address),
- the name and contact details of the joint controller,[146] if applicable (name, postal address, e-mail address, phone number (mandatory)),
- the name and contact details of the controller's representative,[147] if the controller is not established within the EU (name, postal address, e-mail address, phone number (mandatory)), and
- the name and contact details of the data protection officer, if the controller has designated one (salutation, title, name, first name, postal address, e-mail address, phone number (mandatory)).

The DSK's template contains a front page[148] with spaces in which this information can be filled in. If the controller is a legal person, information on managers ("Daten zu Leitungspersonen") is not necessarily required.[149] The LfDI Baden-Württemberg explains in its training video[150] that this information is required for postal, electronic and phone accessibility and rapid contact by the supervisory authority.

For each processing activity, the controller's RPA must contain the information further specified below, which must describe the controller's processing activities in a meaningful way. The sum of the individual descriptions of each processing activity and the general information on contact details will constitute the RPA.[151]

For this purpose, the template of the DSK includes further (main) sheets to be filled in. For each processing activity, a separate main sheet must be completed. If the controller uses the Excel sheet provided by the LfDI Baden-Württemberg, it must fill in the information requested

146 Within the meaning of Art. 26 GDPR.

147 This refers to the representative within the meaning of Art. 4 No 17 GDPR.

148 In German: "Vorblatt".

149 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 4 ("Bei (…) juristischen Personen sind nicht zwingend Daten zu Leitungspersonen gefordert").

150 See fn. 129.

151 DSK, Kurzpapier Nr. 1 – Verzeichnis von Verarbeitungstätigkeiten (fn. 120), p. 2; see also LfDI Baden-Württemberg, training video (fn. 129).

in the columns for each processing activity. Controllers who use the DSK template must insert the following information into the respective fields:

- the name of each relevant processing activity (this is not expressly provided for by the GDPR). The DSK recommends defining the name of each relevant processing activity based on the purpose of the processing (for example, "personnel file management"/"master data", "payroll accounting" etc.) and specifying it in the RPA.[152] The template provided by the DSK includes a sample main sheet. At the top of this main sheet, there is a field in which the name of the respective processing activity must be inserted; this main sheet should be completed for each processing activity,
- a serial number assigned by the controller for each processing activity (this is not expressly provided for by the GDPR),
- the date of introduction of the processing activity (not provided for by the GDPR),
- the date of last modification (not provided for by the GDPR). Presumably, this means the last modification of the processing activity (and not of the RPA sheet); however, this is not specified exactly,
- the responsible department with the controller and the name of the operationally responsible contact person, their e-mail address and phone number (this information is "desirable" from the point of view of the DSK and the LfDI Baden-Württemberg; therefore, an entry "should" be made under "contact person"),[153]
- the purposes of the processing must be documented "as concretely as possible, as abstractly as necessary", but unambiguously and transparently[154] and "sufficiently explicitly" to allow the supervisory authority to make a preliminary assessment of the adequacy of the safeguards and the lawfulness of the processing.[155] The controller is allowed to categorise the purposes of the processing in a certain way.[156]

  Examples:[157]

  - personnel file management/master data,
  - payroll accounting,
  - recording of working hours,

152 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 4.

153 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 4, LfDI Baden-Württemberg, training video (fn. 129).

154 LfDI Baden-Württemberg, training video (fn. 129).

155 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 5.

156 LfDI Baden-Württemberg, training video (fn. 129).

157 The examples stem from the DSK guidance document (fn. 119). The LfDI Baden-Württemberg names further examples in its training video (fn. 129).

- holiday file,
- IT/Internet/e-mail usage logging,
- application procedure,
- phone data collection,
- company car park management,
- video surveillance at workplaces, in schools etc.,
- procurement/purchasing and financial accounting,

- the name of the procedure used[158] (optional),
- a description of the categories of affected data subjects whose data are being processed (for example, employees, prospects, suppliers, customers, patients),
- a description of the categories of personal data, subdivided in sub-categories. In a judgment of 16 December 2021, the German Federal Labour Court (Bundesarbeitsgericht) dealt marginally with Art. 30 and confirmed that according to Art. 30 (1) 2 lit. c GDPR, an RPA does not have to contain a list of all personal data processed, but only a description of the corresponding categories.[159]

  Example (1): the category "employees" could be subdivided into the following data categories:[160]

  - employee master data ("Mitarbeiter-Stammdaten") with address data, date of birth, bank details, tax characteristics, wage group, working hours, previous areas of activity, qualifications etc.,
  - job applications with contact data, qualification data, activities etc.,
  - job references ("Arbeitszeugnisse") with address data, performance data, assessment data etc.,
  - warning letters with address data, work behaviour, performance data etc.,
  - company medical examinations with address data, health data etc.,
  - video surveillance at workplaces.

  Example (2): The category "customer data" could be subdivided into the following data categories:[161]

158 Here, the name of a specific procedure used should be inserted, e.g. the DIPSY procedure (Dialogisiertes Integriertes Personalverwaltungssystem) in the public administration.

159 Bundesarbeitsgericht, judgment of 16 December 2021 (fn. 131).

160 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 6; LfDI Baden-Württemberg, training video (fn. 129).

161 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 6.

- customer contact data with address data, contact persons etc.,
- customer group/interest,
- turnover data to date,
- creditworthiness data,
- payment data.

The DSK advises assigning sequential numbers to the individual categories of personal data so that they can be associated with other specific information in the DPA, for example, with specific deletion rules.[162]

- A separate description[163] of the special categories of personal data according to Art. 9 GDPR (data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs or trade-union membership as well as the processing of genetic data, biometric data for the unambiguous identification of a natural person, health data or data concerning a natural person's sex life or sexual orientation),
- a description of the categories of recipients to whom personal data have been (also in the past) or will be disclosed. In addition, the categories of persons who are or will be authorised to access the data must be indicated (the latter is not required by the GDPR but recommended by the DSK).[164] The information should be subdivided as follows:
  - Categories of internally authorised persons to access the data (no names, but the department and function or role must be indicated so that the respective persons are clearly identifiable) or other internal data recipients, for example, company doctor, staff council,[165]
  - Categories of external recipients (for example, banks, social security institutions, tax offices, creditors in the case of wage and salary garnishments, company pension providers, processors, parent company),
  - Categories of recipients in third countries or international organisations.

  The DSK states that it may be useful to specify the number of persons or bodies authorised to access the personal data.[166]
- Information on transfers of personal data to a third country or to an international organisation. A statement about "third countries" should always be made,[167] either
  - a statement that a transfer to third countries does not take place and is not planned or

162 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 5.

163 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 5.

164 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 6.

165 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 6.

166 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 6.

167 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 6.

- an explanation as to how data are being transferred.

The template[168] provided by the LfDI Baden-Württemberg contains fields requesting the controller to further include the name of the third country and the legal basis for such international data transfer. Furthermore,

- the third country and the concrete recipient(s) within the third country (not only the category of recipients) and/or the international organisation must be named[169], and
- in certain very specific cases of a data transfers,[170] the RPA must include a documentation of the safeguards the controller has provided for such transfers and of the controller's assessment of their appropriateness.[171]

- The deadlines for the deletion of the different categories of data, for example, the applicable retention periods under commercial and tax law for personnel data or customer data, legally stipulated deletion periods and review or deletion periods set by the controller (if applicable). Precise information is required; a general reference to legal retention periods is not sufficient.[172] The RPA template provided by the LfDI Baden-Württemberg[173] contains not only fields for specifying the deadlines for the deletion of data, but even integrates a complete deletion concept ("Löschkonzept"), which – in this broad form – is not required by Art. 33 GDPR but relates to the general principle of storage limitation in Art. 5 (1) lit. e) GDPR.
- A general, easily comprehensible description of the technical and organisational security measures implemented by the controller (this description is usually mandatory, despite the wording being "where possible").[174] The GDPR does not specify how detailed this description must be. According to the DSK, it should be specific enough to allow the competent DPA to make an initial legal check.[175] The description of each measure shall specifically refer to the category of data subjects or personal data, where the controller uses different measures to protect different categories.[176]

  The DSK guidance contains a long list of examples for possible security measures, including

  - pseudonymisation,
  - encryption; it is, however, not sufficient to simply state that the data are encrypted

168 LfDI Baden-Württemberg, sample template for an RPA pursuant to Art. 30 GDPR. It is unclear whether this information is mandatory or not (as it is not printed in bold type like the text in the other columns).

169 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 7.

170 These data transfers are referred to in Art. 49 (1) GDPR.

171 Art. 49 (6) GDPR.

172 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 7.

173 LfDI Baden-Württemberg, sample template for an RPA pursuant to Art. 30 GDPR with a deletion concept pursuant to Art. 17 (1) GDPR (Excel spreadsheet) with sample entries for applicant data.

174 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 8.

175 DSK, Kurzpapier Nr. 1 – Verzeichnis von Verarbeitungstätigkeiten (fn. 120), p. 2.

176 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 8.

end to end; for example, the encryption method used and the key length must also be specified,

- measures to ensure the integrity and confidentiality of systems and services (for example, development of a security policy, access control, security audits),
- measures to ensure the availability and resilience of systems and services (for example, backups),
- measures to restore the availability of data after a security incident (for example, the development of an emergency plan) and
- procedures for regular review of the effectiveness of the measures).[177]

The German DPAs further recommend describing/outlining in the RPA other recommendable measures, such as[178]

- measures to ensure the purpose limitation of personal data (for example, restriction of processing rights, closure of interfaces, prohibition of back-doors),
- measures to ensure transparency (for example, documentation of procedures, accesses and changes) and
- measures to ensure the information rights of data subjects (for example, consent, withdrawal and objection options, traceability of the controller's activities to ensure the rights of data subjects).

The DSK[179] and the LfDI Baden-Württemberg[180] recommend also using the RPA as a basis for the fulfilment of other obligations under data protection law and to include additional information in the RPA so that the latter serves as

- evidence for the compliance with their obligation to determine the purposes of the processing,
- evidence for the compliance with their obligation to be accountable and provide the necessary documentation (Art. 5 (2) and 24 GDPR) for example, to use the RPA as evidence for the lawfulness of the processing, for data minimisation and/or of the accuracy and up-to-dateness of the data,
- evidence for the compliance with their obligation to comply with the rights of the data subjects under Art. 12 (1) GDPR,

177 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), pp. 8–11.

178 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), pp. 11, 12.

179 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 2.

180 LfDI Baden-Württemberg, training video (fn. 129).

- evidence for the compliance with their obligation to apply suitable technical and organisational measures pursuant to Art. 24 (1) and Art. 32 GDPR,
- evidence for the compliance with their obligation to check whether a data protection impact assessment must be carried out (Art. 35 GDPR),
- evidence of their data protection and information security management system or
- a basis for the performance of the tasks of the data protection officer pursuant to Art. 39 GDPR.

Provided that the controller aims to use its RPA for such purposes as well, "it makes sense and is permissible" in the view of the DSK to also include additional information in the RPA, for example,[181]

- individual data fields,
- information on the origin or the source of the data,
- the legal basis for the processing,
- the employees responsible,
- the persons or groups of persons authorised to access the data.

It can thus be regarded as a recommendation by the DSK and the LfDI Baden-Württemberg to include also such additional information in the RPA, for example, the legal basis for the processing. In contrast, the Excel template of the LfDI Baden-Württemberg[182] contains two specific fields to include both the legal basis for the processing in general and the legal basis for the transfer of personal data to a third country (if relevant), without any indication that the stipulation of the legal basis is only optional or recommended.

Beyond this, the DSK recommends that the controller lists in the RPA – at the end of the documentation of the processing activity – any other documentation which, together with the RPA, serves to implement the controller's accountability obligation and to which the RPA refers. This may, for example, include references to the controller's documentation of internal rules of conduct, of a risk analysis, of its general data security description or of the results of a data protection impact assessment, or references to a comprehensive data security or

181 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 2.

182 LfDI Baden-Württemberg, sample template for a processing directory pursuant to Art. 30 GDPR with deletion concept pursuant to Art. 17 (1) GDPR (Excel spreadsheet) with sample entries for applicant data.

restart concept or a certificate.[183] The aim of this recommendation is to create a comprehensive documentation of the controller's data protection strategy.[184]

The above "recommendations" show that the German supervisory authorities regard the RPA as a central component of the controller's documentation and as the core of every data protection concept and thus go beyond the requirements of Art. 30 GDPR.[185] Therefore, the GDD[186] differentiates in its practical assistant guide for controllers[187] between the RPA "in the narrow sense" and the RPA "in the broader sense".

German Data Protection Authorities regard RPA as a central component of controller's documentation – beyond the requirements of Art. 30 GDPR.

bb) Processors

Each processor and, if applicable, its representative must maintain a record of all categories of processing activities carried out on behalf of a controller. This record shall form a register of orders ("Auftragskataster") with details of the principals (clients) and the subcontractors.[188] According to the DSK template and the guidance given by the DSK, the processors' RPA must contain all the information listed enumeratively in Art. 30 (2) lit. a–d GDPR, namely,[189]

- the name and contact details of the processor (name, postal address, e-mail address, phone number (mandatory), internet address),
- a checkbox to indicate whether the processor is in a group of companies ("Firmengruppe") (yes or no),
- the name and contact details of another joint processor, if applicable (name, postal address, e-mail address, phone number (mandatory)),
- the name and contact details of the processor's representative,[190] if the processor is not established within the EU (name, postal address, e-mail address, phone number (mandatory)), and
- the name and contact details of the data protection officer, if the controller has designated one (name, title, first name, postal address, e-mail address, phone number (mandatory)).

183 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 7. The DSK recommends including these references at the end of the documentation of the processing activity under "other information"; however, the DSK template does not contain a respective space.

184 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p 7.

185 See also GDD (fn. 135), Section 1.2.

186 See Section A. III. 4. a) above.

187 See fn. 135.

188 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 12.

189 Cf. DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), pp. 12 et seqq., which refers to the comments on the controller with regard to explanations and definitions.

190 This refers to the processor's representative within the meaning of Art. 4 No 17 GDPR.

The DSK's template contains a front page[191] in which this information can be filled in the respective spaces. If the processor is a legal person, information on managers ("Angaben zu Leitungspersonen") is not necessarily required.[192]

Beyond this, for every principal (client) on whose behalf the processor is acting, the processor must fill in the further (main) sheets contained in the DSK's template and include the information listed hereinafter. However, sub-contractors must only name their direct client (commissioner) and not the further chain of contractors behind them back to the controller.[193] The following information must be included:

- the name and contact details of the respective controller (the DSK template uses the wording principal (client – "Auftraggeber")) (name, postal address, e-mail address, phone number (mandatory)),
- according to the DSK's guidance, the processor must also include in the RPA the contact data of the representative[194] of each controller on whose behalf it is acting; however, the template does not contain a respective field in which this information could be given,
- the serial number[195] of the controller/principal (client) (not provided for by the GDPR),
- a description of the categories of processing carried out on behalf of the respective principal (client); this description must include an explanation of the respective processing.[196] The register of orders ("Auftragskataster") must be differentiated according to the individual orders.[197] The DSK's template contains a field which includes checkboxes for some categories of processing:
  - (paper) document destruction ("Aktenvernichtung"),
  - archiving (of data files),
  - office communication,
  - cloud services,
  - financial accounting,
  - hosting of an e-mail system,
  - hosting of an internet system,

191 In German: „Vorblatt".

192 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 12 and p. 4., referring to its explanations for controllers.

193 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 12.

194 This refers to the processor's representative within the meaning of Art. 4 No 17 GDPR.

195 "Lfd. Nr." – laufende Nummer – meaning that the processor must number them.

196 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 13.

197 DSK, ibid., "Das Auftragskataster ist nach den einzelnen Aufträgen zu differenzieren").

- hosting of processing,
- payroll accounting,
- personnel management,
- advertising/letter shop,
- time recording,
- travel expenses,
- other.

The DSK guidance lists further examples, which are not listed in the DSK's template:

- e-mail database,
- transfer of the company/office phone system,
- advertising address processing,
- scanning of company/office documents,
- support/maintenance service,
- computer service with support and data backup, whose purpose and processing operations the client alone determines,
- deletion and disposal of data media,
- learning platform,
- data processing in an external computer centre,

- information on transfers of personal data to a third country or to an international organisation. A statement about "third countries" should always be made,[198] either
  - a statement that a transfer to third countries does not take place and is not planned or
  - an explanation as to how data are being transferred,

  furthermore,
  - the third country and the concrete recipient(s) within the third country and/or the international organisation must be named[199] and
  - in certain very specific cases of a data transfers,[200] the RPA must include a documentation of the safeguards the processor has provided for such transfers and of the processor's assessment of their appropriateness,[201]

198 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), pp. 13, 6.

199 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), pp. 13, 7.

200 These data transfers are referred to in Art. 49 (1) GDPR.

201 Art. 49 (6) GDPR.

- the name of their subcontractor as well as
- a general, easily comprehensible description of the technical and organisational security measures implemented by the processor (this description is usually mandatory, despite the wording being "where possible").[202] The description of each measure shall specifically refer to the category of data subjects or personal data, where the processor uses different measures to protect different categories.[203]

cc) Guidance on the possible reduction of the effort involved in the creation of the RPA

According to the DSK,[204] in order to avoid redundancies and to reduce the effort for creating and maintaining the directory, references to existing documents can be included in the descriptions of the processing activities, especially those that were created within the framework of information security management, without having to re-insert the detailed information in the RPA. For example, a reference to a company-wide or authority-wide information security framework concept can be made. Only relevant additional or deviating technical and organisational measures for specific procedures must then be mentioned separately in the RPA.

d) Design of the RPA

aa) Format

According to the DSK[205] and the LfDI Baden-Württemberg, the RPA must be maintained in writing. This can be done on paper or in an electronic format. Controllers may (but are not required to) use the template provided on the LfDI website. Both a loose-leaf compilation and a tabular list of processing activities are possible.[206] The DSK template contains a front page and main sheets for the single processing activities. The GDD guidance[207] proposes using two front pages (one for information on the controller and a second front page with information on overlapping regulations and facts) so that repetitive information is only documented once, in order to facilitate the maintenance effort.

202 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 8.

203 For further details and examples of possible security measures, the above apply respectively, cf. DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 14.

204 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), pp. 1 et seq.

205 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 3.

206 34th activity report (Tätigkeitsbericht) of the LfDI Baden-Württemberg 2018 (fn. 127), p. 12.

207 See GDD guidance (fn. 135), Section 5.

bb) Language

The RPA must regularly be maintained in German. At the very least, the company must be able to submit without delay a German translation of its RPA upon request by the DPA (Section 23 (1) and (2) of the German Administrative Procedure Act (VwVfG)).[208]

e) Actualisation/Update of the RPA

So as to be able to track changes to the entries in the RPA (for example, the identity of the controller, processor or data protection officer at a given point in time), any changes to the RPA should be documented with a storage period of one year. This can also be derived from the principle of accountability in Art. 5 (2) GDPR.[209]

f) Exemption from the duty to maintain an RPA (Art. 30 (5))

In the view of the German supervisory authorities, the exemption for SMEs in Art. 30 (5) GDPR will only rarely apply, meaning that in most cases it will be necessary to prepare an RPA. The LfDI Baden-Württemberg recognises that the creation of an RPA is often challenging for SMEs. In its view, the exemption from the duty to maintain an RPA in Art. 30 (5) is in practice almost never relevant for SMEs.[210] The counter-exemptions are so far-reaching that hardly any company benefits from this exemption.[211] When employing slightly fewer than 250 employees, the processing of personal data on an occasional basis is hardly possible: every company with employees inevitably processes at least their data to carry out the employment relationship, including health data (in the context of absence management) or religious affiliation (in the context of tax administration). Personnel management alone already constitutes regular processing – even for the smallest companies.[212] This applies in particular to payroll accounting, except for companies that have outsourced these activities completely to a tax advisor and possibly for smaller associations.[213] The processing of customer data is also likely to be a regular occurrence even in the smallest companies.[214] In the view of the LfDI Baden-Württemberg, the originally envisaged risk-based approach does not work here. The LfDI Baden-Württemberg therefore proposes restricting the counter-exception of Art. 30 (5) GDPR, focussing on

208 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 3, referring to Working Paper (WP) 243 of the Art. 29 Group (Guidelines on the data protection officer under the GDPR), para. 2.3, on the linguistic accessibility of the data protection officer.

209 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 3.

210 35th activity report (Tätigkeitsbericht) of the LfDI Baden-Württemberg 2019 (fn. 128), p. 131, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/01/35.-T%C3%A4tigkeitsbericht-f%C3%BCr-den-Datenschutz-Web.pdf.

211 Cf. also DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), pp. 3 et seq.

212 35th activity report (Tätigkeitsbericht) of the LfDI Baden-Württemberg 2019 (fn. 128), p. 131, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/01/35.-T%C3%A4tigkeitsbericht-f%C3%BCr-den-Datenschutz-Web.pdf.

213 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), pp. 3 et seq.

214 34th activity report (Tätigkeitsbericht) of the LfDI Baden-Württemberg 2018 (fn. 127), p. 11, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/LfDI-34.-Datenschutz-T%C3%A4tigkeitsbericht-Internet.pdf.

companies whose core activity is data processing and applying lower requirements to other data controllers, for example, in business relationships.

Likewise, the examples provided in the DSK guidance[215] demonstrate the narrow interpretation of the exemption clause. According to the DSK, companies with fewer than 250 employees must maintain an RPA if the controller or processor

- carries out video surveillance or credit scoring or fraud prevention procedures, tracking of employees (for example, by GPS) or processing operations which involve the content of communications (as such, processing is likely to result in a risk to the rights and freedoms of data subjects),
- processes data on religious affiliation, health data or biometric data for unique identification (as these are special categories of data) or
- conducts non-occasional processing, which is essentially "any other data processing", for example, payroll, customer data management or IT/internet/e-mail logging.

According to the DSK,[216] a processing is "not only occasional" if the processing occurs either

- continuously or at certain intervals during a certain period or
- recurrently or repeatedly at certain points in time or
- constantly or regularly.

In a judgment[217] of 17 January 2022, the Administrative Court of Wiesbaden did not consider the exemption in Art. 30 (5) to be applicable. The plaintiff, a company in the logistics sector with 76 employees, had installed GPS systems in several vehicles of its company fleet. It used a software which enabled a secret GPS tracking of vehicles and thus of its employees. The court reasoned that although the plaintiff had fewer than 250 employees, the covert collection of data obviously posed a risk to the rights of the employees (Section 26 BDSG, Art. 6 and 13 GDPR) and the processing was not merely occasional.

215 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), pp. 3, 4.

216 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 4.

217 Judgment of the Administrative Court of Wiesbaden of 17 January 2022, Court file No 6 K 1164/21.WI, No 109, available at https://openjur.de/u/2391922.html.

g) Making available of the RPA to the supervisory authority

Every controller and processor must cooperate with the DPA and submit the relevant RPA to this authority upon request, so that the DPA may use the RPA as a basis to examine the individual processing operations or procedures.[218] If the DPA restricts its investigations to certain processing activities, the controller must provide only the relevant sections of the RPA.[219] In Germany, the former right for the general public to inspect the RPA no longer applies.[220]

Where the RPA refers to existing policies explained in other documents (for example, the company's security framework concept), these should also be provided to the DPA upon request.[221] However, in the view of the DSK, it makes sense to voluntarily provide at least the additional documents essential for the understanding and evaluation of the RPA already together with the RPA.[222]

In Germany, the competent DPA may independently determine the format of the submission (in writing in paper form or electronically in text form). The DPA may thus also require the printout of an RPA maintained in electronic form (Section 3a VwVfG). However, the RPA may only request what is proportionate and necessary for the respective supervisory purposes pursued (for example, only the necessary part of the RPA must be printed out).[223]

Failure to maintain an RPA, to maintain a complete RPA or to provide the RPA to the DPA upon request of the latter is punishable by fines up to the amount mentioned in Art. 83 (4) lit. a GDPR.[224]

5. Italy

a) Relevant national legal and other sources

aa) Primary legislation

Data protection in Italy is primarily governed by the GDPR as directly applicable EU law. There is, however, still a national data protection law in Italy. In fact, the rules on the processing and free movement of personal data published in the Gazzetta Ufficiale of 4 September 2018

218 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 2.

219 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 2.

220 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 3.

221 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), pp. 1 et seq.

222 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 7.

223 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 3.

224 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten (fn. 119), p. 7.

came into force on 19 September 2018. With Legislative Decree No 101 of 2018[225] issued by Parliament, the GDPR was thus also implemented by Italy.

Legislative Decree No 196 of 2003,[226] in other words, the "old" Italian Personal Data Protection Code, has not been fully repealed, but the legislator harmonised its content with the GDPR, providing for a partial repeal.[227] There are no further national laws supplementing or concretising the content of Art. 30 GDPR.

bb) Secondary legislation

There is no secondary legislation on the implementation or enforcement of Art. 30 GDPR in Italy.

cc) Guidance from Italian public authorities

In Italy, the authority that oversees the implementation of the GDPR and provides guidance on its correct application is the Italian data protection authority[228] ("Garante per la protezione dei dati personali"), commonly referred to as the Garante della Privacy (hereinafter "Garante").[229]

The Garante is an independent administrative authority established by the so-called privacy law (Law No 675 of 31 December 1996[230]) and regulated subsequently by the Personal Data Protection Code ("Codice in materia di protezione dei dati personali")[231] which also establishes that the Garante is the supervisory authority responsible for monitoring the application of

225 Legislative Decree No 101 of 10 August 2018, Gazzetta Ufficiale Serie Generale No 205 of 4 September 2018, available at https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg.

226 Legislative Decree No 196 of 30 June 2003, Gazzetta Ufficiale No 174 of 29 July 2003 – Suppl. Ordinario n. 123, available at https://www.gazzettaufficiale.it/eli/gu/2003/07/29/174/so/123/sg/pdf.

227 An English translation of the recent version of the Italian Personal Data Protection Code is available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9740796.

228 All information about the organisation, activities and goals of the authority can be found, also in English, on the official site at https://www.garanteprivacy.it/web/garante-privacy-en/home_en.

229 See Section 2-a of the Italian Personal Data Protection Code (fn. 227).

230 Law No 675 of 31 December 1996 – Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, available at https://www.garanteprivacy.it/home/docweb/-/docweb-di-splay/docweb/28335#:~:text=La%20presente%20legge%20garantisce%20che,giuridiche%20e%20di%20ogni%20altro.

231 Legislative Decree No 196 of 30 June 2003 as amended by Legislative Decree No 101 of 10 August 2018.

the GDPR[232] (pursuant to Art. 51 GDPR[233]) which includes the monitoring of the obligations under Art. 30 GDPR.

The Garante's duties are defined by the GDPR and the Italian Personal Data Protection Code. Its main competences are to check that the processing of personal data is carried out in compliance with the law, to receive and examine appeals, complaints and reports on the matter, to prohibit unlawful or improper processing and, if necessary, order its blocking.

The Garante has issued the following documents on Art. 30 GDPR:

Authority in Italy issues guidance and templates; main representative business organisation provides templates for affiliates

- an official guidance document on how to draft an RPA named "Guida all'applicazione del Regolamento UE in materia di Protezione dei Dati Personali"[234],
- a series of FAQ[235] on the RPA and
- two templates for the drafting of a "simplified" RPA for SMEs, one for controllers[236] and one for processors.[237]

dd) Selection of relevant national case law

So far, there have been no rulings in Italian jurisprudence dealing with the RPA.

ee) Other sources

In Italy, the business association "Confindustria"[238], short for Confederazione Generale dell'Industria Italiana (General Confederation of the Italian Industry), has issued an RPA template, which is unfortunately only accessible for Confindustria's affiliates.[239] Confindustria is the main

232 Art. 31 (1) L. 675/1996: 1. The Supervisor is (inter alia) responsible for: (a) establishing and maintaining a general record of processing activities on the basis of notifications received; (b) checking whether processing operations are carried out in accordance with the law and the regulation and in compliance with the notification; (c) notifying the relevant controllers or processors of any changes that are necessary or appropriate in order to bring processing into conformity with the provisions in force.

233 Art. 51 (1) GDPR: Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ("supervisory authority").

234 Guida all'applicazione del Regolamento UE in materia di Protezione dei Dati Personali, available at https://www.privacyitalia.eu/wp-content/uploads/2018/03/Guida-al-Gdpr-2018.pdf.

235 FAQ sul registro delle attività di trattamento, available at https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento.

236 Scheda Registro dei Trattamenti per titolare (contitolare/rappresentante del titolare), available at https://www.garanteprivacy.it/documents/10160/0/Modello+di+%E2%80%9Cregistro+semplificato%E2%80%9D+delle+attivit%C3%A0+di+trattamento+del+titolare+per+PMI.pdf/ca77f44e-0f85-4b01-6135-f3a7fc5182ec?version=1.2.

237 Scheda Registro dei Trattamenti del responsabile/sub-responsabile, available at https://www.garanteprivacy.it/documents/10160/0/Modello+di+%E2%80%9Cregistro+semplificato%E2%80%9D+delle+attivit%C3%A0+di+trattamento+del+responsabile+per+PMI.pdf/5a4dfd05-6c79-ff2f-f48f-14e5a3a87817?version=1.1.

238 https://www.confindustria.it/home.

239 See https://www.confindustria.sa.it/privacy-modello-di-registro-delle-attivita-di-trattamento-e-glossario/.

representative organisation of Italian manufacturing and service companies, grouping together on a voluntary basis more than 150,000 companies, including banks and public companies with a total of 5,439,370 employees.

Beyond this, on the website of the Unione Industriale di Verbania-Cuneo-Ossola, the local section of Confindustria, there is a link to a publicly accessible template[240] for the information to be included in the RPA, joined by an RPA glossary.[241]

b) The notion of a "processing activity"

Neither Italian law nor the Garante provide for a specific notion of processing activities.

c) Information to be included in the RPA

According to the Garante's templates, guidance document and FAQ,[242] in Italy, the following information must be included in the RPA:

aa) Controllers

- the names and contact details – not specified more precisely – of the data controller, the joint data controller, the data controller's representative and the data protection officer,
- the "purpose of the processing", including a precise indication of the purposes of the processing, categorised by types of processing (for example, processing of employee data for the management of the employment relationship; processing of supplier contact data for the management of orders),
- a "description of the categories of data subjects and categories of personal data"; here, both the types of data subjects (for example, customers, suppliers, employees) and the types of personal data subject to processing (for example, personal data, health data, biometric data, genetic data etc.) should be specified,

240 The template is available at http://www.uivco.vb.it/web/binary/saveas?filename_field=datas_fname&field=datas&model=ir.attachment&id=4087.

241 GDPR – Modello registro attività di trattamento – Confindustria – Versione aggiornata.xlsx, available at http://www.uivco.vb.it/blog/lavoro-e-previdenza-6/post/privacy-modello-di-registro-delle-attivita-di-trattamento-e-glossario-146.

242 FAQ sul registro delle attività di trattamento, available at https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento (see fn. 235).

- the "categories of recipients to whom the data have been or will be disclosed"; here, the other controllers to whom the data are disclosed should be listed (for example, social security institutions to whom the data of employees must be disclosed in order to fulfil their contribution obligations); in addition, the Garante advises that other entities to which – in their capacity as processors and sub-processors – the controller transmits the data (for example, an external entity entrusted by the controller with the processing of employees' payroll data or other external entities entrusted with all or part of the processing activities) should also be indicated to allow the controller to know the range and type of external entities entrusted with the processing of personal data,
- any "transfers of personal data to a third country or international organisation"; here, information on such transfers must be included, together with an indication of the third country or countries to which the data are transferred and the "safeguards" adopted pursuant to Chapter V of the GDPR (for example, adequacy decisions, binding corporate rules, standard contractual clauses etc.),
- the "time limits" for the deletion of the different categories of data, which must be identified by type and purpose of processing (for example, in the case of a contractual relationship, the data will be kept for 10 years from the last recording pursuant to Art. 2220 of the Italian Civil Code[243]); where it is not possible to establish a maximum time limit in advance, retention periods may be specified by reference to criteria such as legal provisions or sectorial practices; for example, in case of litigation, the data will be deleted at the end of the litigation,
- a "general description of the security measures"; here, the controller must indicate the technical and organisational measures adopted pursuant to Art. 32 GDPR, bearing in mind that this list is open and non-exhaustive and that it is up to the controller to make, on a case-by-case basis, the final assessment of what level of security is appropriate to the risks presented by the processing activities implemented. The security measures may be described in summary and abbreviated form if this description provides a general and overall picture of those measures in relation to the processing activities carried out.

The FAQ also specify that any other information which the controller or the person in charge deems useful may be recorded in the RPA (for example, the methods for collecting consent, any impact assessments carried out, the indication of any "internal contact persons" identified by the data controller for certain types of processing etc.).

---

243 Art. 2220 Civil Code (Retention of Accounting Records) reads: "The records must be kept for ten years from the date of the last entry. For the same period, invoices, letters and telegrams received and copies of invoices, letters and telegrams received, and copies of invoices, letters and telegrams sent. The records and documents referred to in this article may be preserved in the form of recordings on image media, provided that the recordings correspond to the documents and can at any time be made readable by means made available by the person using such media", available at https://www.brocardi.it/codice-civile/libro-quinto/titolo-ii/capo-iii/sezione-iii/art2220.html.

The RPA must contain the date of its first establishment or the date of the first creation of each individual file for the different processing activities, together with the date of its last update. For example, in case of an update, the RPA must contain an annotation, such as:

- "- file created on [date]"
- "- last updated on [date]".

bb) Processors

Processors must keep a register of "all categories of processing activities carried out on behalf of a controller" (Art. 30 (2) GDPR). The processors' RPA must include the following information:

- the name and contact details of the processor or processors and of each controller on whose behalf the processor is acting; no further information is recommended, and
- a "description of the categories of processing activities carried out" (Art. 30 (2) (b) GDPR); insofar, the processor and/or sub-processor may use the information contained in the contract with the controller pursuant to Art. 28 GDPR; this contract must identify, in particular, the nature and purpose of the processing, the type of personal data and the categories of data subjects concerned by the processing, as well as the duration of the processing.

If one and the same processor (for example, a software house company) acts on behalf of several clients who are autonomous controllers, the information referred to in Art. 30 (2) GDPR must be reported in the RPA with reference to each controller. In such cases, the processor must divide the RPA into as many sections as there are controllers on whose behalf it is acting.

The processors' RPA must contain the date of its first establishment or the date of the first creation of each individual file by type of processing, together with the date of its last update. For example, in case of an update, the record must contain an annotation such as:

- "- record created on [date]"
- "- last updated on [date]".

cc) Guidance on the possible reduction of the effort involved in the creation of the RPA

The Garante states that companies and organisations with fewer than 250 employees, provided they are obliged to maintain an RPA, benefit from simplifications: they are only required to draw up the RPA for the specific processing activities that trigger the obligation to create and maintain an RPA and for other processing activities. For example, where the processing of special categories of data only relates to a single employee, the register may be prepared

and maintained solely with reference to that limited type of processing. This corresponds with the guidance given by the EDPB.[244]

dd) Additional information

Beyond a description of the requirements of Art. 30 GDPR, the Garante's guidance on how to draft an RPA[245] encompasses a recommendation for the preparation of the RPA, which states: "The keeping of a record of processing activities is not a formality but an integral part of a system of proper management of personal data. For this reason, all data controllers and data processors, regardless of the size of their organisation, are invited to take the necessary steps to equip themselves with such a register and, in any case, to carry out an accurate reconnaissance of the processing activities carried out and their respective characteristics. The contents of the register are set out, as mentioned, in Art. 30; however, nothing prevents an owner or manager from including further information if it is deemed appropriate with a view to the overall assessment of the impact of the processing operations carried out."[246]

d) Design of the RPA

aa) Format

The record must be in written form, either on paper or electronically, and must be submitted on request to the Italian DPA.[247]

bb) Language

The Garante's FAQ do not mention in which language the RPA must be compiled or maintained. However, since Italian is the official language of Italy as provided for by constitutional law[248] and ordinary law[249], it can be assumed that Italian organisations must draw up the RPA in Italian (even if they are part of an international group and there is no organisational constraint to use a common vehicular language).

e) Actualisation/Update of the RPA

The Garante's FAQ[250] prescribe that the record must be constantly updated since its content must always correspond with the actual processing operations carried out. Any change, in

---

244 See Section A. III. 1. g) above, referring to the endorsed Art. 29 Working Party Position Paper of 19 April 2018 (fn. 33), p. 2.

245 See fn. 234.

246 See Guida all'applicazione del Regolamento UE 2016/679, pp. 26–27.

247 FAQ No 1 of the Garante, available at https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento.

248 Art. 99, Presidential Decree No 670 of 31 August 1972, "Statute of Autonomy of the Autonomous Region of Trentino-Alto Adige".

249 Art. 1 Law No 482 of 15 December 1999.

250 FAQ No 5 of the Garante, available at https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento.

particular with regard to modalities, purposes, categories of data, categories of data subjects, must be immediately entered in the RPA so that the changes can be followed. As mentioned, the date of an update must be included in the RPA. For example, the RPA must contain an annotation such as:

- "- record created on [date]"
- "- last updated on [date]".

f) Exemption from the duty to maintain an RPA (Art. 30 (5) GDPR)

The Italian DPA does not provide specific guidance on the types of entities exempt from the obligation to maintain a record of processing activities. In the FAQ[251], however, the Garante clarifies that "the category of 'organisations' referred to in Art. 30 (5) GDPR also includes associations, foundations and committees". In the light of Art. 30 (5) GDPR, for example, the following organisations are obliged to maintain an RPA:

- commercial establishments, public establishments or artisans with at least one employee (bars, restaurants, workshops, shops, small retailers etc.) and/or which process customers' health data (for example, hairdressers, beauticians, opticians, dental technicians, tattoo artists etc.),
- self-employed professionals with at least one employee and/or who process health data and/or data relating to criminal convictions or offences (for example, accountants, notaries, lawyers, osteopaths, physiotherapists, pharmacists, doctors in general) and
- associations, foundations and committees which process "special categories of data" and/or data relating to criminal convictions or offences (namely, trend organisations; associations for the protection of so-called vulnerable persons, such as sick or disabled persons, exprisoners etc.; associations pursuing the purpose of preventing and combating gender, racial, sexual orientation, political or religious discrimination etc.; sports associations with reference to health data processed; political parties and movements; trade unions, religious associations and movements).

g) Making available of the RPA to the supervisory authority

The record must be in written form, including in electronic form, and must be submitted on request to the Italian DPA.[252]

251 FAQ No 2 of the Garante, available at https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento.

252 FAQ No 1 of the Garante, available at https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento.

6. Comparative analysis

In the following, a summary and comparison of some of the most relevant national provisions and administrative requirements regarding the obligation to maintain an RPA are provided. The chapter is based on the official templates and guidance given by national DPAs. Among the Member States researched, only Germany has a federal system of data protection supervision. It consists of the data protection supervisory authorities of the Federation (the "Bund") and the 16 federal states (the "Länder"). As far as the data protection supervisory authorities of the federal states are the competent authority, the following tables are based on the templates and guidance provided by the LfDI Baden-Württemberg.

a) National legislation and guidance

Table 1 provides an overview of the national legislation and the official guidance given by the national DPAs.

Table 1: National legislation and guidance by national DPAs

	Austria	France	Germany/BW	Italy
National legislation	Data Protection Act	Act on data processing, data files and individual liberties	Federal Data Protection Act and State Data Protection Act of Baden-Württemberg	Legislative Decree No 101 of 2018 and Legislative Decree No 196 of 2003
Does the above-mentioned national legislation contain specific provisions which concretise, supplement or derogate from the duties under Art. 30 GDPR?	No specific provision	Specific provision, but no derogation (refers to Art. 30 GDPR)	No specific provision applicable to private companies	No specific provision
Official guidance by national DPAs	■ Guideline on Regulation (EU) 2016/679, https://www.dsb.gv.at/dam/jcr:5fc3b77f-d546-4609-aca0-e34035979549/DSGVO_Leitfaden_2022.pdf	■ CNIL guidelines on RPAs, https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement ■ Processor's Guidelines: https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf ■ CNIL's template, https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement	■ Information on the record of processing activities, Art. 30 GDPR, https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf ■ Short Paper No 1 of 17 December 2018 on the record of processing activities – Art. 30 GDPR, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf ■ RPA template for controllers, https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_verantwortliche.pdf ■ RPA template for processors, https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_auftragsverarbeiter.pdf ■ RPA template Baden-Württemberg, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/11/211129_Arbeitshilfe_VV_und_Loeschkonzept_Tabelle-mit-Bsp-Bewerberdaten.xlsx ■ Training video Baden-Württemberg,https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/07/Schulung-Verarbeitungsverzeichnis-2020-07.mp4	■ Guida all'applicazione del Regolamento UE in materia di Protezione dei Dati Personali, https://www.privacyitalia.eu/wp-content/uploads/2018/03/Guida-al-Gdpr-2018.pdf ■ FAQ on the RPA, https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento ■ Template for a simplified RPA for SMEs for controllers, https://www.garanteprivacy.it/documents/10160/0/Modello+di+%E2%80%9Cregistro+semplificato%E2%80%9D+delle+attivit%C3%A0+di+trattamento+del+titolare+per+PMI.pdf/ca77f44e-0f85-4b01-6135-f3a7fc5182ec?version=1.2 ■ Template for a simplified RPA for SMEs for processors, https://www.garanteprivacy.it/documents/10160/0/Modello+di+%E2%80%9Cregistro+semplificato%E2%80%9D+delle+attivit%C3%A0+di+trattamento+del+responsabile+per+PMI.pdf/5a4dfd05-6c79-ff2f-f48f-14e5a3a87817?version=1.1

Table 2 provides examples of non-official guidance documents.

Table 2: Non-official guidance documents

	Austria	France	Germany	Italy
Non-official guidance documents	■ WKO: RPA template for controllers, https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-Verantwortlicher.docx ■ WKO: RPA template for processors, https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-Auftragsverarbeite.docx	■ Bpifrance and CNIL: Practical guideline to GDPR awareness for small and medium-sized businesses, https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf ■ Medinsoft: GDPR white book, https://medinsoft.com/wp-content/uploads/2019/05/LivreBlanc_LegalInTech.pdf	■ Bitkom: Das Verarbeitungsverzeichnis, Leitfaden (for controllers and processors), https://www.bitkom.org/Bitkom/Publikationen/Das-Verarbeitungsverzeichnis.html ■ Gesellschaft für Datenschutz und Datensicherheit: i.a. RPA template for controllers, https://www.gdd.de/downloads/praxishilfen/ph-va-muster-zum-verzeichnis-fuer-verarbeitungstaetigkeiten-vvt; and proposal for a structure for an RPA for processors,https://www.gdd.de/downloads/praxishilfen/ph-vb-muster-zum-verzeichnis-von-verarbeitungstaetigkeiten-fuer-auftragsverarbeiter	■ Confindustria: RPA template, https://www.confindustria.sa.it/privacy-modello-di-registro-delle-attivita-di-trattamento-e-glossario/ (access only for members) ■ Unione Industriale di Verbania-Cuneo-Ossola: RPA template, http://www.uivco.vb.it/web/binary/saveas?filename_field=datas_fname&field=datas&model=ir.attachment&id=4087 ■ Unione Industriale di Verbania-Cuneo-Ossola: RPA glossary, http://www.uivco.vb.it/blog/lavoro-e-previdenza-6/post/privacy-modello-di-registro-delle-attivita-di-trattamen-to-e-glossario-146

b) The notion of a "processing activity"

Table 3 provides an overview of how the notion of a "processing activity", which is not defined in the GDPR, is understood in the Member States researched. The understanding of the notion of a "processing activity" is important for determining the necessary level of detail of the RPA.

Table 3: Notions of a "processing activity"

	Austria	France	Germany/BW	Italy
Notion of a processing activity	Not defined	The main activities of the company, such as recruitment, payroll management, or training	Business process at an appropriate level of abstraction. Each new purpose of the processing constitutes a separate processing activity. Dependence on the size of a company, e.g. the entire personnel administration might be a single processing activity or a differentiation between recruitment, management of current staff and terminations of employment might be required	Not defined

c) Information to be included in the RPA of controllers

Table 4 provides an overview of the information that must be included in the RPA according to Art. 30 (1) lit. a GDPR, namely, information on the controller, joint controller, controller's representative and data protection officer.

Table 4: Specification of information to be included in the RPA according to Art. 30 (1) lit. a GDPR

Category of information required	Austria	France	Germany/BW	Italy
Name and contact details of the controller	Required, but not further specified	Name, postal address, e-mail address, ZIP code, city, phone number	Name, postal address, e-mail address, phone number, internet address (voluntary)	Required, but not further specified
Where applicable, name and contact details of the joint controller	Required, but not further specified	Name, postal address, e-mail address, ZIP code, city, country, phone number	Name, postal address, e-mail address, phone number	Required, but not further specified
Where applicable, name and contact details of the controller's representative	Required, but not further specified	Name, postal address, e-mail address, ZIP code, city, phone number	Name, postal address, e-mail address, phone number	Required, but not further specified
Where applicable, name and contact details of the data protection officer	Required, but not further specified	Name, postal address, e-mail address, ZIP code, city, country, phone number, company details if an external data protection officer is concerned	Salutation, title, name, first name, postal address, e-mail address, phone number	Required, but not further specified

Table 5 provides an overview of the information that must be included in the RPA according to Art. 30 (1) lit. b GDPR, namely, information on the purposes of the processing.

Table 5: Specification of information to be included in the RPA according to Art. 30 (1) lit. b GDPR

Category of information required	Austria	France	Germany/BW	Italy
Purposes of the processing	Required, but not further specified	It is possible to indicate sub-purposes relating to a main purpose	The purposes of the processing must be documented "as concretely as possible, as abstractly as necessary", but unambiguously and transparently and "sufficiently explicitly" to allow the supervisory authority to make a preliminary assessment of the adequacy of the safeguards and the lawfulness of the processing; the controller may categorise the purposes of the processing in a certain way	Precise indication of the purposes of the processing, categorised by types of processing, e.g.: ■ Processing of employee data for the management of the employment relationship ■ Processing of supplier contact data for the management of orders

Table 6 provides an overview of the information that must be included in the RPA according to Art. 30 (1) lit. c GDPR, namely, a description of the categories of affected data subjects and of the categories of personal data.

Table 6: Specification of information to be included in the RPA according to Art. 30 (1) lit. c GDPR

Category of information required	Austria	France	Germany/BW	Italy
Description of the categories of data subjects	Required, but not further specified	Customers, prospects, employees, internal services, providers, candidates	E.g. employees, prospects, suppliers, customers, patients	E.g. customers, suppliers, employees
Description of the categories of personal data	Required, but not further specified	■ E.g. identity, family, economic or financial situation, banking data, connection data, location data, social security identification number ■ Description of the eventual sensitive data	■ Description of the categories of personal data subdivided in sub-categories, such as subdividing customer data into the following categories: ▸ Customer contact data with address data, contact persons etc. ▸ Customer group/ interest ▸ Turnover data to date ▸ Creditworthiness data ▸ Payment data ■ Sequential numbers assigned to the individual categories of personal data (DSK advisory) ■ Separate description of the special categories of personal data according to Art. 9 GDPR	E.g. personal data, health data, biometric data, genetic data

Table 7 provides an overview of the information that must be included in the RPA according to Art. 30 (1) lit. d GDPR, namely, information on the categories of recipients to whom the data have been or will be disclosed.

Table 7: Specification of information to be included in the RPA according to Art. 30 (1) lit. d GDPR

Category of information required	Austria	France	Germany/BW	Italy
Categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations	Required, but not further specified	To be chosen from one of the following categories: ■ Processors ■ Internal services processing personal data ■ Institutional or commercial partners ■ Recipients from third countries or international organisations It is possible to fill in a field to provide for additional clarification regarding the category concerned	The categories of recipients should be subdivided into: ■ Categories of internally authorised persons to access the data (department and function or role to be indicated) or other internal data recipients, e.g. company doctor, staff council ■ Categories of external recipients (e.g. banks, tax offices), ■ Categories of recipients in third countries or international organisations	E.g. social security institutions Recommended: processors and sub-processors

Table 8 provides an overview of the information that must be included in the RPA according to Art. 30 (1) lit. e GDPR, namely, information on the transfer of data to a third country or international organisation.

Table 8: Specification of information to be included in the RPA according to Art. 30 (1) lit. e GDPR

Category of information required	Austria	France	Germany/BW	Italy
Where applicable, transfers of personal data to a third country or an international organisation, including its identification and, if necessary, the documentation of suitable safe-guards	Not mentioned in the DSB guideline	■ Recipient and country ■ Where applicable, the category of safe-guards provided for, such as transfers ■ Reference to the documentation concerned	DSK: In any case, a statement that a transfer to third countries does not take place and is not planned or an explanation as to how data are being transferred should be made. If data are being transferred or transfer is planned: ■ Name of the third country, recipient and/or international organisation ■ Where applicable, documentation of the safeguards and of their appropriateness The LfDI Baden-Württemberg-template contains also a field to include the legal basis for the data transfer (unclear if mandatory for companies)	■ Statement that such transfers are carried out ■ Countries ■ Where applicable, safeguards adopted

Table 9 provides an overview of the information that must be included in the RPA according to Art. 30 (1) lit. f GDPR, namely, information on the envisaged time limits for erasure of data.

Table 9: Specification of information to be included in the RPA according to Art. 30 (1) lit. f GDPR

Category of information required	Austria	France	Germany/BW	Italy
Where possible, the envisaged time limits for erasure of the different categories of data	Required, but not further specified	The retention period or, failing that, the criteria for determining it	■ Retention periods ■ Legally stipulated deletion periods ■ Review or deletion periods set by the controller	The retention period or, failing that, the criteria for determining it

Table 10 provides an overview of the information that must be included in the RPA according to Art. 30 (1) lit. g GDPR, namely, a description of the technical and organisational security measures referred to in Art. 32 (1) GDPR.

Table 10: Specification of information to be included in the RPA according to Art. 30 (1) lit. g GDPR

Category of information required	Austria	France	Germany/BW	Italy
Where possible, a general description of the technical and organisational security measures	Required, but not further specified	To be chosen from one of the following categories: ■ Traceability ■ Software protection ■ Data backup ■ Data encryption ■ Monitoring of users' access ■ Monitoring of processors ■ Other measures to be defined	A general, easily comprehensible description of the technical and organisational security measures, such as: ■ Pseudonymisation ■ Encryption ■ Measures to ensure the availability and resilience of systems and services (e.g. back-ups)	The security measures may be described in summary and in an abbreviated form if this description provides a general and overall picture of those measures in relation to the processing activities carried out

Table 11 provides an overview of the information that must be included in the RPA that are not required according to Art. 30 (1) GDPR, in other words, information requirements that can be regarded as gold plating.

Table 11: Specification of information to be included in the RPA for controllers that can be regarded as gold plating

Category of information required	Austria	France	Germany/BW	Italy
Other information to be included in the RPA	None	■ Name and the number/reference of the processing	■ Name of each relevant processing activity ■ Serial number assigned by the controller for each processing activity ■ Date of introduction of the processing activity ■ Date of last modification ■ Responsible department with the controller and the name of the operationally responsible contact person, their e-mail address and phone number (recommended) ■ Name of the procedure used (optional) ■ LfDI Baden-Württemberg template integrates a complete deletion concept (beyond the necessary deadlines, unclear if mandatory)	None

d) Information to be included in the RPA of processors

Table 12 provides an overview of the information that must be included in the RPA according to Art. 30 (2) lit. a GDPR, namely, information on the processor or processors, of each controller on whose behalf the processor is acting and, where applicable, of the controller's or the processor's representative as well as the data protection officer.

Table 12: Specification of information to be included in the RPA according to Art. 30 (2) lit. a GDPR

Category of information required	Austria	France	Germany/BW	Italy
Name and contact details of the processor(s)	Not mentioned in the DSB guideline	Name, postal address, e-mail address, ZIP code, city, phone number	Name, postal address, e-mail address, phone number, internet address (voluntary)	Required, but not further specified
Name and contact details of the controller on whose behalf the processor is acting	Not mentioned in the DSB guideline	Name, postal address, e-mail address, ZIP code, city, country, phone number	Name, postal address, e-mail address, phone number, serial number ("Lfd. Nr.").	Required, but not further specified
Where applicable, name and contact details of the controller or the processor's representative	Not mentioned in the DSB guideline	Name, postal address, e-mail address, ZIP code, city, phone number	Name, postal address, e-mail address, phone number	Not mentioned by the Garante
Where applicable, name and contact details of the data protection officer	Not mentioned in the DSB guideline	Name, postal address, e-mail address, ZIP code, city, country, phone number, company details if an external data protection officer is concerned	Name, title, first name, postal address, e-mail address, phone number	Not mentioned by the Garante

Table 13 provides an overview of the information that must be included in the RPA according to Art. 30 (2) lit. b GDPR, namely, information on the categories of processing carried out on behalf of each controller.

Table 13: Specification of information to be included in the RPA according to Art. 30 (2) lit. b GDPR

Category of information required	Austria	France	Germany/BW	Italy
Categories of processing carried out on behalf of each controller	Required, but not further specified	For example, the category "service of sending prospecting messages"; this may involve the collection of e-mail addresses, the secure sending of messages, the management of unsubscriptions etc.	DSK's template contains a field which includes checkboxes for some categories of processing, e.g.: ■ (Paper) document destruction ("Akten-vernichtung") ■ Archiving (of data files) ■ Office communication ■ Cloud services ■ Financial accounting ■ Hosting of an e-mail system ■ Hosting of an internet system ■ Hosting of processing ■ Payroll accounting ■ Personnel management ■ Advertising/letter shop ■ Time recording ■ Travel expenses	The processor may use the information contained in the contract with the controller, which must contain information on the nature and purpose of the processing, the type of personal data and the categories of data subjects concerned by the processing, as well as the duration of the processing

Table 14 provides an overview of the information that must be included in the RPA according to Art. 30 (2) lit. c GDPR, namely, information on the transfer of data to a third country or international organisations.

Table 14: Specification of information to be included in the RPA according to Art. 30 (2) lit. c GDPR

Category of information required	Austria	France	Germany/BW	Italy
Where applicable, transfers of personal data to a third country or an international organisation, including its identification and, if necessary, the documentation of suitable safeguards	Not mentioned in the DSB guideline	■ Recipient and country ■ Where applicable, the category of safe-guards provided for such transfers ■ Reference to the documentation con-cerned	In any case, a statement that a transfer to third countries does not take place and is not planned or an explanation as to how data are being trans-ferred should be made; if data are being trans-ferred or planed: ■ Name of the third country, recipient, and/or international organisation Where applicable, documentation of the safe-guards and of their appropriateness	Not mentioned by the Garante

Table 15 provides an overview of the information that must be included in the RPA according to Art. 30 (2) lit. d GDPR, namely, a description of the technical and organisational security measures referred to in Art. 32 (1) GDPR.

Table 15: Specification of information to be included in the RPA according to Art. 30 (2) lit. b GDPR

Category of information required	Austria	France	Germany/BW	Italy
Where possible, a general description of the technical and organisational security measures	Not mentioned in the DSB guideline	To be chosen from one of the following categories: ■ Traceability, ■ Software protection, ■ Data backup, ■ Data encryption, ■ Monitoring of users' access, ■ monitoring of processors ■ Other measures to be defined	A general, easily comprehensible description of the technical and organisational security measures	Not mentioned by the Garante

Table 16 provides an overview of the information that must be included in the RPA that is not required according to Art. 30 (2) GDPR, in other words, information requirements that can be regarded as gold plating.

Table 16: Specification of information to be included in the RPA for processors that can be regarded as gold plating

Category of information required	Austria	France	Germany/BW	Italy
		■ Sub-processor:[253] name, postal address, e-mail address, ZIP code, city, phone number ■ Sub-processor's[254] representative (if applicable): name, postal address, e-mail address, ZIP code, city, phone number ■ Controller's data protection officer: name, postal address, e-mail address, ZIP code, city, phone number, company details if an external data protection officer is concerned	Sub-processor's name[255]	

e) Design of the RPA

Table 17 provides an overview of the required format for the RPA.

Table 17: Design of the RPA

	Austria	France	Germany/BW	Italy
Format	Paper or electronic	Paper or electronic	Paper or electronic	Paper or electronic

f) Actualisation/Update of the RPA

Table 18 provides an overview of the duties related to the update of the RPA.

253 Art. 30 refers to "processor or processors". The plural could include the sub-processors, but as they are not mentioned explicitly, we consider this to be gold plating.

254 Art. 30 refers to "processor or processors". The plural could include the sub-processors, but as they are not mentioned explicitly, we consider this to be gold plating.

255 Art. 30 refers to "processor or processors". The plural could include the sub-processors, but as they are not mentioned explicitly, we consider this to be gold plating.

Table 18: Update of the RPA

	Austria	France	Germany/BW	Italy
Duty to indicate the date of update	Not mentioned in the DSB guideline	Yes, for each form and each processing (including the form's date of creation)	Not specified any further by the authority; however, the date of last modification of the processing activity must be indicated	Yes, e.g. for modalities, purposes, categories of data, categories of data subjects
Duty to document and archive changes of the RPA	Not mentioned in the DSB guideline	No, but recommended by lawyers	Yes, with a storage period of one year	Yes

g) Exemption from the duty to maintain an RPA

Table 19 provides an overview of the application of the exemption from the duty to maintain an RPA according to Art. 30 (5) GDPR.

Table 19: Exemption from the duty to maintain an RPA according to Art. 30 (5) GDPR

	Austria	France	Germany/BW	Italy
Do DPAs concretise the application of the exemption, e.g. by giving examples of processing operations that prevent the application of the exemption?	No examples given	Yes, exemption does not apply in the following cases: ■ Non-occasional processing such as payroll management, customer/prospect and supplier management ■ Processing likely to result in a risk to the rights and freedoms of data subjects such as geolocation systems, video surveillance ■ Processing of sensitive data such as health data, offences	Yes, exemption does not apply in the following cases: ■ Non-occasional processing such as personnel management and customer data management ■ Processing likely to result in a risk to the rights and freedoms of data subjects such as video surveillance, credit scoring or fraud prevention procedures, tracking of employees (e.g. by GPS) or processing operations which involve the content of communications ■ Processing of sensitive data such as data on religious affiliation, health data or biometric data for unique identification	Yes, exemption does not apply in the following cases: ■ Companies with at least one employee (e.g. bars, restaurants, workshops, shops, small retailers) and/or ■ Companies which process customers' health data (e.g. hairdressers, beauticians, opticians, dental technicians, tattoo artists etc.) ■ Self-employed professionals with at least one employee and/or ■ Self-employed professionals who process health data and/or data relating to criminal convictions or offences (for example, accountants, notaries, lawyers, osteopaths, physiotherapists, pharmacists, doctors in general)

7. Conclusion

"Processing activity" not defined by GDPR

From the above information, it can be inferred that it is not always easy for companies to determine the required volume of the RPA. As the main part of the RPA is essentially a list of "processing activities", the understanding of the notion of a "processing activity" is important for determining the necessary level of detail of the RPA. The GDPR does not define what a "processing activity" is; rather, it only contains a wide definition of the term "processing", meaning any operation involving personal data. EU law therefore leaves open to what level of detail these "processing activities" must be described in the RPA.

The guidance given by the national DPAs on this point does not completely clarify all ambiguities. The websites of the Austrian and the Italian DPA do not provide any relevant help on this question. From the templates and official guidance provided by the French and the German DPAs available online, it becomes clear that a "processing activity" can include more than one processing operation. This means that controllers are not required to list every single processing operation in their RPA but may apply a certain level of abstraction. According to the French CNIL, the RPA must contain a list of the main activities of the company involving data collection and processing, and the controller must indicate the required information (such as the purpose of the processing and a description of the categories of data subjects) for each "category" of processing activity. In Germany, the controller's RPA must likewise list the required information for each processing activity, e.g. by completing a separate main sheet for every processing activity, the sum of which – in conjunction with the general information on the controller's contact details – will constitute the RPA. The German authorities apply a "strict standard", stating that each new purpose of processing constitutes a separate processing activity, requiring a separate description in the RPA. Accordingly, the more detailed the subdivision of the processing activities is, the more precise and comprehensive the RPA will be. The LfDI Baden-Württemberg seems to link the volume of a processing activity and thus the required granularity of the RPA to the size of the company and probably to the scope of the processing carried out within such a single processing activity as well, while the GDPR does not establish such a link. On the one hand, this differentiation seems to make the drafting of the RPA for bigger companies more burdensome, as they must subdivide their processing activities and include maybe dozens or even hundreds of processing activities in the RPA. On the other hand, this interpretation offers a flexible solution and makes the drafting of the RPA easier for smaller companies, clarifying that their RPA does not necessarily need to be that detailed. The EDPB should give further guidance on the notion of a processing activity and the required level of detail of the RPA.

Level of detail of "processing activities" significantly different in the Member States researched

In summary, in Austria and Italy, it remains completely open to what level of detail the "processing activities" must be described in the RPA; while in Germany and France, it is clear that a certain abstraction can be made, although the appropriate level of abstraction is not

absolutely clear. In view of the more detailed statements and greater attention of the German DPAs, the required level of detail of the RPA and thus the controller's time and organisational effort in drafting might be greater in Germany than in the other Member States researched, at least for larger companies that must more precisely subdivide their processing activities.

Secondly, the level of guidance and help provided by the national DPAs on the drafting of an RPA differs significantly between the Member States researched. All four national DPAs have published a guideline on their website containing at least some information on the duties under Art. 30 GDPR. The DPA giving the lowest amount of guidance is clearly the Austrian DSB, which offers only very little information on the duty to draft an RPA, while the other DPAs provide significantly more comprehensive guidance. Apart from the Austrian DSB, all national DPAs provide at least one non-mandatory template for the RPA. The French CNIL offers a single template for controllers and processors, without clearly stating which fields do not need to be filled in by processors. The German and Italian DPAs provide separate templates for controllers and processors. While the German templates are suitable for all companies, the two Italian ones only contain simplified RPAs aimed at small and medium-sized enterprises. The most sophisticated template is the one provided by the French CNIL: it consists in a clearly structured Excel spreadsheet which enables the controller to fill in most of the fields by selecting the appropriate information from a drop-down menu, thereby making it substantially easier and quicker to provide the required information. The LfDI Baden-Württemberg also provides a training video on how to prepare an RPA.

Different levels for assistance from authorities – Austria brings up the rear

Regarding information to be included in the RPA, the GDPR lists the information to be provided only roughly, without clarifying what details must be given. As a result, the official templates provided by the DPAs of the four Member States researched differ to a certain extent. While it is clearly specified in the German and French templates which exact contact details of the controller, its representative, joint controller and data protection officer must be indicated, this is not the case in Austria (where the DPA does not provide a template) and in Italy. Regarding the information to be provided for the relevant processing activities, in Germany, the level of necessary details to be provided often appears to be higher, as the template and guidance require the controller to make more subdivisions, e.g. when describing the purposes of the processing or the categories of personal data processed. In France, the template – despite being a "basic" one – is also rather detailed, as there is a considerable number of fields to be filled in and descriptions to be inserted. However, the French template widely uses drop-down menus from which the controller may choose. It therefore allows for a particularly time-saving completion of the RPA. This extremely user-friendly template seems to make the work for French controllers much easier than for their German counterparts, who must first consult the DPA's guidelines to learn what exact information they are required to include. Therefore, the French template seems to be the easiest to handle. The Italian templates

are not easily comparable with the French ones and the one provided by the German DSK as they are simplified templates to be used only by small and medium-sized enterprises. On the one hand, a comprehensive template seems to create a greater burden for controllers. On the other hand, a more comprehensive template makes it clearer for the controller what level of granularity of information is required. It can be assumed that in Member States in which there is no (Austria) or no comprehensive (Italy) official template, the creation of an appropriate RPA is more difficult. The non-existence of an official template does not necessarily mean that less information must be included, but the controller is lacking any guidance regarding the required information and its level of detail.

Gold plating by France and Germany

The French and German templates require the controllers to include a few additional pieces of information that are not expressly required by the GDPR, e.g. a name for each processing activity described and the serial or reference number assigned to it by the controller, and in Germany also the date of introduction of the respective processing activity, the date of last modification, the responsible department with the controller and the name of the operationally responsible contact person. Requesting such additional information can be regarded as gold plating. In Baden-Württemberg, controllers may feel obliged to provide furthermore the legal basis for the transfer of data to third countries, as the template contains a respective field (unclear if mandatory). Overall, as to the required information, the extent of gold plating with regard to Art. 30 GDPR does not seem to be excessive. From the above, it follows that in any case, the bureaucratic burden for controllers and processors also depends on the availability and user-friendliness of the official template provided by the competent DPA.

As regards the assessment of whether the exemption in Art. 30 (5) GDPR applies to a controller with fewer than 250 employees, France and Germany clearly name the reasons for the non-applicability of the exemption stated in the EDPB guidance (processing likely to result in a risk, non-occasional processing, processing of sensitive data) and furthermore provide a few examples for each reason. Italy does not clearly name the reasons brought by the EDPB but provides practical examples which basically reflect the points mentioned in the EDPB guidance, although they are slightly narrower. Austria does not name any reasons for the non-applicability of the exemption or provide any examples at all.

Proposal: EDPB should provide harmonised templates

The EDPB should publish a harmonised template for controllers and a separate one for processors, which the national DPAs can then translate into their official language. These templates should – to the extent possible – combine the advantages of the templates of the four Member States researched. Inter alia, the template should

- be clearly structured,
- be divided in a separate template for controllers and processors,
- be self-explanatory or contain direct links that provide further explanations,
- offer checkboxes or – preferably – detailed drop-down menus like in the CNIL's template with entries at least for the most relevant information from which the controller/processor can choose the suitable answer,
- explain possibilities to simplify the RPA for smaller companies.

IV. Regulatory burdens arising from the obligation to notify the supervisory authority of a personal data breach according to Art. 33 GDPR

This chapter examines the regulatory burdens arising for private companies from the obligations under Art. 33 GDPR with regard to notifying the competent supervisory authority of a personal data breach.

1. EU level

a) Legal sources

aa) Art. 33 GDPR

Art. 33 GDPR obliges the controller to document data breaches and to report certain personal data breaches to the competent DPA within the meaning of Art. 51 and 55 GDPR. Art. 33 GDPR does not contain an explicit opening clause for the Member States.

bb) Guidance from the European Data Protection Board (EDPB)

The former Art. 29 Working Party had adopted revised guidelines on personal data breach notification under the GDPR[256] (hereinafter "Guidelines WP 250"), which in May 2018 were endorsed[257] by the EDPB. These general guidelines concern Art. 33 and 34 GDPR. In 2014, the Art. 29 Working Party had already published an opinion on breach notification.[258] In October 2022, the EDPB published a slightly updated version of the Guidelines WP 250, under the

256 Art. 29 Working Party, Working Paper 250 rev.1 (fn. 288).

257 https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en.

258 Opinion 03/2014 on Data Breach Notification of 25 March 2014, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

name "Guidelines 9/2022 on personal data breach notification under GDPR"[259] (hereinafter referred to as "EDPB Guidelines 09/2022").[260]

As these general guidelines do not address all practical issues in sufficient detail, the EDPB released further guidelines on examples regarding data breach notification in 2021[261] (hereinafter the "EDPB Guidelines 01/2021"). This practice-oriented, case-based guidance intends to complement the Guidelines WP 250 (and now the EDPB Guidelines 09/2022) and reflects the common experiences of the national DPAs since the beginning of the application of the GDPR. It aims to help controllers in deciding how to handle data breaches and what factors to consider during risk assessment.[262] Beyond this, the EDPB has not issued any further written guidance on Art. 33 GDPR.

b) Subject of the duties

According to Art. 33 (1) GDPR, only the controller is obliged to document personal data breaches and possibly report them to the DPA. Once a processor becomes aware of a personal data breach, it must notify the controller without undue delay.[263] This study especially examines the bureaucratic costs in relation to the controller's duties under Art. 33 regarding personal data breaches. Therefore, the processor's obligations under Art. 33 will not be addressed further.

c) Overview and purpose of the duties under Art. 33 GDPR

Art. 33 GDPR obliges the controller to document personal data breaches and to report them to the competent DPA if certain conditions are fulfilled. Its purpose is to create transparency on data breaches that have occurred and to enable also the DPAs to prevent or at least minimise further damages which may result from the data breach.[264] If not appropriately and timely addressed, a personal data breach may result in physical, material or non-material damage to natural persons, such as loss of control over their personal data, limitation of their rights,

259 EDPB, Guidelines 09/2022 of 10 October 2022 on personal data breach notification under GDPR, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-92022-personal-data-breach_en.

260 However, the new EDPB Guidelines 09/2022 do not contain any changes that are relevant for this study. Except for a few editorial changes, the new guidelines correspond verbatim to the text of the WP 250 rev. 1. The EDPB has added numbering and only updated one passage on the requirements concerning personal data breaches at non-EU establishments. The remainder of the WP 250 remains unchanged. However, the version of the guidelines published in October 2022 is still a version for public consultation. It is therefore possible that other changes will be made to the guidelines based on feedback from the consultation process.

261 EDPB, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification of 14 December 2021, Version 2.0, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en.

262 EDPB Guidelines 01/2021 (ibid.), p. 5.

263 Art. 33 (2) GDPR.

264 Gola, DS-GVO, Art. 33 No 2. See also Recital 85 of the GDPR and Guidelines WP 250 (fn. 28), p. 14 / EDPB Guidelines 09/2022 (fn. 259), No 51.

discrimination, identity theft, fraud, financial loss, damage to reputation or other significant economic or social disadvantages.[265]

The notification requirement shall also encourage controllers to act promptly on a data breach, contain it and, if possible, recover the compromised personal data, and to seek relevant advice from the DPA.[266] Art. 33 is closely connected with the controller's obligations under Art. 34 GDPR to inform the data subject of certain data breaches, which are, however, not covered by this study. This study only examines the bureaucratic costs in relation to the controller's obligations under Art. 33 GDPR.

As will be shown below, Art. 33 contains numerous indefinite legal terms, which may lead to varying application in practice and/or to difficulties in its application.

d) The notion of a "personal data breach"

GDPR defines notion of "personal data breach"

The GDPR defines a "personal data breach" as a breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data which are transmitted, stored or otherwise processed.[267] A personal data breach is thus a type of security incident.[268]

e) Categories of personal data breaches

According to the EDPB, personal data breaches can be categorised according to the following three well-known information security principles[269]:

- "confidentiality breach", i.e. where there is an unauthorised or accidental disclosure of, or access to, personal data.

Examples for a confidentiality breach are the so-called mispostal cases, e.g. if an e-mail or another document containing personal data of individuals is sent to an unauthorised recipient by mistake.[270]

265 Recital 85 of the GDPR. Further examples for possible damages can be found in recital 75 of the GDPR, notwithstanding the fact that it does not relate to risks resulting from data breaches but to risks resulting from specific processing activities.

266 Gola, DS-GVO, Art. 33 No 2. See also Recital 85 and Guidelines WP 250 (fn. 28), p. 15 / EDPB Guidelines 09/2022 (fn. 259), No 58.

267 Art. 4 No 12 GDPR.

268 Guidelines WP 250 (fn. 28), p. 7 / EDPB Guidelines 09/2022 (fn. 259), No 15.

269 Guidelines WP 250 (fn. 28), p. 7 / EDPB Guidelines 09/2022 (fn. 259), No 17; EDPB Guidelines 01/2021 (fn. 261), No 5.

270 EDPB Guidelines 01/2021 (fn. 261), p. 28.

- "Integrity breach", namely, where there is an unauthorised or accidental alteration of personal data.

An integrity breach may occur, for example, if a controller is the victim of a cyber-attack which places malicious code on its website and enables the infiltrator to establish changes in the controller's system.[271]

- "Availability breach", namely, where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

A "loss" of personal data may also be assumed when the data still exist, but the controller has lost control or access to them or no longer has them in its possession.[272] An example for a loss of personal data may be a device containing a copy of a controller's customer database being lost or stolen or the only copy of a set of personal data being encrypted by ransomware.[273]

Depending on the circumstances, a breach can concern the confidentiality, integrity and availability of personal data at the same time, as well as any combination of these aspects.[274]

f) Information to be included in the notification

The minimum content of the notification is regulated in Art. 33 (3) GDPR. According to this article, the notification shall contain at least:

- a description of the nature of the personal data breach; "where possible", this description must include
  - the categories of data subjects concerned; while the notion of "category of data subjects" is not defined in the GDPR, guidance by the EU DPAs suggests referring to the various types of individuals whose personal data have been affected by a breach (e.g. children, employees, customers),[275]
  - the approximate number of data subjects concerned,
  - the categories of personal data records concerned; while the notion of "category of personal data" is not defined in the GDPR, guidance by the EU DPAs suggests referring to the different types of personal data that the controller may process (e.g. health data,

271 EDPB Guidelines 01/2021 (fn. 261), p. 15.

272 Guidelines WP 250 (fn. 28), p. 7 / EDPB Guidelines 09/2022 (fn. 259), No 14.

273 Guidelines WP 250 (fn. 28), p. 7 / EDPB Guidelines 09/2022 (fn. 259), No 14.

274 Guidelines WP 250 (fn. 28), p. 8 / EDPB Guidelines 09/2022 (fn. 259), No 18.

275 Guidelines WP 250 (fn. 28), p. 14 / EDPB Guidelines 09/2022 (fn. 259), No 50.

financial details, bank account numbers etc.)[276], and

- the approximate number of personal data records concerned,

- the name and contact details of the controller's data protection officer (if appointed) or another contact point from which the DPA can obtain more information,
- a description of the likely consequences of the personal data breach; if the types of data subjects or the types of personal data indicate a risk of particular damage occurring as a result of a breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy), then it is important to indicate these categories in the notification,[277]
- a description of the measures which the controller has taken or has proposed taking to address the personal data breach, including – "where appropriate" – a description of the measures taken or proposed to mitigate the possible adverse effects of the personal data breach.

g) Where to notify?

According to Art. 33, data breaches must be reported to the competent supervisory authority within the meaning of Art. 55 GDPR, which the Member States must provide for (Art. 51 (1)). Art. 55 states that the supervisory authority provided for by a Member State is competent on the respective Member State's territory.[278]

h) Design of the notification

aa) Format of the notification

Art. 33 GDPR does not specify through which means of communication and in which format the breach must be reported to the competent DPA (e.g. via phone, fax, e-mail or online). National differences may arise in this regard.

bb) Language

The GDPR does not regulate in which language the notification must be made, meaning in which language the required information must be provided to the competent national DPA. This could also result in national differences.

276 Guidelines WP 250 (see fn. 28), p. 14 / EDPB Guidelines 09/2022 (fn. 259), No 50.

277 Guidelines WP 250 (see fn. 28), p. 14 / EDPB Guidelines 09/2022 (fn. 259), No 51.

278 Art. 56 GDPR contains specific competence rules for cross-border processing. However, for the purpose of this study, we are assuming that the data breach takes place within a Member State and is not related to cross-border processing.

i) Timeline of the notification

Art. 33 (1) GDPR provides that the breach must be notified "without undue delay", generally ("where feasible") within 72 hours after the controller has "become aware" of the breach.[279] The time limit for reporting is open to interpretation, as the GDPR leaves undefined which delay is still "due" and when the controller's knowledge of the breach is to be assumed and the time limit thus starts to run. The EDPB has provided[280] some guidance on the interpretation of these terms.

aa) Awareness of the breach

According to the EDPB, it should be presumed that a controller has become "aware" of a data breach when that controller has "a reasonable degree of certainty that a security incident has occurred" and that this incident "has led to personal data being compromised".[281] When, exactly, a controller can be considered to be "aware" of a particular breach depends, however, on the circumstances of the specific breach. In some cases, it may take some time to establish if personal data have been compromised.[282] In any case, the controller should promptly start to investigate the incident.

For example, in the case of loss of an USB key containing personal data, the controller becomes "aware" upon realising that the USB key has been lost because there is a reasonable degree of certainty that an availability breach has occurred.[283] If the controller detects a possible intrusion into its network, it becomes "aware" of the data breach when – after checking its systems – it can confirm that personal data held on that system have been accessed without authorisation or otherwise compromised.[284]

bb) Delay for the notification

Which delay is still "due" also depends on the circumstances of the specific data breach. In this regard, the EDPB guidance only refers to the DPAs' verification of the timely notification, stating that when determining ex post whether the reported security incident has been reported "without undue delay", the DPAs should take into account in particular[285]

- the nature and gravity of the personal data breach,

279 Art. 33 (1) 1st sentence GDPR.

280 This includes the EDPB Guidelines 09/2022 (fn. 259), which replace the WP 250 of the Art. 29 Data Protection Group already endorsed by the EDPB.

281 Guidelines WP 250 (fn. 28), p. 10 et seq. / EDPB Guidelines 09/2022 (fn. 259), No 31 et seq.

282 Guidelines WP 250 (fn. 28), p. 11 / EDPB Guidelines 09/2022 (fn. 259), No 33.

283 Guidelines WP 250 (fn. 28), p. 11 / EDPB Guidelines 09/2022 (fn. 259), No 33.

284 Guidelines WP 250 (fn. 28), pp. 11, 12 / EDPB Guidelines 09/2022 (fn. 259), No 33.

285 Recital 87 of the GDPR, see also Guidelines WP 250 (fn. 28), p. 11 / EDPB Guidelines 09/2022 (fn. 259), No 26.

- the consequences of the personal data breach and
- the adverse effects of the personal data breach for the data subject.

The notification must generally be made within 72 hours and may only in exceptional cases be delayed. If the controller does not make the notification within 72 hours, it must provide reasons for the delay together with the notification[286] in order to justify the delay. However, the EDPB has stipulated that in high risk level cases, even complying with the 72-hour deadline can be viewed as unsatisfactory.[287]

Art. 33 (4) allows the controller to provide information "in phases" when it has become clear that here has been a breach whose extent is not yet known.[288] This means that information that is not initially available may be submitted later, however, "without undue further delay". This is in particular relevant for more complex breaches, such as specific types of cybersecurity incidents which require an indepth investigation.[289] For example, the controller may complete its full risk assessment in parallel to the notification and then provide the information gained to the DPA without undue further delay.[290]

If a controller detects that a series of breaches has taken place which concern the same types of personal data, breached in the same way over a relatively short period, it may also submit a "bundled" notification representing all these breaches.[291]

j) Exemptions from the duty to report a personal data breach to the supervisory authority

Art. 33 GDPR states that, in principle, there is a duty to report a personal data breach, which may, in exceptional cases, be waived due to a lack of risk. Only exceptionally, the notification obligation does not apply if the data protection breach is "unlikely to result in a risk" to the rights and freedoms of natural persons. The controller must therefore assess the risks that could result from the personal data breach.[292] In particular, the controller must – objectively and on a case-by-case basis – assess the likelihood and severity of the impact on the rights and freedoms of natural persons as a result of the personal data breach.[293]

---

286 Art. 33 (1) 2nd sentence GDPR.

287 EDPB Guidelines 01/2021 (fn. 261), No 24.

288 Guidelines WP 250 (fn. 28), p. 15 / EDPB Guidelines 09/2022 (fn. 259), No 53.

289 Guidelines WP 250 (fn. 28), p. 15 / EDPB Guidelines 09/2022 (fn. 259), No 57.

290 EDPB Guidelines 01/2021 (fn. 261), No 8.

291 Guidelines WP 250 (fn. 28), p. 16 / EDPB Guidelines 09/2022 (fn. 259), No 64.

292 Guidelines WP 250 (fn. 28), p. 23 / EDPB Guidelines 09/2022 (fn. 259), No 101.

293 Guidelines WP 250 (fn. 28), p. 8 / EDPB Guidelines 09/2022 (fn. 259), No 22, 101, 103, 114; EDPB Guidelines 01/2021 (fn. 261), No 21.

The EDPB has endorsed guidelines on how to determine whether a certain *processing operation* is "likely to result in a *high* risk".[294] However, these guidelines are barely helpful for the risk assessment required here as the statements within them do not readily allow conclusions to be drawn about whether a personal data breach is likely to result in a *normal* or *low* risk.

According to the EDPB Guidelines 01/2021, the controller should investigate the data breach, e.g. the method of infiltration in a ransomware case, and identify the type of the malicious code to understand the possible consequences of the attack. For example, the controller must thoroughly examine the firewall logs and their implications to determine the risk and should be able to present the factual findings of these investigations upon request.[295]

Controllers must consider the following factors when accessing risk[296]:

- the type of data breach[297];
- the nature, the sensitivity[298], the volume (namely, the number of individuals affected and the overall quantity of affected data)[299] and the context of the personal data,
- the ease of identification of individuals, in other words, how easy it will be for a party who has access to compromised personal data to identify specific individuals or match the data with other information to identify individuals[300],
- the severity of the consequences for individuals, meaning the potential damage[301] to individuals that could result from the breach; for example, where special categories of data (such as health data pursuant to Art. 9 (1) GDPR or other types of sensitive data) are affected, the potential damage to individuals could be severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation[302],

---

294 Art. 29 Working Party, "Guidelines on Data Protection Impact Assessment" (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", WP 248 rev.01, endorsed by EDPB, available at https://ec.europa.eu/newsroom/article29/items/611236, p. 9.

295 EDPB Guidelines 01/2021 (fn. 261), No 28.

296 Guidelines WP 250 (fn. 28), pp. 23 et seqq. / EDPB Guidelines 09/2022 (fn. 259), No 103 et seqq., which also contain further details and explanations; EDPB Guidelines 01/2021 (fn. 261), No 29, 38, 43, 52, 53.

297 The type of the breach can become a risk-enhancing factor, e.g. in an infiltration case in which not only data has been confidentiality curtailed, but the infiltrator also has the means to establish changes in the system so that data integrity also becomes questionable, cf. EDPB Guidelines 01/2021 (fn. 261), No 52, 38.

298 E.g. breaches involving health data, identity documents or financial data such as credit card details can all cause harm on their own, but together they could be used for identity theft, cf. Guidelines WP 250 (fn. 28), p. 24 / EDPB Guidelines 09/2022 (fn. 259), No 108.

299 EDPB Guidelines 01/2021 (fn. 261), No 38, 43. In No 78, the EDPB considers the quantity of data affected as low in a case in which the data breach only concerned about two dozen costumers.

300 Guidelines WP 250 (fn. 28), p. 19 / EDPB Guidelines 09/2022 (fn. 259), No 111.

301 Examples for potential damage have been listed above, cf. Section A. IV. 1 c).

302 Guidelines WP 250 (fn. 28), p. 25 / EDPB Guidelines 09/2022 (fn. 259), No 113.

- the special characteristics of the individual that may affect the level of impact of the breach[303],
- the special characteristics of the controller that may affect the level of impact of the breach,
- the number of affected individuals and
- some general points; for example, the controller should combine all these findings and make an overall assessment of how severe the possible consequences for the affected individuals are as well as how likely they are to occur. The greater the consequences and the greater the probability of their occurrence, the greater is the risk.

Measures taken by the controller before[304] or immediately after the breach may also have an impact on the risk assessment. If the controller takes "appropriate steps" after the data breach, such a breach is unlikely to have any impact on the data subjects' rights and freedoms.[305]

The EDPB Guidelines 01/2021 provide further information on the basis of several example cases (for example, ransomware and data exfiltration attacks, lost or stolen devices or documents, mispostal attacks and identity theft) on whether a risk exists and an incident must therefore by reported.[306]

According to these guidelines, gathering exact information on the data breach is key in determining the risk level. Controllers who are uncertain about the specifics of the illegitimate access should consider the worse scenario and assess the risk accordingly.[307] If in doubt, the controller should act cautiously and report the breach.[308]

In particular, the EDPB considers a notification to be necessary, for example,

- if the restoration of lost data would take longer and cause delays in the delivery to customers,
- if special categories of personal data are affected and thus the care of patients is at risk or

303 An example for a case in which there were no such specific characteristics of the individuals or the controller existed can be found in the EDPB Guidelines 01/2021 (fn. 261), No 77.

304 Cf. EDPB Guidelines 01/2021 (fn. 261), No 18, 24.

305 EDPB Guidelines 01/2021 (fn. 261), No 79 et seq.

306 EDPB Guidelines 01/2021 (fn. 261), No 16 et seqq.

307 EDPB Guidelines 01/2021 (fn. 261), No 30.

308 Guidelines WP 250 (fn. 28), p. 26 / EDPB Guidelines 09/2022 (fn. 259), No 119.

- if identity card numbers and financial data, such as credit card details of clients, are involved in the breach and this causes a risk of identity theft or fraud and/or of financial loss.[309]

An example for a breach which would not require notification of the supervisory authority is the controller losing a securely encrypted mobile device. Provided the lost device does not contain the sole copy of the personal data and the encryption key remains within the secure possession of the controller, the personal data would be inaccessible to an attacker. In this case, the breach is unlikely to result in a risk to the rights and freedoms of the data subjects in question.[310]

The EDPB has clarified that while notification may initially not be required if there is no likely risk to the rights and freedoms of individuals, this may change, at which time the risk would have to be re-evaluated (for example, if it becomes evident later that the encryption key used was compromised).[311]

k) Documentation duties (Art. 33 (5) GDPR)

Art. 33 (5) GDPR stipulates that the controller must document each and every personal data breach, even if the controller is not obliged to report the breach to the DPA in the individual case.[312] It is up to the controller to determine what method and structure to use when documenting a breach.[313] However, the documentation must contain

- the facts relating to the breach, in other words, the details of the data protection incident, in particular its causes, what happened and what personal data have been affected,[314]
- the effects of the personal data breach and
- the action the controller has taken to remedy the breach.

Such documentation assists the controller in demonstrating accountability to the supervisory authority. The purpose of the documentation obligation is to enable the competent DPA to verify the controller's obligation to report and thus its compliance with Art. 33 GDPR.[315] For this

309 EDPB Guidelines 01/2021 (fn. 261), No 33, 45.

310 Guidelines WP 250 (fn. 28), p. 19 / EDPB Guidelines 09/2022 (fn. 259), No 79.

311 Guidelines WP 250 (fn. 28), p. 22 / EDPB Guidelines 09/2022 (fn. 259), No 98; EDPB Guidelines 01/2021 (fn. 261), No 58.

312 Guidelines WP 250 (fn. 28), p. 26 / EDPB Guidelines 09/2022 (fn. 259), No 121.

313 Guidelines WP 250 (fn. 28), p. 26 / EDPB Guidelines 09/2022 (fn. 259), No 123.

314 Guidelines WP 250 (fn. 28), p. 27 / EDPB Guidelines 09/2022 (fn. 259), No 123.

315 Art. 33 (5) 2nd sentence GDPR.

purpose, the DPA may also request to see the documentation.[316] Failure to properly document a breach may lead to the imposition of fines by the competent DPA.[317]

In addition, the European DPAs recommend that the controller also document its reasoning for the decisions taken in response to a breach. Especially if a breach is not reported, a justification for that decision should be documented. This should include reasons why the controller considers that the breach is unlikely to result in a risk to the rights and freedoms of individuals.[318]

This interpretation is also supported by Recital 85 of the GDPR, which states that the controller should report the personal data breach to the DPA "unless it is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."

In view of these duties, the European DPAs encourage controllers to establish an internal register of breaches. The controller may also document breaches as part of its RPA. A separate register is not required, provided the information relevant to the breach is clearly identifiable as such and can be extracted upon request.[319]

l) Other duties

Aligned with the notification and documentation duties is the controller's obligation to establish internal procedures to manage personal data breaches. Each controller and processor should have plans and procedures as well as clear reporting lines and assign responsible persons for the recovery of the data.[320] The EDPB thus recommends that controllers and processors prepare in advance their own "Handbook on Handling Personal Data Breach" which could be used as an internal source of information and allow them to mitigate risks and timely meet their obligations under Art. 33 GDPR.[321]

Beyond this, the controller must implement all appropriate technological protection and organisational measures ("TOMs") to be able to establish immediately whether a personal data breach has occurred and to promptly inform the supervisory authority and the data subject.[322]

---

316 Guidelines WP 250 (fn. 28), p. 8 / EDPB Guidelines 09/2022 (fn. 259), No 22, 122.

317 Art. 58, 83 GDPR, cf. also Guidelines WP 250 (fn. 28), p. 27 / EDPB Guidelines 09/2022 (fn. 259), No 129.

318 Guidelines WP 250 (fn. 28), p. 27 / EDPB Guidelines 09/2022 (fn. 259), No 125; see also Gola, DS-GVO, Art. 33 No 26.

319 Guidelines WP 250 (fn. 28), p. 26 / EDPB Guidelines 09/2022 (fn. 259), No 122.

320 EDPB Guidelines 01/2021 (fn. 261), No 11.

321 EDPB Guidelines 01/2021 (fn. 261), No 13.

322 Recital 87 of the GDPR. The EDPB recommends some TOMs in its Guidelines 01/2021 (fn. 261), No 49, 70, 84, 105, 123.

However, as these obligations are stipulated in other provisions[323] of the GDPR, they will not be further addressed in this study.

2. Austria

a) Relevant national legal and other sources

aa) Relevant national legislation

Legislative competence for data protection law lies with the federal level.[324] Data protection law is laid down in the Data Protection Act (Datenschutzgesetz, DSG).[325] It does not contain specific provisions regarding the duties under Art. 33 GDPR.

Neither is there secondary legislation that contains information on the implementation or enforcement of Art. 33 GDPR.

bb) Guidance from the Austrian public authorities

Guidance by Austrian public authorities: notification form, guideline, quarterly newsletter and annual report.

The Austrian data protection authority , called Datenschutzbehörde (hereinafter referred to as "DSB"), is a federal authority.[326] The DSB has published a form for data breach notifications.[327] Beyond this, it has issued a guideline on the GDPR (hereinafter referred to as the "DSB guideline").[328] Furthermore, the DSB has a quarterly newsletter[329] and publishes an annual report that may also contain information that is relevant for the purpose of this study.[330]

cc) Relevant national case law

Austrian case law: data breach by leaving mail bag briefly unattended on the pavement.

The Federal Administrative Court (Bundesverwaltungsgericht, BVwG), the court that decides about appeals against the DSB's decisions, has ruled on Art. 33 GDPR on one occasion.[331] It found a postal operator to have violated Art. 33 by submitting a data breach notification more than 72 hours after one of their employees had left a mail bag that was only closed with a cord unattended on the pavement for several minutes.

323 See e.g. Art. 24, 25, 32 GDPR.

324 Art. 10 (1) No 13 of the Federal Constitutional Law, available in a bilingual version translated by the Federal Chancellery at https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1930_1/ERV_1930_1.pdf.

325 A bilingual version translated by the Federal Chancellery is available at https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.pdf.

326 https://www.dsb.gv.at/.

327 Available at https://www.dsb.gv.at/dam/jcr:81630a55-648b-4689-b849-ce0732f6a1af/Meldung%20von%20Verletzungen%20des%20Schutzes%20personenbezogener%20Daten%20gem%C3%A4%C3%9F%20Art.%2033%20DSGVO%20Notification%20of%20a%20personal%20data%20breach%20(Art.%2033%20GDPR)%20.pdf.

328 Leitfaden zur Verordnung (EU) 2016/679, available at https://www.dsb.gv.at/download-links/dokumente.html.

329 Available at https://www.dsb.gv.at/download-links/newsletter.html.

330 Available at https://www.dsb.gv.at/download-links/dokumente.html.

331 BVwG, decision of 22 December 2020, W258 2225293-1, available at https://ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20201222_W258_2225293_1_00/BVWGT_20201222_W258_2225293_1_00.pdf.

Furthermore, a DSB decision[332] was published which dealt with an aid and rescue association losing a booklet containing personal health data.

b) The notion of a "personal data breach"

There is no specific definition or interpretation of the notion of a "personal data breach" in Austria. The DSB guideline refers to the EDPB Guidelines of Examples regarding Personal Data Breach Notification.[333]

c) Where to notify?

According to Art. 33 (1) GDPR, the data breach must be reported to the competent supervisory authority. In Austria, for data breaches of private companies, the competent supervisory authority is the DSB. The DSB is an independent authority that serves as national data protection authority according to Art. 51 GDPR.[334] Thus, its competence includes the enforcement of Art. 33 GDPR.

In 2021, the DSB received 1,169 data breach notifications. In 2020 and 2019, the corresponding figures were 860 and 923, respectively.[335]

d) Design of the notification

aa) Format of the notification

While the DSB does not state explicitly in what form notifications can be made, it does state for a number of other submissions that they can be made by mail or by e-mail.[336] Considering this in conjunction with the fact that DSB forms must be signed either by hand or electronically,[337] it is understood that the data breach notification can also be submitted by mail or by e-mail.[338] An Austrian GDPR commentary states – albeit without reference – that the DSB also accepts notifications by fax, notably if the e-mail system is not working.[339] It states likewise that a notification in person or by phone fulfils the GDPR requirements as well, but does not comment on whether the DSB accepts such notifications.[340]

---

332 DSB, decision of 8 August 2018, DSB-D084.133/0002-DSB/2018, available at https://ris.bka.gv.at/Dokumente/Dsk/DSBT_20180808_DSB_D084_133_0002_DSB_2018_00/DSBT_20180808_DSB_D084_133_0002_DSB_2018_00.pdf.

333 DSB Guideline, p. 17.

334 §§ 18, 19 DSG.

335 Datenschutzbericht 2021 p. 9, available at https://www.dsb.gv.at/dam/jcr:1360e98b-d22a-4a49-b3bd-6afca2f86d4c/Datenschutzbericht_2021.pdf.

336 https://www.dsb.gv.at/aufgaben-taetigkeiten/rechte-der-betroffenen.html.

337 https://www.dsb.gv.at/download-links/dokumente.html.

338 Likewise Jahnel, Kommentar zur Datenschutz-Grundverordnung (2020), Art. 33, para. 29.

339 König/Schaupp, in Knyrim (Hrsg.), Der DatKomm, Art. 33 GDPR, para. 43/2.

340 König/Schaupp, in Knyrim (Hrsg.), Der DatKomm, Art. 33 GDPR, para. 43/2.

The use of the data breach notification form is not mandatory, but the DSB considers the forms "useful".[341]

bb) Language of the notification

The notification form is bilingual (German and English), which suggests that the notification can be made in either language. However, the DSB has stated on various occasions that the English translation of forms only serves international cooperation[342] and that in its proceedings, it will only accept documents in German because by constitutional law[343], German is Austria's official language[344].

e) Information to be included in the notification

aa) Required information

The DSB requires the following information to be included in the notification:

- the contact details of the controller affected by the breach (name, postal address and e-mail address),
- the contact details of the data protection officer unless they are identical to that of the controller (name, postal address and e-mail address),
- a description of the personal data breach,
- a categorisation of the personal data breach as breach of confidentiality, breach of integrity or breach of availability (checkbox),
- the categories of the affected data subjects (customers, employees, patients, children etc.),
- the approximate number of affected data subjects,
- the categories of data (purchased products, health data, banking data, political opinion etc.) and the approximate number of data records involved,
- the time at which the breach took place,
- the time at which the breach became known,
- a description of the most likely consequences of the data breach for the data subjects (exposure, discrimination, financial loss, liability towards customers, identity theft),

341 https://www.dsb.gv.at/download-links/dokumente.html.

342 https://www.dsb.gv.at/aufgaben-taetigkeiten/rechte-der-betroffenen.html.

343 Art. 8 of the Federal Constitutional Law, available at https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1930_1/ERV_1930_1.pdf.

344 DSB guideline, p. 44; Datenschutzbericht 2018, p. 16; Datenschutzbericht 2019, p. 14; Datenschutzbericht 2020, p. 15; Datenschutzbericht 2021, p. 14. All annual reports are available at https://www.dsb.gv.at/download-links/dokumente.html.

- the measures that have been taken to address the personal data breach and
- the measures that have been taken to mitigate the possible adverse effects.

The following information must be included, if applicable:

- the reasons for the delay if the notification was not made within 72 hours since the data breach became known,
- information on whether the data are processed jointly with another controller and, if so, the contact details of the other controller[345] (name, postal address and e-mail address),
- information on whether the data are processed by a processor and, if so, the contact details of the processor (name, postal address and e-mail address),
- another contact point for information (name, postal address, function and e-mail address) and
- any attachments.

As mentioned above,[346] the DSB had to decide on a case in which an Austrian aid and rescue association had lost the so-called Suchtgiftbuch, a booklet documenting who received what quantity of which narcotic substance. After receiving the data breach notification, the DSB requested that the aid and rescue association supplement information on whether the data subjects concerned had been informed and, if not, why; on which measures were taken to ensure that the data contained in the Suchtgiftbuch were processed in such a way as to ensure an appropriate degree of security for personal data and which measures had been taken to address the data breach resp. to mitigate its possible adverse effects. Specifically, the DSB asked whether the loss had been reported and whether there was a copy or an electronic version of the Suchtgiftbuch.

bb) Optional information

The following information may be included:

- if the above-mentioned information cannot be provided yet, this can be indicated by checking a box, thereby also declaring that the information will be provided in phases without undue further delay.

345 The form itself merely provides an open text box, but we understand this to mean that the contact details of the joint controller must be provided.

346 DSB, decision of 8 August 2018, DSB-D084.133/0002-DSB/2018, available at https://ris.bka.gv.at/Dokumente/Dsk/DSBT_20180808_DSB_D084_133_0002_DSB_2018_00/DSBT_20180808_DSB_D084_133_0002_DSB_2018_00.pdf.

f) Timeline of the notification

The DSB guideline merely repeats the GDPR and states that the notification must be made without undue delay and, where feasible, not later than 72 hours after becoming aware of the data breach.[347] According to the notification form, if more than 72 hours have passed since the data breach became known, reasons for the delay must be given. Furthermore, if the information required in the form cannot be submitted at the time of notification, it is to be provided in phases without further delay.

g) Exemptions from the duty to report a personal data breach to the supervisory authority

A DSB newsletter[348] lists the following cases in which a data breach notification is not required:

- only corporations' data are affected,
- data are processed by natural persons exclusively for personal or family reasons (for example, a mobile phone with personal contacts is lost),
- a risk to the rights and freedoms of natural persons is unlikely.

The newsletter further states that it is difficult to discern in which cases the third point will be applicable and that it is thus recommendable to submit a notification in case of doubt.

h) Other documentation duties (Art. 33 (5) GDPR)

There are no specific provisions or guidance regarding other documentation duties under Art. 33 GDPR.

3. France

a) Relevant national legal and other sources

aa) Relevant national legislation

There are no specific legislative powers responsible for the legal implementation of Art. 33 GDPR in France.

In France, Art. 58 of the French Act on data processing, data files and individual liberties provides that the controller shall notify the CNIL and communicate to the data subject any personal data breach pursuant to Art. 33 and 34 GDPR.[349]

347 DSB guideline, p. 46.

348 DSB Newsletter 4/2018, available at https://www.dsb.gv.at/download-links/dokumente.html.

349 Art. 58, French Act No 78-17 of 6 January 1978 on data processing, data files and individual liberties, ibid.

In addition, Art. 226–16 to 226–24 of the French Criminal Code[350] deal specifically with violations of personal rights resulting from computer files or processing.

More specifically, Art. 226-17-1 of the French Criminal Code[351] states that the failure, for an electronic communications service provider or controller, to comply with the notification obligation of Art. 33 GDPR is punishable by five years' imprisonment and a 300,000 euros fine.

Moreover, in case of data breaches, other national legislation might apply which requires additional notifications to other French authorities[352], depending on the activity of the controller concerned.[353]

French Criminal Code states significant sanctions in case of data breach

bb) Guidance from the French public authorities

As is the case for the enforcement of Art. 30 GDPR, the CNIL is responsible for the enforcement of Art. 33 GDPR in France.

The CNIL provides the following documents on Art. 33 GDPR:

- an official online form in French for the notification of data breaches to the CNIL according to Art. 33 GDPR, available on the CNIL's website[354], and
- guidelines regarding the implementation of Art. 33 GDPR.[355]

In a recent report dated 7 September 2022[356], the French Ministry of Economy, Finance and Industrial and Digital Sovereignty proposed the reimbursement of the ransom by the insurer,

350 Art. 226-26 to 226-34 of the French Criminal Code, available only in French at https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006165313/#LEGISCTA000006165313.

351 Art. 226-17-1 of the French Criminal Code, available only in French at https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037825500/.

352 For example, the Agence Régionale de Santé (Regional Health Agency, ARS) or the Agence Nationale de la Sécurité des Systèmes d'Information (French National Cybersecurity Agency, ANSSI).

353 See e.g. Art. L. 1111-8-2 of the French Public Health Code (notification form available at https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/choixSignalementPS), Art. R. 1332-41-10 of the French Defence Code (notification form available at https://www.ssi.gouv.fr/uploads/2016/04/formulaire-declaration-incident-lpm_anssi.pdf), Art. 11 of French Decree No 2018-384 of 23 May 2018 on the security of networks and information systems of Essential Service Operators and Digital Service Providers (notification form available at https://www.ssi.gouv.fr/uploads/2018/05/formulaire-incidents-ose_anssi.pdf) and Art. 20 of the same Decree (notification form available at https://www.ssi.gouv.fr/uploads/2018/05/formulaire-incidents-fsn_anssi.pdf).

354 The online form is available at https://notifications.cnil.fr/notifications/index.

355 Guidelines from the CNIL, available only in French at https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles and https://www.cnil.fr/fr/les-violations-de-donnees-personnelles.

356 This report was rendered within the debates surrounded by the draft orientation and programming act of the French Ministry of the Interior which was adopted at first reading by the French Senate on 18 October 2022.

in the event of a ransomware attack, as soon as the victim has filed a criminal complaint within 48 hours before the competent French judiciary authorities[357].

cc) Relevant national case law

Currently, only one national case on the implementation and enforcement of Art. 33 GDPR has been identified.

In a decision rendered on 22 July 2022, the French Council of State ("Conseil d'Etat") revised two CNIL decisions condemning controllers for a breach of Art. 33 GDPR[358] and considered that the controller's obligation to notify the CNIL of a personal data breach likely to pose a risk to the rights and freedoms of individuals does not apply if the CNIL itself has informed the controller of the breach and has initiated its proceeding on the basis of information brought to its attention elsewhere.[359]

b) The notion of a "personal data breach"

The CNIL uses part of the definition given by Art. 4 GDPR. Thus, a security breach is characterised by the accidental of unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. A security breach is any security incident, whether malware or not and whether intentional or unintentional, that results in the compromise of the integrity, confidentiality or availability of personal data.[360]

The CNIL provides the following examples:

- accidental deletion of medical data stored by a health care institution and not otherwise backed up,
- loss of an unsecured USB key containing a copy of a company's customer database,
- malware introduction into school database and modification of the results obtained by the students.

357 Report of the Ministry of Economy, Finance and Industrial and Digital Sovereignty, "The development of cyber insurance", p. 28, published on 7 September 2022, available only in French at https://medias.vie-publique.fr/data_storage_s3/rapport/pdf/286216.pdf.

358 CNIL's deliberations No SAN-2020-014 and SAN-2020-015 dated 7 December 2020, available only in French respectively at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042675720 and https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042676787.

359 Decision of the French Council of State (Conseil d'Etat), No 449694, 22 July 2022, available only in French at https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-07-22/449694.

360 Definition available only in French at https://www.cnil.fr/fr/definition/violation-de-donnees.

c) Where to notify?

According to Art. 33 (1) GDPR, controllers[361] must notify data breaches to the competent supervisory authority.

In France, for data breaches of private companies, the competent supervisory authority is the CNIL.[362]

d) Design of the notification

aa) Format of the notification

The notification according to Art. 33 GDPR is only possible online via the CNIL's teleservices dedicated to controllers (private or public organisations) wishing to notify the CNIL of a breach affecting the personal data they process.[363]

This specific format is mandatory and the online form must be used.[364]

bb) Language of the notification

The CNIL does not give guidelines on language, but as the form is in French and its use is mandatory, the notification shall be made in French.

e) Information to be included in the notification

aa) Required information

In France, the controller may choose between a complete notification or a preliminary notification, depending on the information in its possession at the time of notification.

In a complete notification, all questions must be answered definitively. In a preliminary notification, the whole form must be filled out but the answers can be completed or modified later by a complementary or modified notification.

The CNIL requires the following information to be included in the notification:

---

361 For the sake of completeness, it should be noted that affected individuals can also notify a personal data breach to the CNIL through the CNIL's online complaint service, which is available only in French at https://www.cnil.fr/fr/plaintes. As the possibility to lodge complaints arises from other provisions of the GDPR and is not regulated in Art. 33, complaints by individuals will not be further addressed in this study.

362 However, depending on the activity of the controller, additional notifications to other French Authorities arising from other legislation than the GDPR might be necessary, see the CNIL guidance on such additional notification duties (only in French), available at https://www.cnil.fr/fr/notifications-dincidents-de-securite-aux-autorites-de-regulation-comment-sorganiser-et-qui-sadresser, and fn. 353 above.

363 Guidelines from the CNIL, available only in French at https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles.

364 https://notifications.cnil.fr/notifications/index.

- the identification of the organisation (SIREN code[365]/identification number),
- the contact details of the controller affected by the breach (name of the organisation, postal address, intracommunity VAT number, ZIP code, city, country, sector of activity, number of employees),
- a person to contact for more information (civility, surname, first name, phone number, e-mail address, function, postal address, ZIP code, city, country),
- other organisations involved (name and quality of the third-party organisations),
- the date of the breach (date and time of violation, date and time of start of violation, date and time of end of violation, date and time of awareness of violation, date and time of notification by provider, violation over a definite or indefinite period of time, whether violation is still ongoing); after responding, the controller may comment on the dates, explain the circumstances of the discovery of the breach and state the reasons for the delay if applicable,
- the nature of the violation (multiple-choice item in the form: loss of confidentiality, loss of integrity, loss of availability),
- the origin of the incident (multiple-choice item in the form: lost or stolen equipment, paper lost, stolen or left accessible in an unsecured location, mail lost or opened before being returned to sender, hacking, malware and/or phishing, disposal of digital devices containing personal data without secure deletion, involuntary publication of information, wrong person's data posted on customer portal, personal data sent to wrong recipient, personal information disclosed verbally, other origin); after choosing, the controller must make a detailed description of the violation,
- the cause of the incident (multiple-choice item in the form: internal malware act, internal accidental act, external malware act, external accidental act, unknown, other causes),
- the nature of the data affected by the breach (multiple-choice item in the form: civil status, registration number, contact details, identification or access data, data relating to financial or economic information, official documents, location data, data relating to offences, convictions, security measures, the data concerned are currently unknown, the breach concerns other data),
- any sensitive data affected (multiple-choice item in the form: racial or ethnic origin, political opinions, philosophical or religious views, trade union membership, sexual orientation, health data, biometric data, genetic data),
- the approximate number of records affected by the breach,

365 The SIREN code is the identification number granted to registered legal entities.

- the categories of persons affected by the breach (multiple-choice item in the form: employees, users, members, students/pupils, military personnel, customers (current or potential), patients, minors, vulnerable persons, not determined at this time, other persons),
- the approximate number of data subjects affected by the breach,
- the controller's pre-breach security measures,
- the measures taken to remedy the violation and, if applicable, the measures to mitigate any negative consequences,
- the potential consequences of a loss of confidentiality (multiple-choice item in the form: data have been disseminated more than necessary and have escaped the control of the data subjects, data may be correlated with other information on the data subjects, data may be used for purposes other than those intended and/or in an unfair manner, other consequences related to loss of confidentiality),
- the potential consequences of a loss of integrity (multiple-choice item in the form: data may have been modified and used when it is not true, data may have been modified into other validated data in such a way that processing is hijacked, other consequences related to the loss of integrity),
- the potential consequences of a loss of availability (multiple-choice item in the form: inability to provide a critical service, malfunction and difficulty in providing a critical service, other consequences related to loss of availability),
- the nature of potential impacts on people (multiple-choice item in the form: loss of control over their personal data, limitation of their rights, discrimination, identity theft, fraud, unauthorised lifting of pseudonymisation, financial losses, damage to reputation, loss of confidentiality of data protected by a professional secret, other impacts),
- an estimation of the level of severity (multiple-choice item in the form: negligible, limited, important, maximum),
- a specification as to whether data subjects have been informed (multiple-choice item in the form: yes, data subjects have been informed / no, but they will be / no, they will not be / not determined for the moment),
- a specification as to whether the notification concerns cross-border processing targeting persons from different Member States,
- a specification as to whether the breach has been or will be notified to another European DPA,

- a specification as to whether the violation has been or will be reported to another authority to comply with another legal requirement (NIS[366], EIDAS[367] etc.).

All information must be listed in the online form provided by the CNIL. The processor need only select its answer or to fill in the respective text field.[368]

bb) Optional information

The CNIL's online form available for a notification does not contain spaces for optional information. Controllers must tick the checkboxes and fill in the necessary text fields in the online form. Sometimes, the controller will not have an answer to give, for example, if there are no other organisations involved, and it will be enough to leave the square blank.

f) Timeline of the notification

According to the CNIL[369], the notification must be transmitted to the CNIL as soon as possible following the discovery of a violation presenting a risk to the rights and freedoms of individuals. Controllers that are unable to provide all the information required within the 72-hour timeframe because they need to make further investigations may proceed with a notification in two stages[370]:

- an initial notification within 72 hours from the discovery of the breach, if possible; if the 72-hour deadline is exceeded, the controller must explain the reasons for the delay,
- a supplementary notification as soon as additional information is available.

g) Exemptions from the duty to notify a personal data breach to the supervisory authority

According to the CNIL, the risk assessment is made on a case-by-case basis by the controller and must take into account various elements[371]:

366 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

367 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.

368 Official form to complete to notify a breach to the CNIL, available only in French at https://notifications.cnil.fr/notifications/index.

369 See the guidance at the CNIL website available only in French at https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles.

370 See also the options in the online form, https://notifications.cnil.fr/notifications/index, and the information given in Chapter IV. 3. e) aa) above.

371 Guidelines from the CNIL available only in French at https://www.cnil.fr/fr/les-violations-de-donnees-personnelles.

- the type of breach (affecting data integrity, confidentiality or availability),
- the nature, sensitivity and volume of personal data involved,
- the ease of identifying the individuals affected by the breach,
- the possible consequences of the breach for individuals,
- the characteristics of those individuals (children, vulnerable individuals etc.),
- the volume of individuals affected and
- the characteristics of the controller (nature, role, activities).

The CNIL provides various examples of situations in which there is no risk justifying a notification to the CNIL or to the persons concerned by the breach:

- the disclosure of data already made public,
- the deletion of data saved and immediately restored,
- the loss of data protected by an encryption key if the encryption key has not been compromised and if a copy of the data remains available.

h) Other documentation duties (Art. 33 (5) GDPR)

There are no specific provisions or guidance on the documentation of data breaches in France that deviate from or go beyond the guidance given by the EDPB.

However, the CNIL recommends that controllers list all elements related to data breaches in a record. According to the CNIL, such a record of violations should include the following information:

- the nature of the violation,
- the categories and approximate number of individuals involved,
- the categories and approximate number of records involved,
- the likely consequences of the breach,
- the steps taken to remedy the breach and, where appropriate, to limit the adverse consequences of the breach,
- if applicable, the justification for not notifying the CNIL or informing the persons concerned.

4. Germany

a) Relevant national legal and other sources

aa) Relevant national legislation

German law does not entail specific provisions on the content of the notification of data breaches within the scope of application of the GDPR. As stated above[372], data protection in Germany is primarily governed by the GDPR as directly applicable EU law. There is still a national data protection law, in particular the BDSG[373] on the federal level and the state data protection acts of the individual federal states, for example, the State Data Protection Act of Baden-Württemberg (LDSG-BW).[374] However, as Art. 33 GDPR does not provide for a specific opening clause for the Member States, neither the BDSG nor the LDSG-BW regulate further details concerning the obligations to report and document personal data breaches under the GDPR.[375] There is also no relevant secondary legislation.

However, Sections 42 (4) and 43 (4) BDSG regulate an additional prohibition to use a notification pursuant to Art. 33 GDPR in criminal proceedings or in proceedings under the Code of Administrative Offences against the notifying person or the person responsible for the notification with the controller without the consent of that person.[376] This prohibition is based on the "nemo-tenetur" principle[377] (reflecting the rights against self-incrimination and forced inculpation). It does, however, not apply to the field of civil procedure.

From the above, it follows that there is no relevant specific German primary or secondary legislation governing, clarifying or derogating from the obligations to report and/or document personal data breaches to the competent supervisory authority. Insofar, Art. 33 GDPR applies.

bb) Guidance from the German public authorities

As mentioned above[378], data protection supervision in Germany is split between DPAs on the federal level (mainly the BfDI in Bonn) and the DPAs on the level of the 16 federal states.

---

372 See above Section A. III. 4. a) for further details on the structure of the German data protection law.

373 Federal Data Protection Act (Bundesdatenschutzgesetz) of 30 June 2017 (fn. 107).

374 Landesdatenschutzgesetz Baden-Württemberg (LDSG-BW) of 12 June 2018 (fn. 110). As stated above in Section A. III. 4. a), the LDSG-BW mainly applies to the processing of personal data by public bodies and not by private companies.

375 To avoid any misunderstandings, it should be mentioned here that the BDSG indeed does contain a provision which regulates the notification of data breaches to the BfDI as the competent supervisory authority in its Section 65. However, this provision is an implementing provision which transposes Directive 2016/680 and thus only applies to the processing of personal data by the police and criminal justice authorities.

376 Section 42 (4), 43 (4) BDSG.

377 The principle that no one may be forced to incriminate themselves (nemo tenetur se ipsum accusare) is one of the recognised principles of criminal proceedings under the rule of law, cf. e.g German Federal Constitutional Court (BVerfG), decision of 27 April 2010, 2 BVL 13/07, ECLI:DE:BVerfG:2010:lk20100427.2bvl001307, No 2 with further references.

378 See Section III. 4.) a) cc) above.

Within the scope of application of the GDPR[379], for companies providing telecommunications or postal services, the competent supervisory authority is the BfDI.[380] For all other companies that are not subject to the exclusive jurisdiction of the BfDI – and thus for the majority of companies in the private sector – the supervisory authorities of the Länder are competent.[381]

If the controller or processor has more than one establishment in Germany, the competent DPA is the authority of the federal state ("Land") in which the controller's or processor's central administration is based (unless another establishment must be considered their main establishment).[382] Therefore, for private entities which have their sole establishment or their central administration (main establishment) in Baden-Württemberg, the competent supervisory authority within the meaning of the GDPR is the data protection commissioner of Baden-Württemberg (Landesbeauftragter für Datenschutz und Informationsfreiheit (LfDI)) in Stuttgart (hereinafter referred to as "LfDI Baden-Württemberg").[383]

As mentioned above[384], the LfDI Baden-Württemberg, the other independent DPAs of the Länder and the BfDI have joined together in the so-called Data Protection Conference (Datenschutzkonferenz, hereinafter referred to as "DSK")[385] to coordinate their work. The DSK's guidance applies subject to a different (future) view of the EDPB.

(1) The BfDI

The BfDI has issued the following documents related to Art. 33 GDPR:

---

379 The GDPR is in particular applicable for general personal data of natural persons, in particular inventory data, with regard to which the German Telecommunications Act (TKG) does not contain any sector-specific data protection regulations adopted in the implementation of Directive 2002/58/EC on privacy and electronic communications, cf. Art. 95 GDPR. The TKG, which transposes Directive 2002/58/EC into German law, also contains a notification duty in case of personal data breaches within the scope of the TKG. In cases where the same data breach affects only or also data falling under the specific rules in the TKG, the service provider must report the breach not only to the BfDI, but also to the Federal Network Agency (Bundesnetzagentur), cf. https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Unternehmenspflichten/Datenschutz/Datenschutzverletzungenmelden/start.html.

380 Section 29 of the German Telecommunications and Telemedia Data Protection Act of 21 June 2021 (TTDSG), available at https://www.gesetze-im-internet.de/ttdsg/, and Section 9 (1) BDSG. The BfDI is an autonomous and independent supreme federal authority tasked inter alia with enforcing the GDPR within its competences, cf. https://www.bfdi.bund.de/EN/DerBfDI/UeberUns/DieBehoerde/diebehoerde_node.html.

381 According to Section 40 (1) BDSG, the authorities pursuant to the law of the Länder shall monitor the application of data protection legislation by private bodies within the scope of the GDPR. See also https://www.bfdi.bund.de/EN/Buerger/Inhalte/Allgemein/Datenschutz/Zuständigkeit-BfDI.html. All in all, the state data protection authorities of the Länder are authorised to supervise the data protection law compliance of public bodies of the respective Land and of all non-public bodies whose main establishment is established in this Land and that are not subject to the exclusive jurisdiction of the BfDI.

382 Section 40 (2) 1 BDSG, Art. 4 No 16 GDPR.

383 Section 40 (1), (2) BDSG, Art. 4 No 16 GDPR, Section 25 (1) LDSG-BW. Other relevant special provisions which provide for a different competence are not identifiable here. The website of the LfDI Baden-Württemberg is available at https://www.baden-wuerttemberg.datenschutz.de/.

384 See above Chapter A. III. 4. a).

385 For more information on the DSK see also fn.118 above.

- an information sheet "data breach notifications"[386] and
- an online form[387] for reporting data breaches. Bodies supervised by the BfDI may report data protection violations using this online form.

(2) The DSK

The DSK (composed of the BfDI and the DPAs of the Länder) has issued the following documents related to Art. 33 GDPR:

- Short Paper No 18[388] on risks to the rights and freedoms of natural persons. This paper intends to provide an orientation on how the GDPR should be applied in practical enforcement. It aims to define the term "risk" – which is also used in Art. 33 – in the context of the GDPR and to show how risks to the rights and freedoms of natural persons can be determined and assessed in relation to their legal consequences[389], and
- the Experience Report[390] of 2019 on the application of the GDPR, which also contains statements of the DSK on Art. 33 GDPR.

(3) The LfDI Baden-Württemberg

The LfDI Baden-Württemberg provides the following forms and guidance:

- on its website, the LfDI Baden-Württemberg provides an online form[391] for controllers to directly report personal data breaches to the LfDI. The online form includes a functionality to print out the notification before sending it. It is, however, not mandatory to use the online form; other forms of notification are still possible,[392]

386 Infoblatt BfDI „Meldung von Datenschutzverstößen" of 18 May 2018, available https://www.bfdi.bund.de/DE/Service/Datenschutzverstoesse/Infoblatt_Datenschutzverstoesse.html.

387 The BfDI's online form is available at the BfDI's website at https://formulare.bfdi.bund.de/lip/form/display.do?%24context=15B94DB8E5D9616D42CC.

388 DSK, Kurzpapier Nr. 18 – Risiko für die Rechte und Freiheiten natürlicher Personen of 26 April 2018, available at https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.

389 DSK, Kurzpapier Nr. 18, ibid., p. 1.

390 Experience Report (Erfahrungsbericht) of the DSK on the application of the GDPR of 6 November 2019, available at https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKBeschluessePositionspapiere/98DSK_Erfahrungsbericht-DSGVO-Anwendung.html.

391 The online form for data breach notification is available at https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/.

392 For more details see Section A. IV. 2. D) aa) below.

- for help on the individual input fields of the online form, the LfDI Baden-Württemberg refers to the document "Meldung einer Datenpanne nach Art. 33, 34 EU-DSGVO"[393] (hereinafter: "auxiliary document"), which contains a table with more details on what must and what may be entered in the fields of the online form,
- beyond this, the website of the LfDI Baden-Württemberg includes a data protection notice[394] with regard to the notification of data breaches which also indicates some details around the notification and the data processing by the LfDI in this context,
- the website of the LfDI Baden-Württemberg also provides a hyperlink to the Working Paper 250[395] endorsed by the EDPB.

cc) Relevant national case law

There are some court decisions of mostly lower courts that mention or marginally deal with the obligations under Art. 33 GDPR or explain their purposes[396]. In most cases, Art. 33 was not the focus of these decisions. Hardly any decisions provide selective indications for the interpretation of Art. 33. For example, the Regional Labour Court (Landesarbeitsgericht) of Schleswig-Holstein has taken a position on the format of the notification.[397]

Of the administrative proceedings initiated by the LfDI Baden-Württemberg in data breach cases, inter alia the following has become known:

393 Meldung einer Datenpanne nach Art. 33, 34 EU-DSGVO, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Meldeformular-Datenpanne-Eingabefelder.pdf.

394 The data protection notice of the LfDI Baden-Württemberg is available at https://www.baden-wuerttemberg.datenschutz.de/meldung-von-datenpannen/.

395 Art. 29 Working Party, WP 250 – Guidelines on personal data breaches (fn. 28), replaced in October 2022 by the EDPB Guidelines 09/2022 (fn. 259).

396 For example, the Regional Court of Essen assumed in its judgment of 23 September 2021, court ref. No 6 O 190/21, a violation of Art. 33 due to a failure to report a data breach, without, however, dealing in detail with the necessary content or the necessity of the notification, cf. openJur 2021, 32607, available at https://openjur.de/u/2362644.html; beyond this, the Fiscal Court of Berlin-Brandenburg in its judgment of 26 January 2022, court ref. No 16 K 2059/21, openjur 2022, 7472, available at https://openjur.de/u/2393347.html, stated that the purpose of the notification duty is to minimise the negative effects of the data breach, to preventively protect individuals by setting incentives for the controller to avoid future violations and to enable the DPA to decide on measures to contain and punish the infringement (No 231).

397 Regional Labour Court of Schleswig-Holstein, decision of 6 August 2019, court ref. No 2 TaBV 9/19, available at https://www.iww.de/quellenmaterial/id/211754. This decision will be addressed below (cf. Section A. IV. 4. d) aa.).

German case law: hacked social media platform had to pay a fine for data breach

- in 2018, the chat portal Knuddels.de had to pay a fine of 20,000 euros due to a data breach. The operator of the social media platform had become victim of a hacker attack in which data from 330,000 users consisting of pseudonyms, passwords and e-mail addresses were captured and published. In the proceedings, the LfDI Baden-Württemberg mitigated the fine because the operator himself had reported the data breach and subsequently cooperated extensively with the authority so that the facts could quickly be clarified.[398] The fine became known as the first fine imposed by the LfDI Baden-Württemberg under the GDPR.[399]
- Another case which was reported in the press concerned a data breach at the association Junge Liberale Baden-Württemberg e.V. in April 2022.[400] The chairman of this association had – by mistake – sent an e-mail invitation to a meeting of members of the association which included an excel file containing further sheets with personal data of about 1,000 data subjects. The breach was reported and the LfDI Baden-Württemberg opened a procedure. Due to the number of persons affected and the particular sensitivity of the data concerned (membership of a political association), the case was submitted to the Fines Office at the State Commissioner for examination. However, as the data breach was due to human error, the data were not publicly accessible and the association in which all responsible persons work on a voluntary basis had taken further measures to prevent similar incidents and protect personal data, it was determined that it was not necessary to initiate proceedings for a fine. Thus, the LfDI Baden-Württemberg closed the case.

b) The notion of a "personal data breach"

As far as can be seen, the German data protection authorities do not have an understanding of the notion of a "personal data breach" which would deviate from the above-mentioned interpretation by the EDPB.

c) Where to notify?

According to Art. 33 (1) GDPR, the data breach must be reported to the competent supervisory authority within the meaning of Art. 51 and 55 GDPR. In Germany, within the scope of application of the GDPR, private companies which are subject to the exclusive jurisdiction of the BfDI must report data breaches to the BfDI. All other private companies must report data breaches to the supervisory authority of the federal state ("Land") in which their sole or main establishment (central administration) is based.[401] Therefore, companies having their sole or

398 LfDI, press release of 18 November 2018, available at https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/.

399 https://www.lto.de/recht/nachrichten/n/knuddels-datenschutz-hacker-bussgeld-kooperation/.

400 https://www.baden-wuerttemberg.datenschutz.de/pruefung-abgeschlossen/.

401 Unless another establishment must be considered their main establishment; see above A. IV. 4. a) bb), Section 40 (2) 1 BDSG, Art. 4 No 16 GDPR.

main establishment in Baden-Württemberg must report data breaches to the LfDI Baden-Württemberg as the authority competent for them.[402]

In 2021, the LfDI Baden-Württemberg received more data breach notifications than ever before.[403]

Table 20: Statistical overview of data breaches – period in each year from 1 January to 31 December

Year	2016	2017	2018	2019	2020	2021
Number of data breaches	68	121	900	2,030	2,321	3,136

Source: LfDI, activity report of 2021.[404]

d) Design of the notification

aa) Format of the notification

Notifications to the BfDI can be made via an electronic form on the BfDI's[405] website, notifications to the LfDI Baden-Württemberg via an electronic form on the LfDI Baden-Württemberg's website.[406] Alternatively[407], the notification to the LfDI Baden-Württemberg can be made via e-mail or phone. However, the vast majority of companies in Baden-Württemberg use the online form to report data breaches to the LfDI Baden-Württemberg.

The Regional Labour Court (Landesarbeitsgericht) of Schleswig-Holstein has stated in a decision of 6 August 2019[408] that it cannot be inferred from the provisions of the GDPR that a data breach notification must be necessarily made by e-mail because other notification channels are also conceivable, for example, notification by phone, orally or by SMS.

---

402 See above A. IV. 4. a) bb), Section 40 (1), (2) BDSG, Art. 51, 55, 4 No 16 GDPR, Section 25 (1) LDSG-BW.

403 37th activity report (Tätigkeitsbericht) of the LfDI Baden-Württemberg 2021, p. 120, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/02/22020225_Taetigkeitsbericht_TB-Datenschutz_2021_V1.pdf.

404 37th activity report (Tätigkeitsbericht) of the LfDI Baden-Württemberg 2021, p. 120, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/02/22020225_Taetigkeitsbericht_TB-Datenschutz_2021_V1.pdf.

405 The online form of the BfDI is available on the BfDI's website at https://formulare.bfdi.bund.de/lip/form/display.do?%24context=15B94DB8E5D9616D42CC.

406 Website of the LfDI, available at https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/.

407 See also the data protection notice on the website of the LfDI Baden-Württemberg, available at https://www.baden-wuerttemberg.datenschutz.de/meldung-von-datenpannen/, which allows for alternative notification methods ("We do not work with processors when you report your data breach. This does not apply if you submit your notification using the online notification form").

408 Regional Labour Court of Schleswig-Holstein, decision of 6 August 2019, court ref. No 2 TaBV 9/19, available at https://www.iww.de/quellenmaterial/id/211754.

bb) Language of the notification

As the official language for communicating with German authorities is German[409] and the online forms of the BfDI and the LfDI Baden-Württemberg are written in German, it can be assumed that in Germany, the notifications must generally be made in German. At the very least, the company must be able to submit a German translation of the notification upon request by the DPA without delay.[410]

e) Information to be included in the notification

aa) Required information

As the majority of the companies based in Baden-Württemberg must report data breaches to the LfDI Baden-Württemberg and not to the BfDI, the following presentation is limited to the information that companies must provide when reporting a data breach to the LfDI Baden-Württemberg. According to the online form[411] on the website of the LfDI Baden-Württemberg and the guidance given by the latter, the following information must be included in the notification:

- the name and the address (street, house number, postcode, town) of the controller,
- the name of the person who makes the notification to the DPA,
- the function which the person making the notification holds with the controller,
- the e-mail address of the person making the notification,
- the phone number of the person making the notification,
- under "what has happened",
  - a description of the incident as precise as possible[412], including answers to the following questions:
    - Where did the incident happen?
    - Who was involved?
    - How did you learn about it?
    - Has the responsible organisation already been informed?
    - Which third parties have become aware or have had the opportunity to become aware[413]?

409 See Section 23 (1) of the German Administrative Procedure Act (VwVfG).

410 See Section 23 (2) of the German Administrative Procedure Act (VwVfG).

411 See fn. 391.

412 The LfDI's online form for the notification contains text boxes in which the respective information can be inserted.

413 In German: "Welche Dritte haben Kenntnis erlangt oder hatten die Möglichkeit zur Kenntnisnahme?".

- the time of the incident, meaning the date on which the data breach occurred,
- the time of knowledge of the incident, meaning the point at which the controller became aware of the data breach or was informed of it,
- the types of data affected, for example, employee data, customer data, bank details, health data,
- (not included in the online form of the LfDI Baden-Württemberg, but required according to the auxiliary document[414] to which the LfDI refers): the (at least approximate) number of personal data sets affected,
- the number of affected data subjects; if the number cannot be determined precisely, an estimated upper limit of affected persons,
- a risk assessment, including a list of the probable or already occurred adverse consequences for the affected data subjects which the controller considers likely to occur, for example, unauthorised account debits, identity theft, damage to reputation/image, threat to livelihood, threat to life, exposure, disclosure of secrets,

- under "what countermeasures have been taken or are proposed by the controller",
  - the countermeasures already taken by the controller and the additional countermeasures planned; according to the auxiliary document to which the LfDI refers, a "detailed explanation" of the countermeasures taken or planned regarding the specific incident and the objective of preventing such incidents in the future is required,
  - an indication of whether the controller considers that it has a duty to notify the affected data subjects (either "yes" or "no" must be ticked in the respective checkbox),
    - if the controller ticks "no", a text box opens and the controller must add a justification for its decision as to why there is no obligation to notify the data subjects in this case,
    - if the controller ticks "yes", a text box opens and the controller must also indicate when and how the affected data subjects have been or will be notified and which specific countermeasures the controller has recommended to them.

bb) Optional information

In Germany, the following information may voluntarily be included in the notification and may, according to the LfDI Baden-Württemberg, be useful for processing depending on the case constellation:

- the website (web address) of the controller,
- under "other communications",

414 See fn. 393.

- an indication as to whether criminal charges have been filed and, if yes, the relevant office and the file number, and
- other notifications/messages to the DPA,

- an indication as to how the controller wishes to be informed about the progress of its notification (mail, e-mail, encryption etc. – not included in the LfDI's online form, but in the guidance document to which the LfDI refers).

In practice, the LfDI Baden-Württemberg might request the submission of further documents by the controller later in the process, for example, the controller's IT forensics report (submission voluntary, but many controllers do submit the information on the technical and organisational measures (TOMs) taken by the controller).

f) Timeline of the notification

The LfDI Baden-Württemberg repeats on its website that controllers are obliged to report data breaches without delay and, if possible, within 72 hours, if an incident has resulted in a risk to the rights of data subjects.[415]

Notifications should, but do not necessarily have to be complete from the outset; information that is not initially available may also be submitted as soon as it is available.

The online notification form of the LfDI Baden-Württemberg and the related guidance on the input fields do not expressly require the controller to give reasons for the delay once the notification is not made within 72 hours. However, the online form contains at the end a text box named "other notifications (messages) to the DPA" in which such reasoning could be inserted.

In a judgment of 31 March 2021[416], the Higher Regional Court of Stuttgart confirmed that in principle, the controller is required to notify the authority within 72 hours, but, according to its own assessment, may refrain from doing so if the breach is "unlikely to result in a risk to the rights and freedoms of natural persons".

415 See the LfDI Baden-Württemberg's data protection notice, available at https://www.baden-wuerttemberg.datenschutz.de/meldung-von-datenpannen/.

416 Higher Regional Court of Stuttgart, judgment of 31 March 2021, court ref. No 9 U 34/21, No 56, openJur 2021, 29387, available at https://openjur.de/u/2354794.html.

g) Exemptions from the duty to notify a personal data breach to the supervisory authority

In its Short Paper No 18[417] on risks to the rights and freedoms of natural persons, the DSK acknowledged that the term "risk" is not defined in the GDPR. In this paper, the DSK deducts from the GDPR that a risk within the meaning of the GDPR is the possibility of the occurrence of an event which itself causes physical, material or immaterial harm or which may lead to further harm to one or more natural persons. According to the paper, a risk has two dimensions: firstly, the severity of the harm, and secondly, the likelihood that the event and the consequential harm will occur.[418] In this paper, the DSK interprets the wording "is unlikely to result in a risk" in Art. 33 GDPR from its meaning and purpose as "leading only to a low risk" because "processing is never completely risk-free". From this, it can be inferred that the controller must assess whether the personal data breach is only likely to lead to a low risk.

DSK Short Paper No 18[419] provides further guidance on how to

- identify the (baseline) risk of data processing, based on objective criteria, taking into account the circumstances of the processing,
- assess the probability of occurrence and severity of possible harms and
- assign the results found to the risk level "low risk"; inter alia, it provides a risk matrix for the risk assessment.

The DSK paper clarifies that ultimately, all conceivable negative consequences for the rights and freedoms of natural persons, their economic, financial and intangible interests, their access to goods or services, their professional and social reputation, their state of health and all their other legitimate interests must be considered. Examples for such consequences given by the DSK are discrimination, identity theft or fraud, financial loss, reputational damage, economic or social disadvantages, impairment of the exercise of rights and prevention of control by data subjects, exclusion or restriction of the exercise of rights and freedoms, profiling through assessment of personal aspects or physical harm resulting from actions based on disclosed data.

As regards the determination of the severity of possible harms, the DSK paper lists some essential factors, including the sensitivity of data, processing of uniquely identifying data, vulnerability of the affected data subjects and the volume of affected individuals.[420]

---

417 DSK, Kurzpapier Nr. 18 – Risiko für die Rechte und Freiheiten natürlicher Personen of 26 April 2018, p. 1, available at https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf. The paper intends to provide a guidance for all risk assessments necessary under the GDPR, not only in Art. 33 but also e.g. in Art. 24, 25, 32, 34, 35, 36 GDPR).

418 DSK, Kurzpapier Nr. 18, ibid., p. 1.

419 DSK, Kurzpapier Nr. 18, ibid., pp. 2–6.

420 DSK, Kurzpapier Nr. 18 (fn. 417), p. 5.

The DSK paper affirms that the statements contained therein are subject to a possible deviating interpretation by the EDPB.[421] However, there is no guidance for controllers on determining whether and to what extent the paper deviates from the later EDPB guidance on Art. 33 GDPR.[422]

h) Other documentation duties (Art. 33 (5) GDPR)

Neither the DSK nor the LfDI Baden-Württemberg provide specific guidance on the documentation of data breaches beyond the notification.

German jurisprudential literature takes the view that due to the accountability principle, the controller must also document the prognosis decision (risk assessment) leading it to the conclusion that the data breach is not likely to result in a risk to the rights and freedoms of natural persons.[423]

5. Italy

a) Relevant national legal and other sources

aa) Relevant national legislation

As stated above,[424] data protection in Italy is primarily governed by the GDPR as directly applicable EU law. Italian law, including the Italian Personal Data Protection Code (Codice della Privacy),[425] does not entail specific provisions on the content of the notification of data breaches within the scope of application of the GDPR.[426]

Italian Data Protection Code: imprisonment in case of wilful provision of false information

The Italian Personal Data Protection Code punishes the wilful provision of false information to the "Garante per la protezione dei dati personali" (hereinafter: Garante) by imprisonment between six months and three years, unless the offence is more serious.[427]

421 DSK, Kurzpapier Nr. 18 (fn. 417), p. 1.

422 On the EDPB guidance, see above Sections A. IV. 1. a) bb). and A. IV. 1. i).

423 Gola, DS-GVO, Commentary, 2nd edition 2018, Art. 33 No 26.

424 See above Section A. III. 5. a) for further details on the structure of the Italian data protection law.

425 An English translation of the Italian Personal Data Protection Code is available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9740796.

426 Italian law contains in Art. 26 Legislative Decree 51/2018 a provision which regulates the notification of data breaches to the Garante. However, this provision is an implementing provision which transposes Directive 2016/680 and thus only applies to the processing of personal data by the police and criminal justice authorities.

427 See Section 168 Italian Personal Data Protection Code.

bb) Guidance from the Italian public authorities

In Italy, the Garante is responsible for the enforcement of Art. 33 GDPR.[428] The Garante provides on its website an online service portal with information and instructions on the procedures to be followed for data breach notifications as required by Art. 33 GDPR.[429] The page contains, inter alia, links to the GDPR and interpretative documents, fact sheets and topic pages and is continuously updated. In particular, the Garante has issued the following guidance documents on Art. 33 GDPR:

- an order of 30 July 2019 on the notification of personal data breaches[430] prescribing that controllers required to report personal data breaches shall provide the Garante with the information required by Art. 33 GDPR according to the modalities in force in the year 2019,
- explanations of terms and concepts related to the notion of a data breach,[431]
- an order of 27 May 2021[432] establishing a new telematic procedure for personal data breach notification (hereinafter: "online notification procedure"),
- the respective official online form for the notification of data breaches under the online notification procedure,[433]
- a fact sheet[434] with instructions on how to use the online notification procedure,
- a facsimile template containing all the information to be included in the various steps of the online notification procedure,[435] and
- a self-assessment tool helping controllers to identify the actions to be taken following a data breach.[436]

cc) Relevant national case law

So far, there have been no rulings in Italian jurisprudence dealing with the obligations under Art. 33 GDPR.

---

428 See Section 2-a Italian Personal Data Protection Code, available at https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9740796. See already Section A. III. 5. a) cc).

429 Violazioni di dati personali (data breach) in base alle previsioni del Regolamento (UE) 2016/679, available at https://www.garanteprivacy.it/regolamentoue/databreach.

430 Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) of 30 July 2019 [9126951]), available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9126951.

431 See https://www.garanteprivacy.it/regolamentoue/databreach.

432 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9667201.

433 https://servizi.gpdp.it/databreach/s/scelta-auth.

434 https://servizi.gpdp.it/databreach/s/istruzioni.

435 The facsimile template is available at https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni.

436 The tool is available at https://servizi.gpdp.it/databreach/s/self-assessment.

Italian authority gives examples for "personal data breach" and definitions in self-assessment procedure form

b) The notion of a "personal data breach"

In the dedicated section of its website,[437] the Garante essentially repeats the definition of a "personal data breach" provided in Art. 4 (12) GDPR, defining a personal data breach as a security breach leading – accidentally or unlawfully – to the destruction, loss, modification, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed which may compromise the confidentiality, integrity or availability of personal data.

The Garante provides the following examples:

- the access or acquisition of data by unauthorised third parties,
- the theft or loss of computer devices containing personal data,
- the deliberate alteration of personal data,
- the inability to access data due to accidental causes or external attacks, viruses, malware etc.,
- the loss or destruction of personal data due to accident, adverse event, fire or other calamity, and
- unauthorised disclosure of personal data.

Furthermore, in its self-assessment procedure form,[438] the Garante defines a personal data breach as a particular type of security incident which, by causing loss of confidentiality, integrity or availability of personal data, causes the data controller to no longer be able to ensure compliance with the principles relating to the processing of personal data.[439] For example, a personal data breach may consist in

- access to personal data by unauthorised third parties,
- loss of confidentiality as a result of sending an e-mail containing personal data to the wrong recipient,
- loss or theft of a device or storage medium containing personal data,
- loss of availability of personal data stored in a database, for example, through ransomware,
- loss of availability of personal data if, for example, such data have been accidentally deleted permanently or made temporarily unavailable due to the interruption of a service.

437 https://www.garanteprivacy.it/regolamentoue/databreach.

438 https://servizi.gpdp.it/databreach/s/self-assessment.

439 See Art. 5 GDPR.

In its self-assessment procedure form, the Garante also defines a security incident as an event (or series of events) of malicious or accidental origin, external or internal to the organisation, that may result in the compromise of data held by an organisation, putting at risk one or more of the three principles of information security: confidentiality, integrity and availability. A security incident may simultaneously affect the confidentiality, integrity or availability of data and information or consist of any combination of these. The Garante provides the following examples: a security incident may occur, for example, as a result of a cyberattack, unlawful or accidental human behaviour, natural disaster, hardware or software malfunction, for example,

- a breach of confidentiality in the event of unauthorised or accidental disclosure of or access to data,
- a breach of integrity in the event of unauthorised or accidental modification of the data,
- a breach of availability in the event of unauthorised or accidental loss or destruction of data.

c) Where to notify?

The controller must notify the Garante of the personal data breach.

In 2021, the Garante received 2,071 data breach notifications.[440] For the years before, the exact figures cannot be clearly indicated as the figures for the previous years published by the Garante are more general and comprise not only data breach notifications but also complaints and other notifications, without indicating how many of them are data breach notifications.[441]

d) Design of the notification

aa) Format of the notification

The notification of a personal data breach must be transmitted via a special online notification procedure to the Garante by means of an online form, available on the Garante's online services portal.[442]

440 See https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9787195.

441 See e.g. https://www.garanteprivacy.it/documents/10160/0/Relazione+annuale+2019.pdf/4fcc5ca8-5ca7-432f-c3f8-4e9e69181a23?version=1.1 (for 2019) and https://www.garanteprivacy.it/documents/10160/0/Relazione+annuale+2020.pdf/286a6332-896a-d4b1-a2da-e32d7d4838c9?version=2.0 (for 2020).

442 The portal is available at https://servizi.gpdp.it/databreach/s/. The portal was established by the order of 27 May 2021 (see Chapter A. IV. 5 c).

The Garante's online service portal contains a fact sheet with instructions on how to use the online notification procedure[443]. The online service portal also offers a facsimile of the form with instructions that must be followed when filling in the online form.[444]

To simplify the requirements for controllers, the Garante has devised and made available a self-assessment tool to help controllers identify the actions to be taken following a personal data breach resulting from a security incident.[445] By means of a small number of questions, the controller is guided in fulfilling the obligations regarding the notification of personal data breaches to the Garante. This tool is to be considered solely an aid to the controller's decision-making process and does not anticipate the Garante's assessment of the potential data breach. The information provided during its use will not be retained.

During the self-assessment procedure, the controller must complete the following steps and answer the following questions:

- Did a security incident occur that resulted in the loss of confidentiality, integrity or availability of data? (yes or no)
- Did the security incident involve personal data? (yes or no)
- Does the security incident constitute a personal data breach? (yes or no)
- Are you the processor or the controller of the personal data subject to the breach? (processor or controller)
- Is the breach likely to present a risk to the rights and freedoms of the persons concerned? (yes or no)
- Is the personal data breach likely to present a high risk to the rights and freedoms of natural persons? (yes or no)

bb) Language of the notification

There are no explicit indications from the Garante on the language to be used in the notification. It can be assumed that, since the form is in Italian and the addressee is the Italian Garante, the language to be used is Italian.

443 The instructions are available at https://servizi.gpdp.it/databreach/s/istruzioni.

444 The facsimile form is available at https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni.

445 Available at https://servizi.gpdp.it/databreach/s/self-assessment.

e) Information to be included in the notification

aa) Required information

The notification must contain the information provided for in Art. 33 (3) GDPR.[446]

In Italy, the controller may choose between a complete notification or a pre-liminary notification, depending on the information in its possession at the time of notification.

In a complete notification, all questions must be answered definitively. In a preliminary notification, the whole form must be filled out but the answers can be completed or modified later by a complementary or modified notification.

According to the online form and the facsimile template, the Garante requires the following information to be included in the notification:

Data on the notifying party and the type of notification:

- data of the notifying person (name, surname, e-mail address),
- the type of notification, either
  - a first notification (here, the controller may choose between a complete or a preliminary notification[447]) or
  - a supplementary notification;[448] in this case, the controller must indicate the file number of the first notification and the reason for the supplementation; the controller can either
    - provide additional information without completing the notification process,
    - provide additional information and complete the notification process,
    - complete the notification process without providing additional information or
    - cancel a previous notification and indicate the reason for the cancellation,
- an indication as to whether the notification is made pursuant to Art. 33 GDPR or pursuant to Art. 26 of Legislative Decree No 51/2018.[449]

---

446 Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) of 30 July 2019 [9126951]), available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9126951.

447 The data controller shall initiate the notification process in the absence of a complete picture of the breach by undertaking to make a subsequent supplementary notification to provide the information it does not yet possess.

448 The data controller, availing itself of the provisions of Art. 33 (4) GDPR, supplements a previous notification.

449 Art. 26 of Legislative Decree No 51/2018 (online, available at https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2018-05-18;51!vig=) regulates data breach notifications according to Directive (EU) 2016/680, transposed into Italian law. It is not relevant here as it only applies to the processing of personal data by the police and criminal justice authorities and provides that such data controllers shall also report, breaches to the Garante in the manner set out in Art. 33 GDPR.

Information on the data controller:

- an indication as to whether the controller is registered in the national index of digital domiciles of companies and professionals (INI-PEC)[450] or not (checkbox),
- the contact details of the controller (country, province, municipality, post-code, address, phone number and tax code); if the controller is registered in the INI-PEC register, it must provide its PEC address[451] (e-mail address optional); if it is not registered in that register, provision of the e-mail address is mandatory (and PEC optional),[452]
- the name and contact details of the controller's representative, if the controller is obliged to assign a representative within the EU.

Contact details for information on the breach:

- the name and the contact details of the data protection officer (surname, first name, e-mail address, phone number) or of another contact person from whom more information can be obtained (surname, first name, e-mail address, phone number, position held).

Information on additional parties involved in the processing:

- the references of further parties involved in the processing and their role, for example, joint controller/other controller, processors and sub-processors (name of the company, not of the legal representative), tax code, VAT number, if applicable).

Information on the data breach:

- the date of the breach (one of the following boxes must be checked: date / since – to / since – (if breach is ongoing) / at a time not yet determined) and there is a text box to include further information on the dates on which the breach occurred),
- the means by which the controller became aware of the breach, for example, (checkbox to be ticked):
  - detection by the controller, for example, during an internal audit or monitoring,
  - communication by the controller,
  - report by a data subject,
  - report by an external party,

---

450 INI-PEC is the National Index of Certified Electronic Mail (PEC) Addresses established by the Ministry of Economic Development. INI-PEC collects all the PEC addresses of companies and professionals on Italian territory; anyone can access the search section of the portal (inipec.gov.it) and search for the certified e-mail address of interest. See https://www.registroimprese.it/ini-pec.

451 Certified e-mail address.

452 Indicate the information on the data controller (in the case of a company or public entity, indicate the data of the legal entity and not the natural person corresponding to the legal representative).

- press reports or
- other (to be specified),

- the time at which the data controller became aware of the breach (date and time),
- the reasons for delay (in case of notification after more than 72 hours),
- the nature of the breach; here, the controller must tick one of the following checkboxes:
  - loss of confidentiality,[453]
  - loss of integrity,[454]
  - loss of availability,[455]
- the cause of the breach; here, the controller must tick one of the following checkboxes:
  - intentional internal action,
  - accidental internal action,
  - external intentional action,
  - accidental external action,
  - unknown (to be specified in a text box) or
  - not yet determined,
- a description of the violation, meaning an indication of the circumstances under which the breach occurred and the technical or organisational causes that led to it,
- a description of the systems, software, services and IT infrastructure involved in the breach, including their location,
- the technical and organisational measures in place at the time of the breach taken to ensure the security of the personal data involved,
- the categories of data subjects involved in the breach, for example,
  - employees/consultants,
  - users/subscribers/customers (current or potential),
  - associates, members, supporters,
  - persons holding corporate offices,
  - beneficiaries or guests,
  - patients,

453 Unauthorised or accidental disclosure or access.

454 Unauthorised or accidental modification.

455 Unauthorised or accidental access or destruction.

- minors,
- vulnerable persons affected by the breach (for example, victims of violence or abuse, refugees, asylum seekers),
- other (to be specified) or
- categories not yet determined,

- the number (also approximate) of data subjects involved in the breach; here, the controller must tick one of the following checkboxes:
  - __ data subjects involved,
  - approximately __ data subjects involved,
  - not determinable,
  - not yet determined,
- the categories of personal data affected by the breach; the controller must tick the applicable checkbox(es):
  - master data (name, surname, sex, date of birth, place of birth, tax code),
  - contact data (postal or e-mail address, fixed or mobile phone number),
  - access and identification data (username, password, customer ID, other),
  - payment details (bank account number, credit card details, other),
  - data relating to the provision of an electronic communication service (traffic data, internet browsing data, other),
  - data relating to criminal convictions and offences or related security measures,
  - profiling data,
  - data relating to identification/recognition documents (identity card, passport, driving licence, CNS[456], other),
  - location data,
  - data revealing racial or ethnic origin,
  - data revealing political opinions,
  - data revealing religious or philosophical beliefs,
  - data revealing trade union membership,
  - data concerning sexual life or sexual orientation,

456 CNS stands for Tessera Sanitaria – Carta Nazionale dei Servizi (TS-CNS). The CNS is issued by the Revenue Agency, which is responsible for producing and distributing the card throughout the country.

- health data,
- genetic data,
- biometric data,
- other (to be specified),
- categories not yet determined,

- the number (also approximate) of records (for example, invoices, orders, reports, images, database records or transactions) of personal data that are subject to the breach; here, the controller must tick one of the following checkboxes:
  - exact number ___,
  - approximate number ___,
  - not determinable,
  - not yet determined,
- a detailed description of the categories of personal data concerned by the breach for each category of data subjects,
- attachments (the controller may attach documents with further information).

A description of the probable consequences of the breach:

- the likely consequences of the data breach for the data subjects concerned,
  - in case of loss of confidentiality, the controller must tick one of the following check-boxes:
    - the data have been disclosed outside the scope of the information notice or the relevant regulations,
    - the data may be correlated, without unreasonable effort, with other information relating to the data subjects,
    - the data may be used for purposes other than those intended or in an unlawful manner,
    - other,
    - under assessment,
  - in case of loss of integrity, the controller must tick the applicable check-box:
    - the data have been modified and rendered inconsistent,
    - the data have been modified while maintaining consistency,
    - other (to be specified),

        - under evaluation,
    - in case of loss of availability, the controller must tick the applicable checkbox(es):
        - lack of access to services,
        - malfunctioning and difficulty in using services,
        - other,
        - under evaluation,
    - further considerations on the likely consequences (to be specified in a text box),
- the potential impact of the data breach on data subjects; the controller must tick the applicable checkbox(es):
    - loss of control over personal data,
    - limitation of rights,
    - discrimination,
    - identity theft or usurpation,
    - fraud,
    - financial loss,
    - unauthorised decryption of pseudonymisation,
    - loss of reputation,
    - loss of confidentiality of personal data protected by professional secrecy,
    - knowledge by unauthorised third parties,
    - any other significant economic or social damage,
    - not yet defined,
- the severity of the potential impact for data subjects; the controller must tick one of the following checkboxes and insert the reasons for its assessment in a text box:
    - negligible,
    - low,
    - medium,
    - high,
    - not yet defined,
- attachments (the controller may attach documents with further information).

A description of the measures taken by the controller following the data breach:

- a description of the technical and organisational measures taken or proposed by the controller to remedy the breach and reduce its negative effects on the data subjects concerned, broken down by
  - measures already adopted and
  - measures in the process of being adopted,
- a description of the technical and organisational measures taken (or proposed to be taken) to prevent similar future breaches, broken down by
  - measures already adopted and
  - measures in the process of being adopted,
- attachments (the controller may attach documents with further information).

An assessment of the risk to the affected data subjects:

- the controller must tick one of the following boxes, indicating whether it considers that
  - the breach is likely to present a high risk to the rights and freedoms of natural persons,
  - the breach is not likely to present a high risk to the rights and freedoms of natural persons,
  - further elements are necessary to carry out the risk assessment for the rights and freedoms of natural persons, and
- the controller must indicate the reasons which led it to the assumption that the personal data breach is likely, or not, to present a high risk to data subjects,
- attachments (the controller may attach documents with further information).

Information on the notification of the breach to the affected data subjects:

- the controller must specify whether it has communicated the data breach directly to the affected data subjects by ticking one of the following boxes:
  - yes, it was communicated on: dd/mm/yyyy,
  - no, it will be communicated on: dd/mm/yyyy,
  - no, because assessments are still ongoing,
  - no, because the breach is not likely to present a high risk to the rights and freedoms of natural persons,
  - no, and it will not be communicated because
    - the controller has implemented appropriate technical and organisational protection

measures and those measures have been applied to the personal data subject to the breach, in particular those designed to render the personal data unintelligible to anyone not authorised to access them (for example, encryption); the controller must describe the applied measures in a text box,

- the controller has subsequently taken measures to prevent a high risk to the rights and freedoms of the data subjects; the controller must describe the measures applied,
- such disclosure would require disproportionate efforts; the controller has proceeded or will proceed with a public notice or similar measure by which data subjects are or will be informed in a similarly effective manner; the controller must describe the manner in which the data subjects were informed,

- the controller must specify the number of affected data subjects notified of the breach,
- the channel it has used for communication to data subjects (SMS, paper mail, e-mail or other),
- the content of the communication to the data subjects (in a text box), and
- attachments (the controller may attach documents with further information).

Further information:

- the controller must also specify
  - whether the data breach has been reported to other supervisory or control bodies by virtue of additional regulatory provisions[457] (yes or no); if yes, the controller must indicate to which body and under which regulation,
  - whether a report has been made to the judicial or police authority (yes or no); there is a text box to insert more information.

Information on cross-border data breaches:[458]

- the controller must
  - tick a checkbox depending on whether the breach concerns cross-border processing carried out by a controller established within the European Economic Area (yes; no; the necessary assessments are still ongoing),
  - indicate the lead control authority (Garante or other DPA (to be selected from a list)),

457 For example, Regulation (EU) 910/2014 (eIDAS), Legislative Decree No 65/2018 implementing Directive (EU) 2016/1148 (NIS).

458 A cross-border processing operation (see Art. 4 (23) Regulation (EU) 2016/679) is a processing operation that takes place in the context of establishments in more than one country of the European Economic Area (which includes the Member States of the European Union as well as Iceland, Liechtenstein and Norway) or that takes place in the context of a single establishment in one country of the European Economic Area but which may have significant impacts on the rights and freedoms of data subjects in more than one country of the European Economic Area.

- specify by choosing from a list all countries of the European Economic Area in which establishments of the controller are located, specify by ticking a box which of those establishments in other countries are involved in the breach and in which of those countries there are data subjects involved in the breach,
- indicate by choosing from a list any other supervisory authorities notified of the breach,
- indicate whether it attaches a copy (in English) of the notification made, and

Information relating to breaches concerning a processing carried out by a controller established outside the European Economic Area:[459]

bb) Optional information

As the Garante's online form does not distinguish between mandatory and optional information, it can be assumed that all the data mentioned under aa) must be provided on a mandatory basis.

f) Timeline of the notification

The Garante repeats[460] that the controller shall report data breaches to the Garante without undue delay and, where possible, within 72 hours (first notification). If and to the extent that the data controller does not have all the information, it may provide it at a later stage with the help of a supplementary notification) without further undue delay.[461] Notifications to the Garante made after the 72-hour deadline must be accompanied by the reasons for the delay.

g) Exemptions from the duty to notify a personal data breach to the supervisory authority

The Garante reiterates that in the event of a personal data breach, the controller shall report the breach to Garante "unless the personal data breach is unlikely to present a risk to the rights and freedoms of natural persons".[462]

According to the information provided by the Garante in the self-assessment procedure form, the risk exists when the breach is likely to result in harm, material or immaterial, to the individuals whose data are affected by the breach. The Garante refers to Recital 85 of the GDPR, which lists some of the harms that may result from a personal data breach, such as: discrimination,

459 Not further specified here, as it is irrelevant for private businesses based in the EU. For more information see the Garante's online form and the facsimile template.

460 See the facsimile template, available at https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni, p. 3.

461 For more information on the first and supplementary notification see above A. IV. 5, e) aa).

462 See https://www.garanteprivacy.it/regolamentoue/databreach#:~:text=senza%20ingiustificato%20ritardo%20e%2C%20ove,le%20libert%C3%A0%20delle%20persone%20fisiche.

identity theft or usurpation, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised pseudonymisation or any other significant economic or social harm.

For the assessment of the risk, the Garante[463] refers to Recitals 75 and 76 of the GDPR and the Working Paper 250 guidelines endorsed by the EDPB.[464] The Garante repeats that as a general rule, both the likelihood and the seriousness of risks to the rights and freedoms of data subjects should be taken into account in the risk assessment and that these risks should be determined on the basis of an objective assessment. In that assessment, the following factors must be considered: the type of breach; the nature, sensitivity and volume of personal data; the ease of identification of data subjects; the severity of the consequences for data subjects; the particular characteristics of the data subject; the particular characteristics of the data controller as well as the number of data subjects involved.

Beyond these references to the GDPR and the EDPB guidance, no further official guidance of the Garante on the risk assessment could be found on the Garante's website.

h) Other documentation duties (Art. 33 (5) GDPR)

The controller must document all personal data breaches that occur, regardless of whether a breach must be reported to the Garante, including the circumstances and consequences thereof and the measures taken. They can do so, for instance, by preparing a register. This documentation allows the Garante to carry out compliance checks.[465] The Garante therefore advises that the controller take the necessary steps to document any breaches, also because they are required to provide such documentation, upon request, to the Garante in the event of an investigation.[466]

6. Comparative analysis

In the following, a summary and comparison of some of the most relevant national provisions and administrative requirements regarding the obligations to notify data breaches to the competent DPA are provided. This chapter is based on the official guidance given by national DPAs. Among the Member States researched, only Germany has a federal system of data protection supervision, consisting of the data protection supervisory authorities of the Federation (the "Bund") and the 16 federal states (the "Länder"). As far as the data protection supervisory

463 Facsimile template, available at https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni, p. 16.

464 See Section A. IV. 1. a) bb).

465 Garante della Privacy, Violazioni di dati personali (data breach) in base alle previsioni del Regolamento (UE) 2016/679, available at https://www.garanteprivacy.it/regolamentoue/databreach.

466 See https://www.garanteprivacy.it/home/doveri.

authorities of the federal states are the competent authority, the following tables are based on the form and guidance provided by the LfDI Baden-Württemberg.

a) Applicable legislation and guidance

Table 21 provides an overview of the applicable national legislation and the official guidance by the competent national DPAs and the LfDI Baden-Württemberg (for example, via forms, templates and guidance documents).

Table 21: National legislation and guidance by DPAs

	Austria	France	Germany/BW	Italy
National legislation	Data Protection Act	Act on data processing, data files and individual liberties	Federal Data Protection Act and State Data Protection Act of Baden-Württemberg	Personal Data Protection Code
Does the national legislation mentioned above contain specific provisions which concretise, supplement or derogate from the duties under Art. 33 GDPR?	No specific provision	Art. 58: obligation to notify the CNIL of any personal data breach according to Art. 33 GRPR (i.e. no derogation from Art. 33)	No specific provision	No specific provision

	Austria	France	Germany/BW	Italy
Main official templates and guidance from DPAs	■ Data breach notification form, https://www.dsb.gv.at/dam/jcr:81630a55-648b-4689-b849-ce0732f6a1af/Meldung%20von%20Verletzungen%20des%20Schutzes%20personenbezogener%20Daten%20gem%C3%A4%C3%9F%20Art.%2033%20DSGVO%20Notification%20of%20a%20personal%20data%20breach%20(Art.%2033%20GDPR)%20.pdf ■ DSB guideline, https://www.dsb.gv.at/download-links/dokumente.html	■ Data breach online notification form, https://notifications.cnil.fr/notifications/index ■ Guidelines on the implementation of Art. 33 GDPR, https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles	■ BfDI information sheet "on data breach notifications", https://www.bfdi.bund.de/DE/Service/Datenschutzverstoesse/Infoblatt_Datenschutzverstoesse.html ■ BfDI online form for the notification of data breaches, https://formulare.bfdi.bund.de/lip/form/display.do?%24context=15B94D-B8E5D9616D42CC ■ DSK Short Paper No 18 on risks to rights and freedoms of natural persons, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf ■ LfDI Baden-Württemberg online form for notification of data breaches, https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/ ■ Auxiliary document with input on how to fill online form "Meldung einer Datenpanne nach Art. 33, 34 DSGVO", https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Meldeformular-Datenpanne-Eingabefelder.pdf	■ Data breach online notification form, https://servizi.gpdp.it/databreach/s/scelta-auth ■ Explanations of terms and concepts related to the notion of data breach, https://www.garanteprivacy.it/regolamentoue/databreach ■ Fact sheet with instructions on how to use the online notification procedure, https://servizi.gpdp.it/databreach/s/istruzioni ■ Facsimile template, https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni ■ Self-assessment tool helping controllers to identify the actions to be taken following a data breach, https://servizi.gpdp.it/databreach/s/self-assessment

b) The notion of a "personal data breach"

As regards the notion of a "personal data breach", no diverging interpretations from the GDPR and/or the guidance provided by the EDPB could be found in the Member States researched.

c) Where to notify?

Table 22 provides an overview of the competent DPAs to be notified of data breaches according to Art. 33 (1) GDPR.

Table 22: Specification of the competent DPA to be notified according to Art. 33 (1) GDPR

	Austria	France	Germany/BW	Italy
Competent supervisory authority to be notified of a data breach of private companies	Datenschutzbehörde (DSB)	Commission Nationale de l'Informatique et des Libertés (CNIL)	■ Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) for companies subject to the exclusive jurisdiction of the BfDI (e.g. companies providing telecommunications or postal services) ■ For all other companies, the DPA of the federal state in which the controller's central administration (main establishment) is based, meaning for companies having their sole establishment or their central administration in Baden-Württemberg, the LfDI Baden-Württemberg	Garante per la protezione dei dati personali, also commonly referred to as the Garante della Privacy (Garante)

d) Design of the notification

Table 23 provides an overview of the required design of the notification of data breaches to the competent DPA, including the format and the language of the notification.

Table 23: Design (format and language) of the notification

	Austria	France	Germany/BW	Italy
Format of the notification	Mail or e-mail Use of notification form is not mandatory	Online notification form (mandatory)	■ BfDI and LfDI Baden-Württemberg: electronic notification form ■ LfDI: alternatively by e-mail or phone	Online notification form (mandatory)
Types of notification, e.g. preliminary, supplementary and complete notification	Only one notification form; controller can check a box that information cannot be provided yet and must add information later without further delay, but no separate online form/procedure provided	Controller can choose between preliminary notification and complete notification	Only one online notification form; controller can add information later, but no separate online form/procedure provided	Controller can choose between preliminary, supplementary and complete notification
Language of the notification	German	French	German	Italian

e) Information to be included in the notification

The following tables provide an overview of the information that must be included in the notification of data breaches to the competent DPA[467] under Art. 33 GDPR.

Table 24 provides an overview of the information on the personal data breach that must be included in the notification according to Art. 33 (3) lit. a GDPR, supplemented by the requirement to accompany the notification by reasons for the delay if the notification is not made within 72 hours according to Art. 33 (1) GDPR.

467 For Germany, the presentation is limited to the information that companies must provide when reporting a data breach to the LfDI Baden-Württemberg (and not to the BfDI).

Table 24: Specification of information to be included in the notification according to Art. 33 (3) lit. a GDPR, supplemented by the reasoning required according to Art. 33 (1) GDPR

Category of information required	Austria	France	Germany/BW	Italy
Description of the nature of the personal data breach	■ Text box for the description of the personal data breach ■ Categorisation of the personal data breach (checkbox): either breach of confidentiality, breach of integrity or breach of availability	■ Checkbox on the origin of the incident: i.a. lost or stolen equipment, hacking, malware and/or phishing, personal data sent to wrong recipient etc. ■ Detailed description of the violation ■ Checkbox on the cause of the incident: e.g. external malware act ■ Categorisation of the personal data breach (checkbox): either loss of confidentiality, loss of integrity or loss of availability	Text box for a description of the data breach as precise as possible, including: ■ Place of the incident ■ The persons involved ■ How the notifying person learned of it ■ Whether the responsible organisation has been informed ■ Which third parties have become aware or had the opportunity to become aware	■ An indication of the circumstances under which the breach occurred and the technical or organisational causes that led to it ■ The systems, software, services and IT infrastructure involved in the breach, including their location ■ Checkbox on the cause of the breach, e.g. external intentional action ■ Categorisation of the personal data breach (checkbox): either loss of confidentiality, loss of integrity or loss of availability
Where possible, the categories of data subjects concerned	Categories of the affected data subjects, e.g. customers, employees, patients, children	Categories of affected data subjects; checkbox: e.g. employees, users, customers, patients	See below "Where possible, the categories of personal data records concerned"	E.g. employees, users, patients, minors
Where possible, the approximate number of data subjects concerned	Approximate number of affected data subjects	Approximate number of affected data subjects	Precise number (or at least estimated upper limit) of affected data subjects	Checkbox: ■ __ data subjects involved ■ Approximately __ data subjects involved ■ Not determinable ■ Not yet determined
Where possible, the categories of personal data records concerned	Affected categories of data, e.g. purchased products, health data, banking data, political opinion	■ Checkbox on the nature of the affected data: e.g. civil status, registration number, contact details, financial information ■ Checkbox on sensitive data: e.g. racial or ethnic origin, political opinions	Types of data affected, e.g. employee data, customer data, bank details, health data	Checkbox, e.g. contact data, access data, payment details, health data

	Austria	France	Germany/BW	Italy
Where possible, the approximate number of personal data records concerned	Approximate number of data records involved	Approximate number of data records affected by the breach	Information required according to auxiliary guidance document, but the online form of the LfDI Baden-Württemberg does not include a respective field	Checkbox: ■ Exact number ■ Approximate number ■ Not determinable ■ Not yet determined
Reasons for the delay if the notification was not made within 72 hours	Specific text box to insert the reasons for the delay	Reasons for the delay can be stated after having indicated information on the date of the breach	Not expressly requested in the online form Could be inserted in the text box "Other notification to the DPA"	Not further specified

Table 25 provides an overview of the information that must be included in the notification according to Art. 33 (3) lit. b GDPR, namely, the name and contact details of the data protection officer or other contact point where information can be obtained.

Table 25: Specification of information to be included in the RPA according to Art. 33 (3) lit. b GDPR

Category of information required	Austria	France	Germany/BW	Italy
Name and contact details of the data protection officer	Name, postal address and e-mail address (unless identical to that of the controller)	Not requested	Not requested	Surname, first name, e-mail address, phone number
Name and contact details of any other contact point where information can be obtained	Name, postal address, function and e-mail address	Civility, surname, first name, phone number, e-mail address, function, postal address, ZIP code, city, country	Not requested	Surname, first name, e-mail address, phone number, position held

Table 26 provides an overview of the information that must be included in the notification according to Art. 30 (1) lit. c GDPR, namely, a description of the likely consequences of the personal data breach.

Table 26: Specification of information to be included in the notification according to Art. 33 (3) lit. c GDPR

Category of information required	Austria	France	Germany/BW	Italy
Description of the likely consequences of the personal data breach	Description of the most likely consequences of the data breach for the data subjects, e.g. exposure, discrimination, financial loss, liability towards customers, identity theft	■ Checkbox on the nature of impacts: e.g. loss of control over personal data, discrimination, identity theft, fraud, financial loss ■ Checkbox on potential consequences of a loss of confidentiality: e.g. data may be used for purposes other than those intended and/or in an unfair manner ■ Checkbox on potential consequences of a loss of integrity: e.g. data may have been modified and used when they are not true ■ Checkbox on potential consequences of a loss of availability: e.g. inability to provide a critical service	Risk assessment including a list of adverse consequences that are probable or have occurred for the affected data subjects which the controller considers likely to occur, e.g. unauthorised account debits, identity theft	■ Checkbox on risk assessment, e.g. on whether the breach is likely to present a high risk to the rights and freedoms of natural persons ■ Reasons for the decision above ■ Checkbox on potential impact on data subjects e.g. discrimination, identity theft, fraud ■ Checkbox on loss of confidentiality: e.g. data may be used for purposes other than those intended or in an unlawful manner ■ Checkbox on loss of integrity: e.g. data may have been modified and rendered inconsistent ■ Checkbox on loss of availability: e.g. lack of access to services ■ Further considerations on the likely consequences

Table 27 provides an overview of the information that must be included in the notification according to Art. 33 (3) lit. d GDPR, namely, a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Table 27: Specification of information to be included in the notification according to Art. 33 (3) lit. d GDPR

Category of information required	Austria	France	Germany/BW	Italy
Description of measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects	■ Measures taken to address the personal data breach ■ Measures taken to mitigate the possible adverse effects	■ Measures taken to remedy the breach ■ Measures taken to mitigate any negative consequences (if applicable)	The countermeasures already taken by the controller and the additional countermeasures planned (according to auxiliary document, a "detailed explanation" of the measures with regard to the specific incident and the objective of preventing such incidents in the future is required)	■ Measures to remedy the breach and reduce its negative effects ■ already adopted ■ in the process of being adopted ■ Measures to prevent similar future breaches ■ already adopted ■ in the process of being adopted

Table 28 lists several pieces of information that controllers must include in the notification of data breaches according to the official forms published by the national DPAs, although Art. 33 GDPR does not expressly require such information. This includes information on the notifying controller itself and on other relevant parties as well as information on the time and duration of the data breach and the controller's awareness of the latter. However, it follows implicitly from Art. 33 GDPR that the controller must provide the respective information to enable the competent DPA to handle the data breach or to verify whether the controller has adhered to the notification period. Therefore, the request for this information in the forms makes sense and should not be considered gold plating.

Table 28: Specification of information on the controller and other relevant parties as well as the time, duration and awareness of the data breach that must be included in the notification

Category of information required	Austria	France	Germany/BW	Italy
Information on the controller	Name, postal address and e-mail address	■ SIREN code/identification number ■ Name, postal address, VAT number, ZIP code, city, country, sector of activity ■ Number of employees	Name, address (street house number, postcode, town)	■ Checkbox whether the controller is registered in the national index of digital domiciles of companies and professionals; if yes, also PEC address; if not, e-mail address ■ Name, country, province, municipality, postcode, address, phone number and tax code
Information on the notifying person	Not requested	Not requested	Name, function, e-mail address, phone number	Name, surname, e-mail address
Information on other parties involved	■ Processor: name, postal address and e-mail address ■ Joint controller: whether data are processed jointly with another controller and presumably contact details	Name and quality of third-party organisations involved	Not requested	■ Name and contact details of the controller's representative, if the controller is obliged to assign one ■ Joint controller, processors and sub-processors: name, tax code, VAT number
The time at which the personal data breach took place	Time at which the breach took place	Date of data breach (date and time of violation)	Date of data breach	Date of data breach
The time at which the controller became aware of the personal data breach	Time at which the breach became known	Date and time of awareness of violation, date and time of notification by provider	Time at which the controller became aware of the breach	Date and time
Duration of the personal data breach	Not expressly requested	Date and time of start of violation, date and time of end of violation, violation over a definite or indefinite period, whether violation is still ongoing	Not expressly requested	Date of end of violation or whether the violation is still ongoing

Table 29 provides an overview of other information requested by the national DPAs in their notification forms, though Art. 33 does not require controllers to include such information in the notification to the competent DPA. This information could be regarded as gold plating.[468]

468 As regards the question of whether information relating to the notification of data subjects can be classified as gold plating, it must be taken into account that the controller might – under the narrower conditions of Art. 34 GDPR – also be required to report the data breach not only to the competent DPA but also to the affected data subjects. Therefore, the controller must deal with the related questions either way, and the national DPAs have a certain interest in knowing whether the controller has informed the data subjects. However, the conditions of Art. 34 require an even more complex assessment by the controller. Beyond this, recital 86 of the GDPR states that communication to data subjects should be made in close cooperation with the competent DPA. Therefore, it seems excessive to require the controller to include the respective information also (or already) in the notification to the DPA according to Art. 33 (for which the deadline of 72 hours applies).

Table 29: Other information to be included in the notification

Category of information required	Austria	France	Germany/BW	Italy
Other information to be included in the notification	None	■ The controller's pre-breach security measures ■ Checkbox on the estimated level of the data breach's severity: negligible, limited, important, maximum ■ Checkbox on whether data subjects have been informed ■ Specification as to whether the notification concerns cross-border processing targeting persons from different Member States ■ Specification as to whether the breach has been or will be notified to another European DPA ■ Specification as to whether the breach has been or will be notified to another authority to comply with another legal requirement	Checkbox on whether the controller considers that it must inform the affected data subjects; if yes: the controller must indicate when and how the affected data subjects have been or will be notified and which specific countermeasures the controller has recommended to them; if no: the controller must explain why it has no obligation to notify the data subjects	■ The technical and organisational measures in place at the time of the breach taken to ensure the security of the personal data involved ■ Checkbox on how the controller became aware of the breach, e.g. communication by the controller, report by a data subject, report by an external party, press reports ■ Checkbox on the estimated level of severity of the data breach: negligible, low, medium, high, not yet defined ■ Detailed description of the categories of personal data concerned by the breach for each category of data subjects ■ Checkbox on whether data subjects have been informed ■ If yes, date must be indicated ■ If not, reasons must be given ■ Number of data subjects notified ■ Mode of notification (e.g. e-mail) ■ Content of the notification ■ Whether the data breach has been notified to other authorities; if yes, the controller must indicate to which authority and under which regulation ■ Whether a report has been made to the judicial or police authority ■ Checkbox on whether the breach concerns cross-border processing carried out by a controller established within the EEA ■ Indication of the lead supervisory authority ■ Choosing from a list, all EEA countries where establishments of the controller are located, which of those establishments are involved in the breach and in which of those countries there are data subjects involved in the breach ■ Choosing from a list any other supervisory authorities notified of the breach

Table 30 provides an overview of the exemptions from the duty to notify a personal data breach to the supervisory authority according to Art. 33 (1) GDPR.

Table 30: Exemptions from the notification duty according to Art. 33 (1) GDPR

	Austria	France	Germany/BW	Italy
Criteria specified by national DPAs that controller must take into account for risk assessment	None	■ Type of breach (affecting data integrity, confidentiality or availability) ■ Nature, sensitivity and volume of personal data involved ■ Ease of identifying the individuals affected by the breach ■ Possible consequences of the breach for individuals ■ Characteristics of those individuals (children, vulnerable individuals etc.) ■ Volume of individuals affected ■ Characteristics of the controller (nature, role, activities)	■ DSK paper: all conceivable negative consequences for individuals must be taken into account ■ Likelihood of harm ■ Severity of the harm (essential factors for determining the severity are inter alia the sensitivity of data, processing of uniquely identifying data, vulnerability of the affected data subjects and the volume of affected individuals) ■ General referral to EDPB guidance	■ Likelihood of risks to data subjects ■ Seriousness of the risk to data subjects ■ Type of breach ■ Nature, sensitivity and volume of personal data ■ Ease of identification of data subjects ■ Severity of the consequences for data subjects ■ Particular characteristics of the data subject ■ Particular characteristics of the data controller ■ Number of data subjects involved ■ Concrete referral to EDPB guidance regarding criteria for risk assessment
Does the national DPA provide examples of cases where there is no duty to notify the data breach to the DPA?	■ Only corporations' data are affected ■ Data are processed by natural persons exclusively for personal or family reasons (e.g. a mobile phone with personal contacts is lost) ■ A risk to the rights and freedoms of natural persons is unlikely	■ Disclosure of data already made public ■ Deletion of data saved and immediately restored ■ Loss of data protected by an encryption key if the encryption key has not been compromised and if a copy of the data remains available	No	No

7. Conclusion

Information requirements in Member States vary significantly in level of detail

When comparing the information requirements in the Member States researched, it is obvious that they vary significantly in their level of detail. The Austrian form requests the smallest amount of information, followed by the Baden-Württembergian, French and Italian form with the latter having the longest list of information requirements. However, it must also be taken into account that the Italian form operates mainly with checkboxes as opposed to the open

text boxes that the Austrian form and the form of the LfDI Baden-Württemberg use predominantly. Furthermore, while Italy requests more information than the other three Member States researched, it also offers guidance on some aspects that are not further specified in the other Member States researched, for example, regarding the measures taken or proposed to be taken by the controller to address the personal data breach. Thus, it is an empirical question whether the need to provide more information also results in a larger bureaucratic burden.

Additional information required by national data protection authorities mostly very useful

All Member States researched require some information that is not explicitly required by the GDPR but implicitly necessary or at least very useful; hence, we do not consider it gold plating for the purpose of this study. This includes the name and contact details of the controller as well as the time at which the data breach took place and the time at which the controller became aware of it. Given that according to Art. 33 (1) GDPR a data breach must, where feasible, be notified within 72 hours upon becoming aware of it, the time at which the controller became aware of it is necessary to assess compliance with this time limit. In addition to these common information requests, each Member State researched requires some information that not all or even none of the others request. For instance, France and Italy ask whether the data breach is still ongoing and when it came to an end, respectively. Italy and the LfDI Baden-Württemberg ask for the name of the notifying person. France requests the controller's identification number, VAT number, sector of activity and number of employees, Italy whether the controller is registered in the national index of digital domiciles of companies and professionals (depending on the answer, the required contact details vary slightly).

Some cases of gold plating in Italy, France and Germany

However, in France, Baden-Württemberg and Italy, there are also information requirements that we do consider gold plating, Italy having the largest number of them. All three require information on whether the affected data subjects have been informed of the data breach. France and Italy ask for security measures taken before the data breach took place, the data breach's estimated level of severity, whether the data breach concerns cross-border processing within the EU/EEA, whether it has been/will be notified to DPAs in other Member States and whether it has been/will be notified to other authorities based on other legislation. Italy adds further notification points, including information on how the controller became aware of the breach and the lead authority for the data breach.

Interestingly, not all notification forms request every piece of information that Art. 33 GDPR requires. For instance, the online notification form of the LfDI Baden-Württemberg does not require the name and contact details of the data protection officer or other contact point where information can be obtained. France does not ask for the data protection officer either.

There are also differences regarding the form of the notification. In France and Italy, the use of the online notification form is mandatory. In Baden-Württemberg, online notification is

predominantly used, but not mandatory, as notification by phone and e-mail is also possible. Austria, in contrast, does not provide for an online notification form. Here, notifications must be made by mail or e-mail.

Part B: Assessment of regulatory burdens by Prognos AG and CSIL

Part B prepared by:

Prognos AG
Goethestraße 85
10623 Berlin
Germany

Jan Tiessen
Michael Schaaf
Jan-Felix Czichon

CSIL
Corso Monforte 15
20122 Milan
Italy

Jessica Catalano
Sara Banfi
Anthony Bovagnet

I. Introduction

The General Data Protection Regulation (GDPR) entered into force in 2016 and applies since 25 May 2018 to companies and entities which process personal data as part of their activities. This study addresses legal and administrative requirements for private businesses with regard to creating and maintaining a record of processing activities according to Art. 30 GDPR and the requirements related to the notification of personal data breaches to the supervisory authority according to Art. 33 GDPR.

Since the Regulation came into force, various studies have dealt with the degree of implementation of the GDPR. Little attention has been drawn to the question of what efforts and costs are associated with compliance for companies. Therefore, the following questions are answered for each of the four Member States researched (see sections III, IV, V, VI) and summarised in the following chapter:

- How is EU legislation transposed in national law?
- How are the provisions implemented in the administrative context?
- What are the standard processes (procedures) for companies to comply with the requirements of the registers?
- What are the average compliance costs to cover the standard process?
- What burdens do companies perceive?
- What changes could improve the process?

II. Comparison

The country comparison includes the key results for the country analysis of Austria, Germany, France and Italy (details are reported in sections III, IV, V, VI) and a differentiation by company size. Due to the design of this study, this distinction is not applicable at the country level.

1. Transposition and administrative implementation

On 25 May 2018, the European General Data Protection Regulation (GDPR) came into effect and has since been the standard regulating the protection of personal data within the European Union (EU). The GDPR applies directly in all Member States of the EU, including Germany, Austria, France and Italy. Therefore, the regulations regarding the documentation of processing activities (Art. 30 GDPR) and the obligation to report data breaches (Art. 33 GDPR) are generally uniform throughout the EU and apply in the same way in all Member States.

In Austria, the data protection authority (DPA) is responsible for monitoring and enforcing the GDPR. This authority is an independent administrative body attached to the Federal Chancellery. In France it is the "Commission Nationale de l'Informatique et des Libertés" (CNIL) as an independent administrative authority that reports to the French government. In Italy, the responsibility for monitoring and complying with the GDPR is assigned to the "Garante per la protezione dei dati personali", an independent administrative authority subordinate to the Italian Parliament. In these countries, responsibility is organised centrally. In contrast, the responsibility in Germany lies within the data protection authorities of the federal states. There are 16 data protection authorities, each of them responsible for supervising companies and organisations in their respective federal state and additionally the Federal Commissioner for Data Protection and Freedom of Information (BfDI) as a supervisory authority at federal level.

Before the GDPR came into effect, there were no consistent rules on the obligation to maintain a record of processing activities (RPA) or to report data breaches across the EU. Although there were national laws in place before, the requirements varied across countries for keeping processing records or reporting data protection incidents. In Germany, for example, the Federal Data Protection Act (BDSG-alt) regulated the handling of personal data; similar laws existed in Austria (Datenschutzgesetz von 2000 (DSG 2000)), Italy (Law No 196/2003) or France (Loi informatique et libertés). The GDPR has supplemented and expanded them.

Art. 30 GDPR regulates the obligation of controllers and processors to maintain an RPA, while Art. 33 GDPR requires the reporting of data breaches to the competent supervisory authority and, if necessary, to the affected individuals. A controller is the entity that determines the purposes and means of the processing of personal data. The controller is responsible for ensuring that personal data are processed in accordance with the GDPR and must be able to demonstrate compliance with its requirements. The processor, on the other hand, is the entity that processes personal data on behalf of the controller. Processors have specific obligations under the GDPR. They are required to conclude written contracts with controllers specifying the purpose and nature of the processing, the duration, the type of personal data, the categories of data subjects and their obligations and responsibilities. They may only act on the instructions of the controller and must take appropriate technical and organisational measures to protect personal data.

Both in the creation of processing directories and in the reporting of data protection breaches, the GDPR has detailed and differentiated existing regulations and thus created a Europe-wide standard. The GDPR contains new provisions and requirements, such as the comprehensive requirements for the processing record under Art. 30 and the reporting obligations in case of personal data breaches under Art. 33. At the same time, the GDPR builds on the existing case

law and legislation on data protection and further develops it by adapting the requirements for the protection of personal data to the developments in technology.

However, the GDPR includes opening clauses in certain articles allowing the Member States a certain degree of flexibility in implementing the regulation. For example, Member States can issue provisions on the handling of personal data that are specific to the national context and go beyond the general provisions of the GDPR.

Regarding the articles examined in this study, there are no specific opening clauses that allow a deviation from the general provisions of the regulation for Art. 30 and 33. In this respect, the following provisions apply to all countries.

a) Provisions of Art. 30 GDPR

An RPA must contain the following information according to Art. 30 GDPR (1)[469]:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer,
- the purposes of the processing,
- a description of the categories of data subjects and of the categories of personal data,
- the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations,
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Art. 49 (1), the documentation of suitable safeguards,
- where possible, the envisaged time limits for the erasure of the different categories of data,
- where possible, a general description of the technical and organisational security measures referred to in Art. 32 (1).

As there is no official definition of the notion of a "processing activity" and the required level of detail in the RPA, companies regularly used and are still using templates to create or revise their RPA.

469 Art. 30 GDPR.

In terms of the availability of templates from public authorities, variation across countries has been observed. Austria provides the lowest amount of guidance regarding the creation of the RPA according to Art. 30. The French authorities provide more details on which information should be included in the RPA. In Germany, it depends on the respective authority in the federal state. Due to the number of data protection authorities, there are a variety of templates and information available in Germany. This information includes contact details of the controller, the joint controller and the data protection officer of the entity, necessary details on the processing activities carried out and additional information that is not explicitly required by the GDPR (for instance, the date of creation of the processing activity as well as the date of revision, if any). Compared to France or Germany, the template provided by the Italian authority is quite simple and according to the companies and experts interviewed only used by small or micro-companies.

Quantity of data protection authorities lead to high amount of templates and information in Germany

Especially in Germany, various institutions, including the data protection authorities of the federal states, and consulting firms have emerged with the provision of such templates. While in Austria, the Chamber of Commerce (WKO) is the only public institution through which templates have been made available, there are also a variety of consulting firms or certified individuals that offer consulting services regarding Art. 30. Also, in France and Italy, consulting firms have taken up the topic as a service and support companies in the implementation and compliance with the GDPR.

b) Provisions of Art. 33 GDPR

In case of a personal data breach, the supervisory authority must be notified within 72 hours. Art. 33 (1) GDPR stipulates the time frame in which a company representative is required to conduct above-mentioned steps:

> In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.[470]

Although Art. 33 allows for a preliminary notification, companies across all countries surveyed stated that they rarely use this option. Exclusively in France, companies reported the use of this possibility, especially when 72 hours are not enough to collect sufficient information on the incident or for conducting a risk assessment on the reported data breach.

470 Art. 33 GDPR.

According to Art. 33 (3) GDPR, the notification shall at least:

- describe the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned as well as the categories and approximate number of personal data records concerned,
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained,
- describe the likely consequences of the personal data breach and
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.[471]

The main differences regarding the transposition of Art. 33 is the granularity of the information requested by the authorities and the administrative implementation of the reporting process. The latter is described in detail in the legal part of the study. The effects of the administrative implementation on the bureaucratic burden for companies are described in more detail in the following chapter.

2. Efforts and compliance costs for standard activities

Bureaucratic costs in the countries surveyed arise from compliance with the regulatory requirements of the GDPR. Specifically, these are costs of performing standard activities to meet the requirements of Art. 30 and 33. The same activities were identified in all countries surveyed to establish compliance with the Art. 30 and 33. Variations have only been identified in the way companies organise the activities internally.

Table 31 summarises the standard activities necessary to comply with the GDPR, applicable for all countries surveyed.

471 Art. 33 GDPR.

Table 31: Standard activities related to GDPR compliance

Scope of Art. of the GDPR	Activities relating to compliance with the GDPR
Criteria specified by national DPAs that controller must take into account for risk assessment	Familiarisation with GDPR legislation
Art. 30	■ Creation of the RPA ■ Maintenance of the RPA
Art. 33	■ Internal processes for identifying and assessing the data protection incident, including: ▸ Reporting the incident to the data protection officer (DPO) ▸ Collecting information related to the incident ▸ Conducting a risk assessment ▸ Deciding whether a notification to the supervisory authority is necessary ■ Notifying the data protection authority

Company representatives stated that the risk assessment indirectly related to the notification process (Art. 33 (1)) requires a significant amount of resources. As there is no official definition for the term "risk" in Art. 33 (1) GDPR, especially larger companies expend substantial effort to complete this assessment. Some companies reported creating complicated spreadsheets to conduct the assessment in a comprehensible manner and independently of expert knowledge. Another difference was identified in the extent of the existing processes and structures for handling data protection incidents.

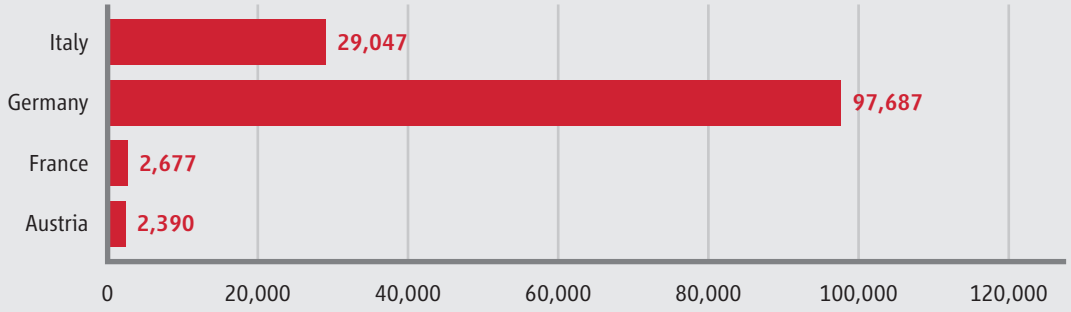
Lack of definition of the term "risk" increases the effort considerably

Familiarisation with GDPR legislation

Only a small number of companies were able to specify the estimates of the effort required for familiarisation regarding the selected articles of the GDPR. The results therefore relate to assessments of the familiarisation effort in general.

The results show the highest burden for German companies with an average of approximately 97,000 euros (Figure 1). With an average of approximately 30,000 euros, Italian companies also incur significant costs due to the introduction of the GDPR. With an average of approximately 2,500 euros, the familiarisation costs for companies in Austria and France are comparably low.

Figure 1: Familiarisation costs in EUR



Familiarisation costs result from the average time for familiarisation and the associated personnel costs as well as the costs for external consulting (see Table 32). While Italian companies invested the most time, with an average of 431 hours, in familiarising themselves with the legal requirements imposed by the introduction of the GDPR, German companies faced the highest consulting costs and thus the highest familiarisation costs.

Table 32: Composition of familiarisation costs

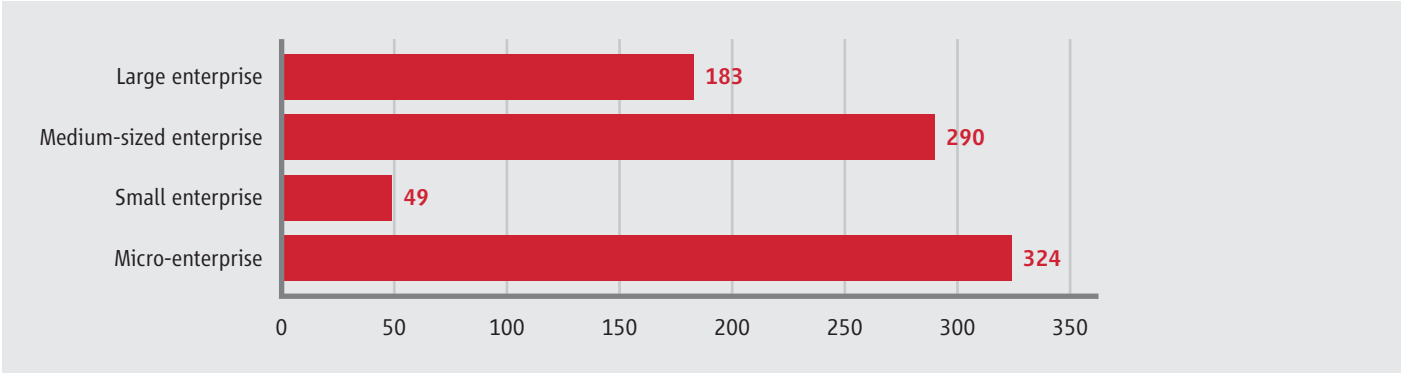
	Familiarisation time in hours	Personnel costs in EUR	Consulting costs in EUR
Austria	27	1,329	1,043
France	57	2,657	0
Germany	142	8,579	89,108
Italy	431	25,658	3,372

With an average of 89,000 euros, German companies relied the most on external support. As Italian companies invested a significant amount of time in familiarising themselves with the new legislation, they spent less money on additional consulting services. Companies in Austria invested an average of approximately 1,100 euros while no external costs were reported for French companies.

A differentiation by company size[472] provides further information on bureaucratic costs and underlying effects[473].

A breakdown by company size shows that micro-enterprises on average spent the most time on familiarisation. According to the interviewees, this is due to missing legal knowledge, as micro-enterprises usually do not have a legal or compliance department and therefore had to familiarise themselves more intensively with the new legal norm. Small enterprises interviewed have taken a very pragmatic approach, which is not representative. In the opinion of the experts interviewed, the efforts required are to be considered higher.

Figure 2: Time required for familiarisation by company size in hours



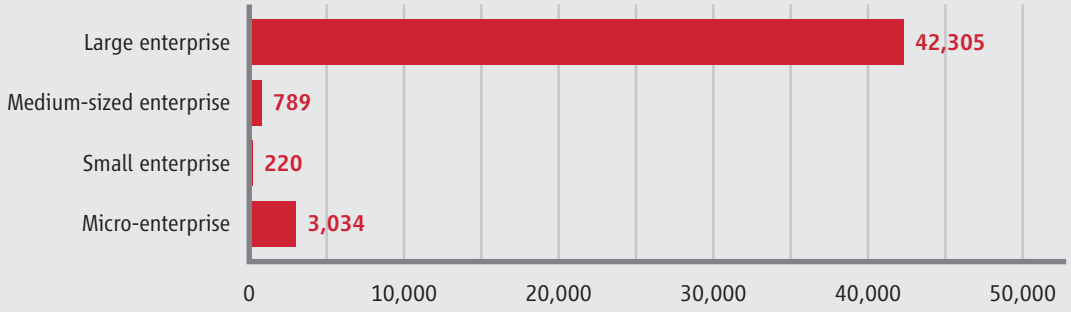
Missing competencies can be substituted by contracting external consultants. Likewise, efforts for the review of regulatory compliance or the preparation of documents can be outsourced to external service providers. This is also reflected in the surveyed spendings on consulting services (Figure 3).

Differentiated by company size across all companies and countries, the results show that micro-enterprises and large corporations invested more in consulting services than their small and medium-sized counterparts.

472 Company categories by threshold for employees and revenue: micro-enterprises with up to 9 employees and 2 million EUR in revenue, small enterprises with up to 49 employees and 10 million EUR in revenue, medium-sized enterprises with up to 249 employees and 50 million EUR in revenue, large enterprises with 250 or more employees.

473 At country level, these data are not available due to the study design, as the number of different company sizes per country is too small.

Figure 3: Average costs for consulting services by company size in EUR



A possible explanation for this pattern, as company representatives reported, is that micro-enterprises often lack sufficient resources and/or competencies and are therefore particularly dependent on external service providers. Especially for Austria, where 99,6 per cent of the companies are small or micro-enterprises[474], these expenses are in relation to lower revenues and were therefore described as an additional financial burden by the company representatives.

Large companies, on the other hand, frequently have more complex business models that operate with personal data. In this respect, the companies reported that external consulting was necessary to ensure a timely and sufficient level of compliance to prevent sanctions and damage to the companies' brand reputation. Compared to micro-enterprises, large companies also represent potential audit cases which, if sanctioned, would have resulted in severe penalties.

Creation of the RPA

According to Art. 30 GDPR, processing activities involving personal data must be documented in a directory. Hence, the RPA consists of a variety of process documentations, which determines the size of the RPA. To create an RPA, companies must systematically review their business processes and assess whether personal data are being processed. Even with an existing RPA under former national legislation, companies conducted a complete revision. Thus, the effort is directly attributable to the GDPR and was also reported as a significant bureaucratic burden.

For the documentation, companies used templates to collect and store the required information per processing activity. As part of the survey, all participants were asked if the design of the templates had an impact on the time spent on creating the RPA. Templates could not be identified as a systematic influencing factor.

474 Bundesministerium für Arbeit und Wirtschaft, "KMU in Österreich", 2023.

Costs for recreating the RPA result from the average time spent and corresponding labour costs[475] to document a processing activity and the associated personnel costs as well as the average number of processing activities included in the RPA. Differences in the costs of documenting a processing activity mainly stem from the different labour costs per country (Table 33); the surveyed companies in Austria needed more time on average to document a process activity than their counterparts in Germany, France or Italy.

Table 33: Cost composition for creating the RPA

	Time spent documenting one processing activity in hours	Costs of documenting one processing activity in EUR	Average size of the RPA (number of processing activities)
Austria	13	643	33
France	1	49	248
Germany	5	325	379
Italy	4	237	45

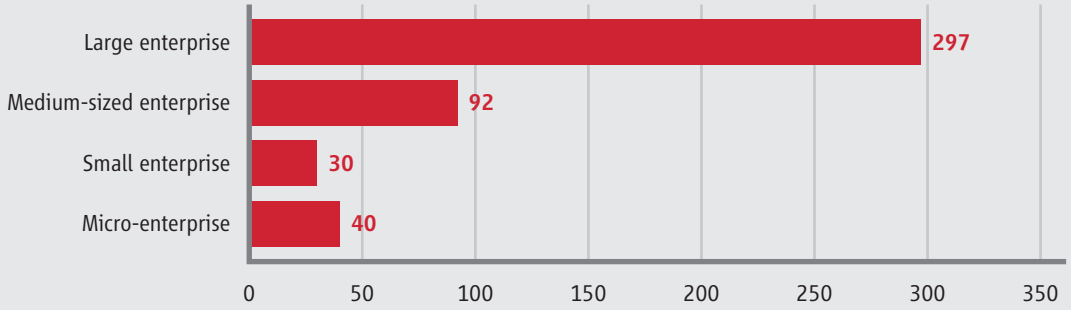
In addition, separate consulting costs for the preparation of an RPA were reported for Austria and Italy, averaging 1,124 euros and 3,582 euros, respectively.

Consequently, bureaucratic costs depend on the number of processing activities, which in turn are highly dependent on the size of the company and its business model. Again, a differentiation by company size provides further insight into bureaucratic costs and their effects.

Figure 4 confirms that large companies have significantly more documented processing activities (size of the RPA) than small, medium-sized or micro-enterprises. This was further confirmed by the experts interviewed and highlighted that especially companies with a B2C business model are affected by Art. 30 as most of their business processes contain personal data.

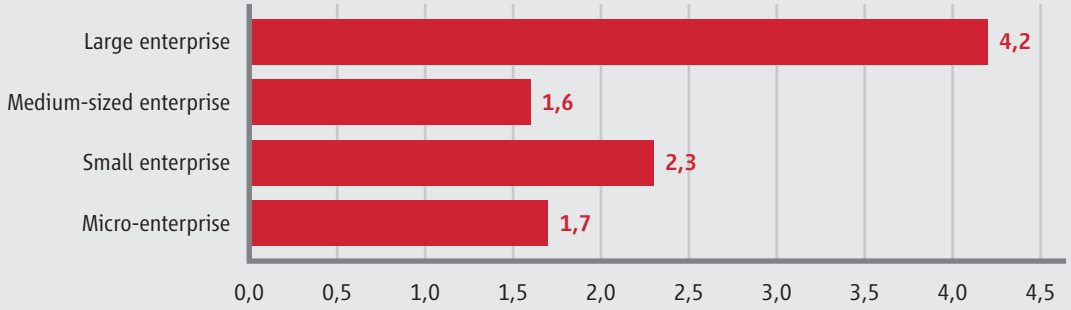
475 Personnel costs are determined using the average time per standard activity multiplied by the hourly labour costs. The total cost is calculated by multiplying the average cost per case by the average number of processing activities.

Figure 4: Size of the RPA in terms of processing activities by company size



The fact that large companies are particularly affected by the requirements of Art. 30 GDPR is also reflected in the reported time spent. Figure 5 shows that large companies spent significantly more time on the creation of the RPA than their smaller counterparts.

Figure 5: Time spent per processing activity by company size in hours

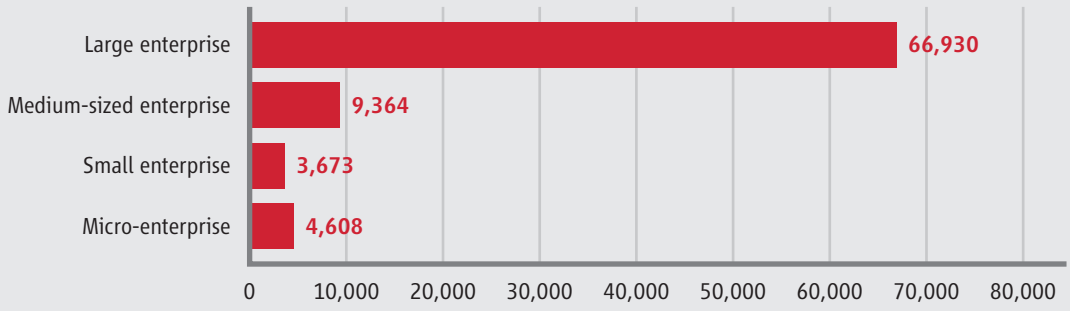


While micro-, small and medium-sized enterprises require on average about 2 hours for the documentation, the effort in large enterprises amounts to approximately 4 hours on average.

Comparing small and medium-sized companies, the results show that micro-enterprises are affected to the same degree as small businesses, even though they have significantly fewer employees and lower revenues. These findings confirm expert statements that Art. 30 imposes a distinct bureaucratic burden on micro-enterprises and that the benefitcost ratio is not balanced. The companies surveyed were asked whether they use the directory for other purposes or business processes. The majority reported that the RPA is only used for compliance reasons. An indirect value added mentioned was the increased involvement of company representatives, including the founder/management, with the processing of personal data. Consequently, compliance costs from Art. 30 are higher for large companies than for small and medium-sized

enterprises, due to the higher number of processing activities. The data also confirm that the effort for micro-enterprises is higher than for small businesses (see Figure 6).

Figure 6: Compliance costs for creating the RPA by company size in EUR



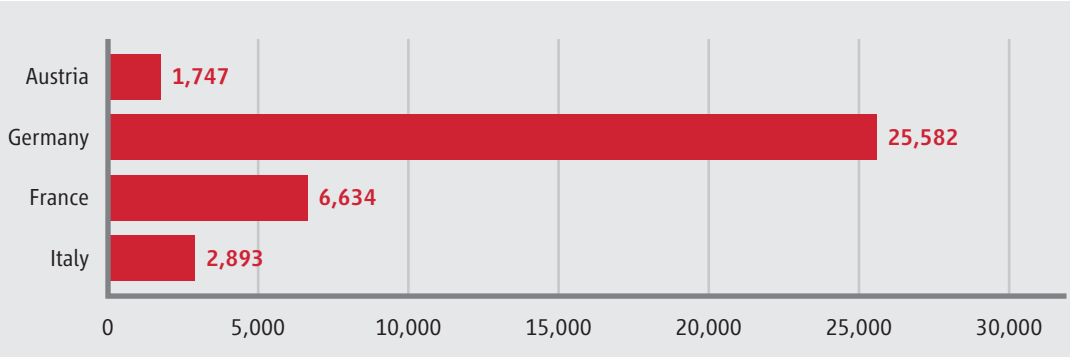
Maintenance of the RPA (recurring efforts and costs)

Due to the information required for the documentation of a processing activity, the RPA must be regularly reviewed to ensure overall compliance. The interviews showed that most of the companies review their RPA once per year. Hence, the associated efforts and costs are annual and recurring for companies. They represent a regular financial burden in addition to the cost of the initial preparation or revision of the RPA.

The companies interviewed stated that they spent annually an average of 1 hour per processing activity to maintain the included information. There was no country difference identified for the estimated time required to maintain a processing activity; thus, compliance costs are dependent on the average size of the RPA.

The compliance costs for maintaining the RPA are presented in Figure 7.

Figure 7: Compliance costs for maintaining the RPA in EUR



In analogy to the previous findings, the differentiation by company size shows that the costs are higher for large companies than for small and medium-sized enterprises (Figure 8).

Figure 8: Compliance costs for maintaining the RPA by company size in EUR

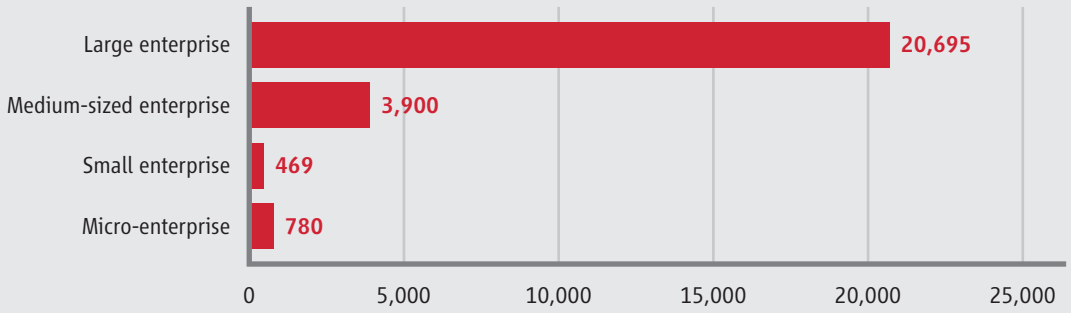
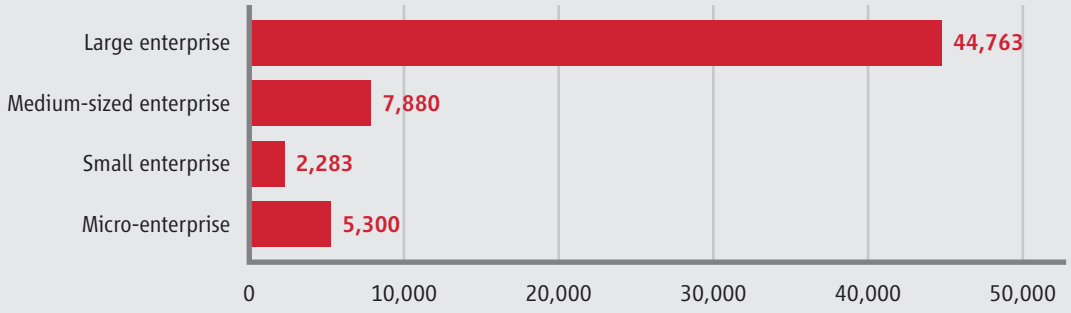


Figure 9 shows that large companies also spend more money on annual consulting services than small or medium-sized companies. The trend of micro-enterprises incurring higher costs for compliance with the GDPR is also reflected in the annual expenditures for consulting services.

Figure 9: Annual costs for consulting services regarding the GDPR in EUR



As stated above, according to company representatives and experts, this is due to the resources available to micro-enterprises and the complexity of the business models of large companies and their concern to avoid brand damage from compliance sanctions.

In summary, the bureaucratic burdens for compliance with Art. 30 depend on the size of the company (number of employees/revenues) rather than on country-specific differences. With approximately 45,000 euros, the compliance costs for one article of the GDPR represent a significant expense even for large companies, with the value added rated as very low by the interviewed companies' representatives. The same applies for micro-businesses, for whom

the GDPR means additional compliance costs in relation to the inherent lower revenues due to their size.

Notification of a personal data breach to the supervisory authority

The costs for reporting a data protection breach to comply with Art. 33 depend on the type of case. The following data refer to *typical* data protection incidents, i.e. whose processing entails comparable efforts.

The company managers interviewed reported that conducting internal processes requires the most time. The notification itself takes less effort than the gathering of information and the assessment of whether the incident requires a notification.

Systematic differences due to the implementation of the reporting process were identified in France (see Figure 10). The online platform for notifying the French supervisory authority was described as not user-friendly and non-optimal. For instance, it is impossible to save a draft during the notification process or to return to previous pages for modifications. Hence, it was stated that submitting the notification requires up to 5 hours, whereas the average time in Austria, Germany and Italy was estimated to be approximately half to one hour depending on the incident.

Insufficient user experience of the platform in France increases efforts for companies.

Figure 10: Effort to report a personal data breach in hours

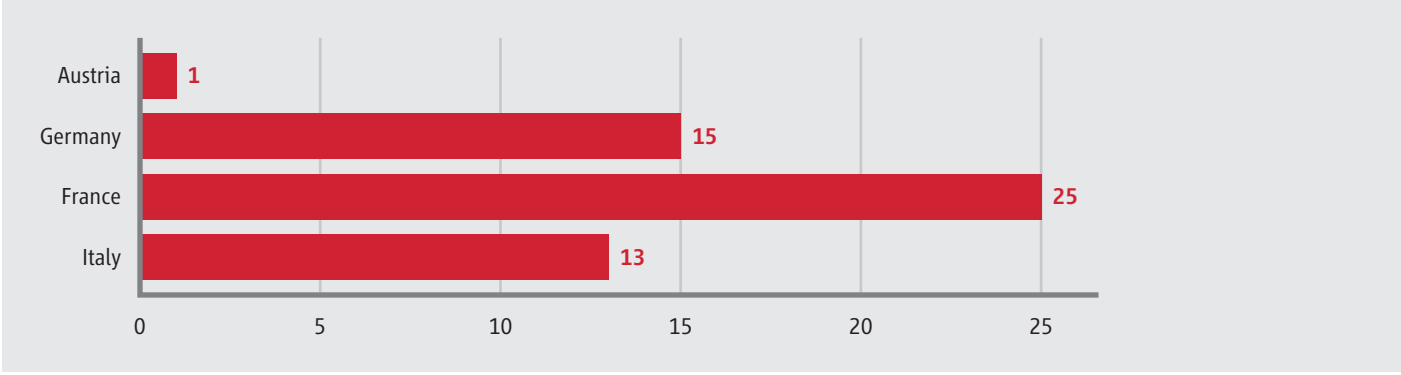
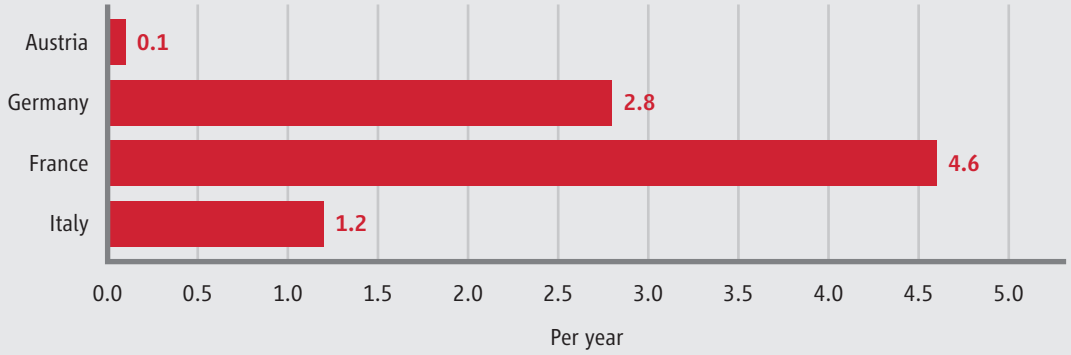


Figure 11 shows that the interviewed companies in France have the highest average number of reported data breaches[476] (due to the low number of responses, the value for Austria is inconclusive).

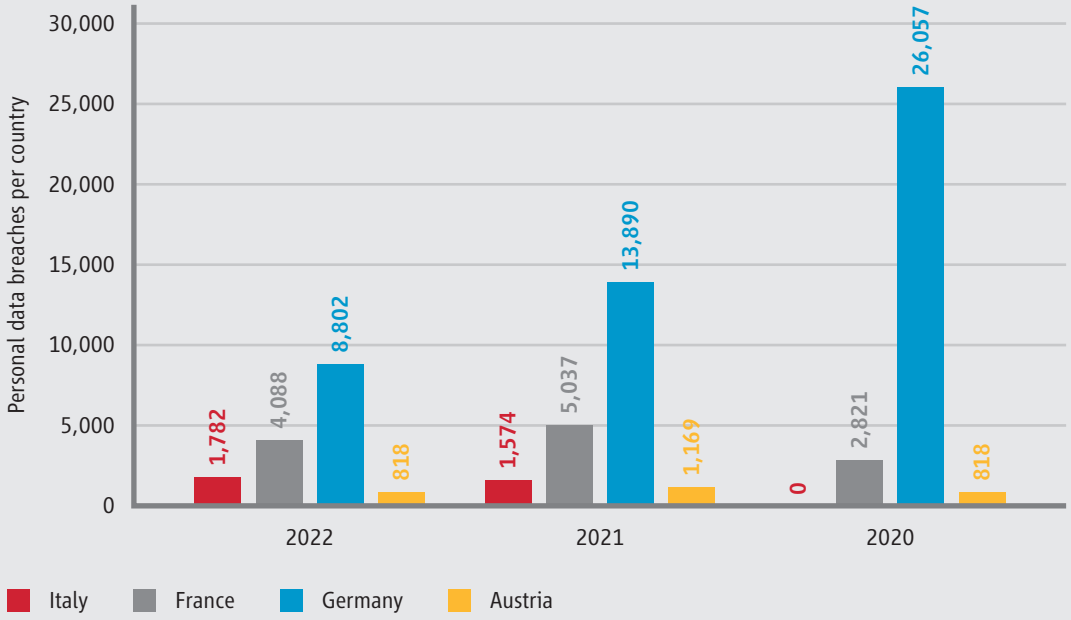
476 Since the information on the violation of data protection is sensitive data, it is impossible to exclude the possibility of a bias in the responses of the companies surveyed. In particular, the number of reported incidents is subject to a potential bias, which is an important factor in calculating the average processing time.

Figure 11: Average number of reported personal data breaches per year



Statistics regarding the number of data breaches reported shown in Figure 12 corroborate the pattern that German and French companies report personal data breaches more often than Italian and Austrian ones. The figures also confirm that Austrian companies are less likely to report.

Figure 12: Official reports on personal data breaches per country



Sources: Austria: Österreichische Datenschutzbehörde (2023): Datenschutzbericht 2022, France: Daten der CNIL (https://www.data.gouv.fr/fr/datasets/notifications-a-la-cnil-de-violations-de-donnees-a-caractere-personnel/), Germany: https://www.dsgvo-portal.de/ (Compliance Essentials GmbH), Italy: DLA Pieper (2022): DLA Piper GDPR fines and data breach survey.

It should be noted that the absolute number of reports is only one indicator and that it also depends on the number of companies and organisations in the country. Similarly, it is likely

that the actual number of data breaches may be higher, as not all breaches are reported and some may be undetected.

Many possible explanations for this pattern exist; for example, data protection incidents may be identified less frequently or the security structure may be better than in other countries. However, it is more likely that companies do not report incidents, either because they do not consider them worth reporting or because they generally refrain from reporting them. According to the experts interviewed, the latter is the case especially in Austria and Italy.

Table 34 shows the compliance cost for reporting a personal data incident based on the country's labour costs.

Table 34: Compliance costs of a data privacy incident

	Costs per data privacy incident in EUR
Austria	Reported number of data privacy breaches is too small to draw any reliable conclusions regarding the bureaucratic burdens. The information from the expert interviews indicates a three-digit number comparable with Germany and Italy.
France	1,174
Germany	880
Italy	749

The findings further support the statement of the surveyed companies in France that the form of implementation significantly influenced the time spent on the notification. The estimated time of half to one hour to submit a data breach incident to the authority was also confirmed by Austrian experts. Thus, an effort similar to the ones in Germany or Italy can be assumed for Austria.

The implementation of Art. 33 is therefore not expected to result in a distinct bureaucratic burden in Austria, Germany and Italy. For France, on the other hand, the optimisation of the reporting process to the authority would lead to a reduction in bureaucracy for companies.

With the GDPR and the associated sanctions, it can be assumed that the actual efforts have been increased and the associated expenses often represent additional costs that were not incurred in this form before. Moreover, due to the media coverage of data breaches and still increasing user awareness, companies will continue to address the obligation of Art. 33 to avoid damage to their brand reputation.

3. Perceived burdens

The statements of the company representatives on the perceived burdens are summarised below. The highlighted aspects were rated as particularly burden-some across all countries, thus complementing the quantitative picture of the bureaucratic burden.

Personnel resources and existing knowledge were noted as a distinct influencing factor. Especially small and medium-sized enterprises as well as micro-enterprises considered implementing the new data protection regulation to be challenging, as they often lack legally trained staff or compliance or legal departments. In particular, the missing specification of the indeterminate legal terms used in Art. 30 GDPR requires legal knowledge to translate the requirements into operational practice. Companies required a great amount of time and often the support of external consultants.

While larger companies could rely on trained staff and/or their own compliance departments, it was noted that many people were necessary for the creation of processing directories. On the one hand, this leads to a higher effort in general; on the other hand, the complexity of the data protection organisation is increased. Particularly in large companies operating in multiple countries, it was reported that additional employees have been hired and that data privacy coordinators (DPCs) process data privacy issues at the local premisses. This is associated with a permanent increase in personnel costs, in response to the requirements and the complexity of the GDPR due to different opening clauses[477] across European countries.

For companies of all sizes, the initial creation of the RPA required an analysis of their business processes, which was regularly reported as a burden. While it took significant efforts for large companies, especially those with B2C business models, small and medium-sized enterprises reported that the effort was too high compared to the overall value. One reason for this is that the RPA was only in few cases used for other business processes; therefore, the effort was associated exclusively with compliance. Even large companies that already work more in a process-oriented manner rated the effort as high, although they were able to benefit from existing management systems and process documentation.

Maintaining and updating the RPA is perceived as a burden, especially when a detailed review involving departments is conducted annually. The reasons provided for this were that time must be spent on their work on data protection, which in turn requires acceptance and awareness, which is often missing outside the legal or compliance departments.

477 Not applicable for Art. 30 and 33 GDPR.

Along with a stronger focus on data protection through the GDPR, there is also a need to raise awareness among employees, e.g. through regular training. The companies surveyed reported that trainings were conducted regarding both the creation of processing directories and the reporting of data protection incidents. Data protection in general also requires regular follow-up trainings which impose additional costs on companies.

Educating and training employees were cited as the biggest challenge regarding Art. 33. To report a data privacy breach to the supervisory authority, the incident has to be recognised and reported to the data protection officer (DPO). The training and/or instructions required for this are often perceived as a burden and might lead to lower acceptance among the workforce. One of the reasons for this is to protect the company from potential sanctions or damage to its brand reputation.

Proposals to reduce regulatory burdens

The majority of the suggestions expressed by the companies relate to the support of the data protection authority. The following aspects were expressed in all the countries surveyed and can be understood as both country-specific and cross-country proposals to reduce the regulatory burdens of Art. 30 and 33.

Companies want more support and feedback from data protection authority

- Improving guidance and support for companies, by providing guidelines and best-practice examples. As many companies recognise the necessity and the potential benefits of the GDPR, they would like to see more support in the practical implementation of the data protection requirements.
- Regarding Art. 30, the data protection authority could use guidelines to support companies regarding the scope of the directory. The provision of templates was considered insufficient because the terms did not define the scope or depth of the information to be included.
- Consistent templates across European countries for the RPA were mentioned as a potential for optimisation, especially by large companies that operate across several countries. As Part A of the study shows, there is currently a rather heterogeneous approach while the GDPR is implemented as a European standard at its core.
- The administrative implementation of Art. 33 should be standardised as an online solution. Reporting via an – ideally automated and user-friendly – online platform would save time, especially if company data can be stored and thus the number of entries can be reduced.

- Feedback from data protection authorities on the reporting of data protection incidents is another possible area for improvement. Many of the companies interviewed did not receive any feedback after reporting a personal data breach. This led to a certain degree of uncertainty as to whether a case is considered closed and what conclusions can be drawn for operational practice.

Suggestions for improvement with regard to the GDPR itself were also made but are significantly more difficult to implement.

The aspect most frequently mentioned by companies is the opening clause for small and medium-sized enterprises (SMEs) and micro-enterprises of Art. 30 (5). This is associated with the criticism that companies of different sizes, business models or industries are subject to the same requirements, regardless of how much personal data they process.

Binding defintions reduce uncertaincy.

A binding definition of indeterminate legal terms was also expressed as an improvement that should be addressed not only through the provision of guidelines and templates, but also through the legal norm itself. In summary, it can be concluded that a reduction of bureaucratic burdens would very likely lead to a more positive perception of the GDPR and data protection in general. In particular, the proposals on the role of national data protection authorities seem to be a viable short-term option. Naturally, it must be considered that national supervisory authorities are subject to restrictions in terms of the support they can provide given their resources.

III. Austria

1. Transposition in national law

Prior to the new General Data Protection Regulation (GDPR), the Data Protection Act (Datenschutzgesetz, DSG) was already applicable for the processing of personal data by public and private entities. The Data Protection Act came into effect on 1 January 2000 and has been amended several times (most recently in February 2023). Since 25 May 2018, it has regulated the protection of personal data in Austria together with the GDPR.

The record of processing activities (RPA) according to Art. 30 was introduced as part of the GDPR and replaced the data processing registry ("Datenverarbeitungsregister") that existed under the DSG. Art. 33 concerns the notification of personal data breaches to the supervisory authority. The DSG does not contain specific provisions regarding the duties under Art. 30 and 33 GDPR. Furthermore, there is no secondary legislation in Austrian law that contains information on the implementation or enforcement of Art. 30 and 33 GDPR. Since both Art. 30 and 33 do not contain any opening clauses, there is no deviating national interpretation in Austria.

In Austria, the data protection authority is responsible for monitoring and enforcing compliance with the GDPR. It is an independent administrative authority that is attached to the Federal Chancellery.

2. Creation of records of processing activities

To comply with the requirements of Art. 30, companies must familiarise themselves with the requirements, (initially) create the RPA and regularly maintain it with regard to changes in responsibilities or processing activities that have been added (see Table 31). No deviations from that process were reported in Austria.

As there exists no official definition of the notion of a "processing activity" and the required level of detail in the RPA, companies regularly used and are still using templates to create or revise their RPA. However, the Austrian data protection authority provides no official template for the RPA. Thus, compared to France, Italy or Germany, the Austrian authorities provide the lowest amount of guidance regarding Art. 30 (see Part A, Chapter III).

3. Notification of a personal data breach to the supervisory authority

In Austria, in contrast to the other countries examined, Art. 33 is not implemented as an online notification to the local data protection authority. Companies can either use the data breach notification form or submit data breaches by mail or by e-mail (see Part A, Chapter IV). No deviations from the standard process (Table 31) were reported in Austria.

4. State of research on bureaucratic burdens arising from the GDPR in Austria

The state of research in Austria provides limited insights into the bureaucratic burdens resulting from the GDPR. Only a small number of studies address the bureaucratic burdens of the GDPR for companies[478]. The results of these surveys indicate that the implementation of the GDPR is associated with a significant effort.

A study on the digital transformation of SMEs in Austria states that the GDPR has a significant impact on the digital development of SMEs and engenders considerable obstacles for companies. More than half of the companies surveyed rated the implementation of the GDPR as the greatest challenge for digitalisation in 2018[479]. In the following year, the GDPR also ranked first among the top 5 challenges for digitalisation in companies, although the proportion declined and companies felt better-informed[480]. Another study deals with bureaucratic burdens

478 E.g. Arthur D. Little (2018, 2019); Enichlmair et al. (2019); Schmiedhofer (2019).

479 Arthur D. Little (2018), p. 12.

480 Arthur D. Little (2019), p. 14.

in Lower Austrian trade and commerce[481]. According to the study, the GDPR has resulted in a higher bureaucratic burden in companies, especially in the implementation phase[482]. In this context, bureaucratic expenses are a burden especially for small and medium-sized enterprises, as they possess fewer resources and often do not have their own legal department[483]. Overall, according to the authors, the quantified costs for data protection in Lower Austrian trade and commerce were 12.2 million euros in 2019[484]. Finally, a qualitative survey of 24 data protection officers of Austrian companies shows that the GDPR was almost constantly perceived as a burden. However, this was especially the case during the implementation phase[485].

The studies show that the bureaucratic burden of the GDPR is a relevant issue for companies in Austria. However, the studies provide little detail or do not quantify the costs associated with the efforts to comply with the GDPR for the entire Austrian economy. Therefore, this study includes 13 interviews with both companies and experts in the field of data protection in Austria to provide further insights into the implementation and the resulting bureaucratic burdens of Art. 30 and 33.

5. Perceived burdens and compliance costs

a) Measurable burdens

To determine the burden, the responsibility for compliance with data protection requirements was determined as a first step in the interviews. A special characteristic in Austria is the structure of the economy: the Federal Ministry of Labour and Economics reports for 2021,

> that 99.6 per cent of companies are SMEs (companies with fewer than 250 employees and total sales of up to 50 million euros or total assets of up to 43 million euros). Approximately 87 per cent of the SMEs were micro-enterprises with fewer than ten employees. This category also includes one-person companies, which accounted for around 41 per cent of all companies in 2021. About 11 per cent of SMEs were classified as small enterprises (10 to 49 employees) and 2 per cent as medium-sized enterprises (50 to 249 employees)[486].

As a result, external service providers are often appointed as data protection officers for companies in Austria. Especially micro-enterprises lack the necessary resources and/or competences

481 Enichlmair, H. et al. (2019).

482 Ibid., p. 20.

483 Ibid., pp. 2/46.

484 Ibid., p. 46.

485 Schmiedhofer, H. (2019), p. 67.

486 Bundesministerium für Arbeit und Wirtschaft, "KMU in Österreich", 2023.

to incorporate the subject of data protection within the company. In those cases, the management was the contact person for the external consultants. In larger and medium-sized enterprises, the role of the data protection officer was held by executives in the legal or compliance department. In both cases, consulting/managerial remuneration is to be applied. For Austria, an hourly labour cost of 49.90 euros is applied to calculate the financial burden of carrying out the activities associated with Art. 30 and 33 GDPR.

Effort for Art. 30

The companies interviewed stated that the main effort of complying with Art. 30 GDPR was incurred at the time of implementation. The process started with an assessment of the company's existing processing activities, followed by the creation of the RPA. The familiarisation with the requirements of the GDPR and the creation thereby overlapped. Despite the fact that a few companies already had processing directories (under the requirements of the former DSG), they decided to conduct a general revision. Therefore, the efforts of creation and revision are not further distinguished.

The average time of familiarisation with the requirements was estimated to be 27 hours. These estimates refer to the total time required to become familiar with the GDPR since the majority could not separately estimate the time required for Art. 30 or 33. The interviewed companies in Austria substantially relied on the expertise of external data protection officers; thus, the management's engagement in familiarisation with the requirements was relatively low. The familiarisation was accomplished through joint meetings and/or executive training by the external data protection officer.

In the absence of official guidelines, Austrian companies use the templates and information provided from Bavaria.

To create the RPA, companies stated that they used templates, which were either provided by the Austrian Federal Economic Chamber (WKO) or an external consultant. In Austria, the authorities did not and still do not provide an official template or guidelines. Due to these circumstances, a company from Austria reported that it had used templates from the Bavarian authority for the preparation.

Table 35: Effort for familiarisation in Austria

Standard activity	Average time spent in hours	Average costs consulting in EUR	Personnel costs in EUR	Total costs in EUR
Familiarisation	27	1,043	1,329	2,372

The average time to create the RPA within the interviewed companies in Austria was estimated to be an average of 419 hours. With an average of 33 activities, the RPA is smaller than in France, Germany or Italy. This results in an average of 13 hours and 643 euros of personnel costs for the creation of one processing activity. As the companies interviewed relied on an external consultant for the initial creation, external costs of 3,582 euros are associated with the initial creation. Based on the average number of processing activities and costs for external consulting services, this results in total costs of 24,494 euros for the initial creation of the RPA.

Companies in Austria spent more time on creating the RPA (time per processing activity) compared to their counterparts in France, Germany or Italy. The interviewees reported that due to the small size of the company, a review of the business processes was often necessary before they were able to create the RPA. In smaller companies, processes have frequently not been documented, which has already been done in large companies – e.g., through other certifications or process management in general.

Seven of the interviewed companies in Austria stated that the RPA is reviewed once per year. The following expenses are therefore reported as annual costs. As several companies in Austria did not update their RPA since the first compilation, the efforts are consequently lower than in France, Germany or Italy. As a result, the number of available data points for the effort of maintaining the RPA is lower compared to other countries and is therefore reported as an indicative value.

The average time for the maintenance of the RPA was estimated to be 35 hours. Based on the average of 33 processing activities, this results in 1.08 hours and 54 euros of personnel costs for the maintenance of one processing activity. Based on the average size of the RPA, this results in total costs of 1,747 euros per year. Experts confirmed that the effort for maintaining and updating the RPA is significantly lower than it is for the creation and was estimated to be approximately one hour per processing activity.

Table 36 summarises the standard activities to comply with Art. 30 GDPR.

Table 36: Effort for Art. 30 GDPR in Austria

Standard activity Art.30 GDPR	Average time spent in hours	Average number of processing activities	Average time spent per processing activity in hours	Personnel costs per processing activity in EUR	Average consulting costs in EUR	Total costs in EUR
Creation or revision	419	33	13	643	3,582	24,494
Maintenance (indicative)	35	33	1.08	54		1,747

Personnel costs were determined using the average time per standard activity multiplied by the hourly labour costs. The total costs are calculated by multiplying the average cost per case (processing activity) by the average size of the RPA.

In addition to internal efforts, the companies interviewed also use consulting services. This includes a flat fee for the external data protection officer and general consulting, for example, to obtain advice on legal changes, contract updates etc. In this regard, companies reported an average of 909 euros of annual costs. The companies interviewed were unable to differentiate the services with reference to Art. 30.

Compared with France, Germany and Italy, the annual costs for consulting are significantly lower in Austria. Experts stated that the general interest in the requirements of the GDPR has decreased considerably, which could explain the lower demand for consulting.

Extrapolation

In 2021, there were about 360,040 companies in Austria for which the GDPR applied. There are no reports on the implementation status of the GDPR or Art. 30 from the Austrian government. According to experts, the implementation level of the GDPR in general and Art. 30 in particular can be improved. Especially for SMEs, experts reported a lower acceptance and implementation rate than in larger companies.

According to a study by Deloitte from 2021, 36 per cent of the surveyed companies in Austria have already fully implemented the requirements of the GDPR, and another 46 per cent are at least compliant to a large extent. However, 11 per cent stated that they have only partially

completed the implementation. For 3 per cent, this topic has not been addressed or hardly at all, and 5 per cent did not know the status quo of their own company[487].

Assuming 8 per cent have not yet started or completed the creation of the RPA, this results in costs of 705 million euros.

Table 37: Extrapolation of efforts to create an RPA in Austria

Year	Number of legal entities in Austria	Estimated percentage of compliance with Art. 30 GDPR	Costs for initial compliance with Art. 30 GDPR in EUR	Costs in EUR
2021	360,040	92	24,494	705,518,673

Since several of the surveyed companies in Austria had not established a practice for updating and maintaining their RPA yet, this study does not include an extrapolation for those expenses. According to a study by Deloitte published in 2022, 47 per cent of the companies surveyed intend to conduct a review of their RPA[488].

Further research could address the financial implications of this process for companies.

Effort for Art. 33

In the companies interviewed, the responsibility for reporting a data breach is assigned to the data protection officer. For the Austrian sample, the reported number of data privacy breaches is too small to draw any reliable conclusions regarding the bureaucratic burdens. Experts estimated that the notification itself takes between half an hour and one hour, during which companies fill out a pre-defined document provided by the Austrian authority.

Official statistics[489] on data breaches under Art. 33 show an almost constant number of reported cases.

487 Deloitte (2021): Datenschutz in Zeiten von COVID-19.

488 Deloitte (2022): Deloitte Umfrage zum Datenschutz 2022.

489 Österreichische Datenschutzbehörde (2023): Datenschutzbericht 2022.

Table 38: Number of cases under Art. 30 in Austria

Year	Number of reported data breaches in Austria	Costs per breach in EUR	Total costs in EUR
2022	818	Data basis does not allow for an extrapolation of the financial expenses for Austria	
2021	1,169		
2020	818		

In comparison with the other countries surveyed, the statistic confirms that comparatively few cases are reported to the data protection authority in Austria. This is also reflected in our sample. Therefore, an extrapolation of the financial expenses is not possible with this data basis.

Due to the sample in Austria, a further differentiation of the effort with regard to a company's size and business model is impossible.

b) Qualitative burdens

In addition to the quantitative burdens of the GDPR described in the previous section, the qualitative statements of the respondents are used to specify the perceived burdens associated with Art. 30 and 33 GDPR.

In interviews with experts, attention was drawn to the importance of the special corporate structure in Austria for the implementation of the GDPR. There are many small and medium-sized enterprises (SMEs) in Austria, which are also significantly smaller than their counterparts in Germany. Smaller companies possess fewer resources and less know-how than larger companies; hence, the effort of implementing the GDPR tends to be higher. Accordingly, acceptance of the topic of data protection is low among smaller companies. According to the experts surveyed, this is reflected in a lower level of implementation of the GDPR in Austria compared to Germany.

The challenges of data protection for smaller companies in Austria became apparent in the phase of initial familiarisation with the requirements of the GDPR. Familiarisation with the requirements of the GDPR was often outsourced to external consultancies due to a lack of resources and knowledge within the companies interviewed. As a result, the burdens of the GDPR tended to be reflected in higher expenses for external services in the initial phase.

This also refers to the creation of the RPA based on Art. 30 GDPR. The necessary templates were provided by consultancies or the Austrian Economic Chamber ("Wirtschaftskammer

Österreich"). To complete them, companies again relied on external support, as they lacked competencies since the terms and categories used are primarily legal terms and have little relation to their daily business practice.

Since large companies usually have more processing activities, the creation of the RPA is more time-consuming than in smaller companies. For smaller companies, on the other hand, the identification of their data processes was a time-consuming process in the implementation phase. One SME surveyed had not implemented the directory at all because the effort would be disproportionate to the benefit.

Regarding the maintenance and updating of the RPA, the statements of the interviewed companies and experts were heterogeneous. While some companies conducted regular reviews, others did not. Smaller companies lacked the incentive to maintain the directory due to missing enquiries from authorities and customers. Lack of awareness and lack of further benefits of the RPA were also mentioned as reasons for not maintaining it regularly.

6. Proposals for reducing bureaucratic costs

Respondents' feedback on optimising data protection procedures and regulations for businesses is described as follows. On the one hand, suggestions refer to the GDPR in general, and on the other hand to Art. 30 and 33 specifically.

Several of the companies surveyed requested better communication by the authorities. For instance, feedback from the Austrian authorities was often missing and their work is lacking transparency. In addition, the authorities should improve their communication of the benefits of the GDPR to increase acceptance among businesses. More assistance in the implementation of the GDPR and specifically Art. 30, for instance, in the form of information and advice services and templates, was also suggested.

The legal text was criticised for containing a large amount of formalism and therefore often being difficult to understand and implement in practice. Thus, the transfer of the GDPR into practice requires a great deal of knowledge and resources within the companies. Suggestions for improvement included having clearer definitions and a higher reference to business practice, for example, in the form of concrete recommendations or examples of typical processing procedures.

Another point of criticism concerns the lack of differentiation by company size and type in the application of the GDPR. According to the interviewees, the rules are particularly useful for large companies, but not for small and medium-sized ones and enterprises that hardly work

with personal data. In this context, Art. 30 (5), according to which SMEs are exempt from the obligation to maintain the RPA, was pointed out in the interviews. However, this exemption is currently not applicable, since even basic business processes include special categories of personal data under Art. 9, for example, the payroll process. According to the experts interviewed, this would lead to an overall increase in acceptance of the GDPR among SMEs in Austria. Additionally, respondents also suggested a consistent EU-wide implementation of Art. 30. The GDPR leaves too much room for interpretation; hence, a coherent standard and binding templates would be helpful.

Regarding Art. 33, an automated, consistent process for data breach notifications to the authority was suggested. Currently, the data breach notification is conducted in text form and submitted via e-mail. In addition, many companies have low awareness of data breaches and how to report them to the authority. Thus, increasing awareness of data breaches as well as sufficient monitoring by the authorities could contribute to a successful implementation of Art. 33.

Austrian companies suggest an automated and consistent process

IV. France

1. Transposition in national law

The General Data Protection Regulation (GDPR) was introduced in France in the continuity of the previous French Data Processing and Civil Liberties Act ("Loi Informatique et Libertés"), which has been applicable to the processing of personal data by public and private entities in France since 1978. On 25 May 2018, the GDPR came into force in France and was integrated into the previous Act by the Personal Data Protection Act of 20 June 2018.

Thus, the Personal Data Protection Act modified the previous Data Processing and Civil Liberties Act so that the French law would comply with the new EU requirements[490]. With this Act, the GDPR was also placed under the responsibility of the National Commission for Data Processing and Liberties (Commission Nationale de l'Informatique et des Libertés, CNIL) and, in the interest of all stakeholders, the structure of the former Act was maintained.

The introduction of the GDPR in France led to a significant change in the logic of compliance and controls carried out by the French supervisory authority, moving towards an increased responsibility for institutions by introducing the obligation to immediately demonstrate compliance with the new legal framework instead of a retrospective assessment of compliance by the

490 The French Personal Data Protection Act also modified the previous legislation by integrating the new EU requirements with regards to penitentiary personal data and processing activities (Directive (EU) 2016/680, available at https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex:32016L0680, online, accessed 29 March 2023).

CNIL. The former supervisory system, which was based on the expost assessment of compliance with the legal requirements by the supervisory authority (CNIL), is no longer applicable[491]. Instead, the GDPR introduced the obligation for all the entities to immediately demonstrate their compliance with the new legal framework in case of control. In return, the CNIL's competencies and resources have been significantly expanded by the Personal Data Protection Act.

The record of processing activities (RPA) was first introduced in France by Art. 30 GDPR. As the logics of compliance and control were not the same prior to the implementation of GDPR in France, the notification of personal data breaches to the supervisory authority was also first introduced in France by Art. 33 GDPR. Moreover, since both Art. 30 and 33 do not contain any opening clauses, there is no deviating national interpretation in France.

In France, the CNIL is responsible for compliance with the GDPR. The CNIL is an independent administrative authority that is subject to the French government.

2. Creation of records of processing activities

To comply with the requirements of Art. 30, companies have to familiarise themselves with the requirements, (initially) create the RPA and regularly maintain it with regard to changes in responsibilities or processing activities that have been added (see Table 31). No deviations from this process were reported in France.

As there is no official definition of the notion of a "processing activity" and the required level of detail in the RPA, companies used and are still using templates to create their RPA. Compared to Italy, the official templates made available by the French supervisory authority[492] provide more details on which information should be included in the RPA, e.g. contact details of the controller, the joint controller and the data protection officer of the entity, necessary details on the processing activities carried out and additional information that is not explicitly required by the GDPR (for instance, the date of creation of the processing activity, as well as the date of revision, if any). The French templates are thus more similar to the German ones than to the Italian ones.

491 Prior the GDPR, all entities concerned by the Data Processing and Civil Liberties Act had to declare to the CNIL all data processing activities performed. The CNIL then assessed their compliance. With the GDPR, this compliance and control logic only remained for specific sectors (police/justice and for some particular processing activities of health data).

492 RPA templates provided by the CNIL, available at https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement (online, accessed 29 March 2023).

3. Notification of a personal data breach to the supervisory authority

Art. 33 is implemented in France as an online notification to the CNIL. The notification of a personal data breach to the supervisory authority must be submitted through a specific electronic proceeding, made available on the CNIL's website[493]. Notifications by phone or e-mail are not possible in France, unlike in Germany and Austria.

As the logics of compliance and control were not the same prior to the GDPR coming into force neither a similar notification process nor the notification itself existed before. This was a novelty introduced with Art. 33. No deviations from the standard process (see Table 31) were reported in France.

Art. 33 provides the option of a preliminary notification. As stated by the French companies, they sometimes make use of this possibility, especially when the 72 hours set by Art. 33 (1) are not enough to collect sufficient information regarding the incident or for conducting a risk assessment on the notified data breach. However, in most cases, companies do not use this option and directly carry out the complete notification.

4. State of research on bureaucratic burdens arising from the GDPR in France

The state of research in France provides very limited insights into the bureaucratic burdens imposed by the GDPR. Only two studies address the bureaucratic burdens arising from the GDPR for companies in France.

Much like in Germany, the findings of the available studies indicate that the implementation of the GDPR is associated with a high level of effort in France. Smaller enterprises seem to have faced higher burden than larger ones regarding the implementation. This is also true for companies which never had an RPA before compared to those who already had such records to comply with the previous Data Processing and Civil Liberties Act.

In the first study[494], the authors demonstrate that the digitalisation of processes in companies produced significant impacts on how businesses collected, managed and processed personal data. Digitalisation led to an increased number of data processing activities in companies which did not exist before. At the same time, however, digitalisation allowed data processing activities to become more effective, for instance, with the introduction of digitalised direc-

493 CNIL, Notification d'une violation de données personnelles, available at https://notifications.cnil.fr/notifications/index (online, accessed 29 March 2023).

494 Boulesnane, S., Bouzidi, L. & Varinard, C., (2020), "RGPD et e-administration : besoins, pratiques et défis", available at https://www.cairn.info/revue-i2d-information-donnees-et-documents-2020-1-page-101.htm (online, accessed 3 April 2023).

tories. Moreover, the study highlights that the main obstacle for companies' compliance with GDPR remains the human factor. Indeed, it seems quite difficult for data protection officers (DPOs) to involve their colleagues in the compliance process, especially for recurring tasks related to maintenance of the RPA.

A second study carried out by KPMG[495] in 2021 provides further information on the burden for companies in France related to Art. 30 GDPR. The study covers a representative sample of SMEs and mid-caps[496] which already complied with the GDPR. For 80 per cent of them, actions for GDPR compliance have been motivated by the risk of sanctions by the supervisory authority, while 66 per cent have developed interest in the GDPR for reputational reasons. In most cases, it is the executive management or control functions that have carried out the first actions for GDPR compliance. Moreover, 80 per cent of the companies covered by this study declared they had appointed a DPO in 2021. According to this study, the realisation of risk assessments and the retention duration of personal data are the two least developed activities within French companies. These activities seem to be neglected due to scarce resources, both financial and human, within SMEs and mid-caps in France. Companies also faced difficulties regarding GDPR-related workload and with GDPR familiarisation, respectively 66 per cent and 39 per cent of them. However, for those companies which complied with GDPR requirements, the related activities brought important benefits such as a better data governance (not only for personal data) or a significant improvement of cybersecurity.

5. Perceived burdens and compliance costs

a) Measurable burdens

To determine the burden, the responsibility for compliance with data protection requirements was determined as a first step in the interviews. In the companies interviewed, the role of the data protection officer (DPO) is held by executives or staff members in the legal or compliance departments or directly by company owners, especially in small and medium-sized enterprises (SMEs). External service providers can also be appointed as DPO, but this was only the case for one company interviewed in France. Looking at multinational companies specifically, DPOs generally provide support at the local or regional levels, while data protection coordinators (DPC) ensure global coordination and provide support to the local/regional DPO. In the companies interviewed, activities related to Art. 30 and 33 GDPR are sometimes directly performed by the DPO or business owner in SMEs. However, in most of the cases, they are conducted by managers, as in Austria and Italy, whereas in Germany, they are mostly carried out by

495 KPMG (2021), "Baromètre RGPD de KPMG France, RGPD : 3 ans après, une conformité en demi- einte ? Etat d'avancement de ce chantier au sein des entreprises françaises", available at https://kpmg.com/fr/fr/home/media/press-releases/2021/07/rgpd-conformite-etat-avancement-entreprises-francaises.html (online accessed, April 03 2023).

496 Differentiation into large-, mid- and small-cap companies based on market capitalization. Mid-cap companies have a market capitalisation between 2 billion and 10 billion USD.

executives in the legal or compliance department. Therefore, for France, an hourly labour cost of 46.96 euros is applied to calculate the financial burden of conducting the standard activities.

Effort for Art. 30

The interviewed companies in France made a clear distinction between the burden related to the initial familiarisation with the GDPR, the initial creation of the RPA (when needed) and the recurring tasks related to its maintenance. In some cases, the RPA already existed to comply with the previous Data Processing and Civil Liberties Act. It was thus revised to comply with the new GDPR requirements or completely renewed if needed. Therefore, the efforts of creation and revision are not further distinguished (Table 39).

Most of the companies interviewed reported that a project structure was created either before or with the introduction of the GDPR to coordinate the implementation of the GDPR in general between the different departments of the companies. The process started with the familiarisation with the GDPR requirements, followed by an assessment of the company's existing processing activities and then by the creation of the RPA. The familiarisation with the requirements of the GDPR and the creation overlapped. However, interviewed companies in France made a clear distinction between the burden related to familiarisation and the initial creation of the RPA (when needed).

The familiarisation with the GDPR and initial creation of the RPA (when needed) were managed within the project structure by the data protection officers responsible for the process. Since the creation of the RPA requires knowledge of all business processes, department representatives were also involved in the process, represented by their department managers. Even if the familiarisation with the GDPR and initial creation of the RPA are sometimes carried out in parallel within companies, especially when the RPA did not exist before GDPR came into force, interviewees made a clear distinction between the burdens incurred from GDPR familiarisation and those related to the initial creation of the RPA.

On average, the estimated time for familiarisation with GDPR requirements is 57 hours[497]. It should be noted that the interviewed companies in France, much like in Germany, already had legal and compliance knowledge given the former requirements of the Data Processing and Civil Liberties Act. Therefore, the effort required for familiarisation with the new GDPR requirements is probably lower than for companies that do not have these competencies.

497 Most of the companies interviewed for France could estimate the effort required for Art. 30 separately, distinguishing between the effort related to familiarisation, RPA creation and maintenance. However, Table 39 provides an overall overview of the effort related to Art. 30 (familiarisation).

Table 39: Effort for familiarisation in France

Activity	Average time spent in hours	Personnel costs in EUR	Total costs in EUR
Familiarisation	57	2,657	2,713

After the initial familiarisation phase, interviewees reported that trainings are sometimes organised within companies to raise awareness about the implications and requirements of the GDPR among the employees. These trainings are organised and managed directly by the DPOs or by external experts, such as specialised lawyers, specialised members from business organisations or even by experts from the French supervisory authority (group trainings, for instance, specially dedicated to SMEs). When the trainings were managed and organised by external experts, a detailed estimate of the costs was impossible; therefore, the related expenses are not included in the table above. Moreover, unlike enterprises in the other countries analysed, many interviewed companies in France did not use external consulting services for compliance with the GDPR, including familiarisation and the creation of the RPA. In these cases, those activities were entirely managed internally by DPOs and departments managers. Therefore, the total costs average of consulting for compliance with the GDPR was not representative and thus not included in the table above.

To create the RPA, interviewed companies in France stated that, unlike in Germany, Austria or Italy, they mostly use the templates made publicly available by the national supervisory authority[498] or templates provided by an external consultancy. Rarely, they used specific software dedicated to personal data processing or simple Excel sheets created from scratch by the company itself.

The average time required to create the RPA within the interviewed companies in France is estimated to be 259 hours, which is less than in Germany and Austria, but more than in Italy. With an average of 248 activities, the overall record is significantly larger than in Italy and Austria, but smaller than in Germany due to the size of the companies interviewed. This results in an average of 1 hour and 49 euros of personnel costs for the creation of one processing activity. Based on the average number of processing activities, this results in a total cost of 12,163 euros for the initial creation of one RPA.

498 CNIL, Le registre des activités de traitement – Modèle de registre, available at https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement (online, accessed 2 April 2023).

Table 40 summarises the burden related to the creation or revision of the RPA to comply with Art. 30 GDPR.

Table 40: Effort for the creation or revision of an RPA in France

Standard activity Art.30 GDPR	Average time spent in hours	Average number of processing activities	Average time spent per processing activity in hours	Personnel costs per processing activity in EUR	Total costs in EUR
Creation or revision	259	248	1	49	12,163

Personnel costs are determined using the average time per standard activity multiplied by the hourly labour costs. The total cost is calculated by multiplying the average cost per case (processing activity) by the average number of processing activities.

Main effort in France arises from annual review of the register

In most cases, companies interviewed for France state that the main effort of complying with Art. 30 GDPR was incurred by recurring tasks related to the maintenance of the RPA. A large majority of them reported that these tasks are conducted once per year through interviews organised internally within companies and during which the entire record of processing activities is reviewed and updated if necessary. The expenses below are therefore reported as annual costs. Since the maintenance of the RPA required knowledge of which data processing needs to be added into the record, or revised, interviews involved DPOs and members from the different departments concerned with data processing. The maintenance efforts are lower in France than in Germany or Italy, but higher than in Austria, both as regards the time spent on this activity and costs in euros.

The average time for the maintenance of the RPA is estimated to be 141 hours. Based on the average of 248 RPAs, this results in 0.6 hours and 27 euros for personnel costs for the maintenance of one RPA. Based on the average number of processing activities, this results in total costs of 6,634 euros per year.

In addition to internal efforts, the companies interviewed also use consulting services regarding the GDPR, for example, to obtain advice on legal changes, contract updates etc. In this regard, companies reported an average of 6,447 euros of annual costs for consulting services. Much like in Austria or Germany, the interviewees were not able to differentiate the services with reference to Art. 30.

Table 41: Effort for the maintenance of an RPA in France

Standard activity Art. 30 GDPR	Average time spent in hours	Average number of processing activities	Average time spent per processing activity in hours	Personnel costs per processing activity in EUR	Total costs in EUR
Maintenance	141	248	0.6	27	6,634

Extrapolation

Based on the data made available by the French National Institute of Statistics and Economic Studies[499] (Institut National de la Stratistique et des Etudes Economiques; INSEE), it is possible to extrapolate data for France related to the burden of maintaining the RPA. Table 42 provides an overview of these extrapolated data for France:

Table 42: Extrapolation of efforts for maintaining an RPA in France

Year	Number of legal entities in France in million	Share of entities matching sample in %	Number of comparable entities	Annual costs in EUR
2021	4.3	0.14	6,137	51,642,855

Effort for Art. 33

For all companies interviewed for France, the responsibility for reporting a data breach is assigned to the data protection officer.

Given the individuality of data breach cases, it is difficult to determine an estimate required to meet the requirements of Art. 33 in general. To obtain an estimate at all, companies were asked for the effort of "a typical" case. Those cases are generally less complex and thus to be considered standard cases.

On average, the time required to report a data breach for the entire process is estimated to be 25 hours, higher than in Germany (15), Austria (1.45) and Italy (13). Companies reported on average 5 data breaches per year, resulting in an effort of 5 hours and 257 euros per data

499 INSEE (2021), Les entreprises en France – Edition 2021, available at https://www.insee.fr/fr/statistiques/5758732?sommaire=5759063 (online, accessed 3 April 2023).

breach case. For more serious or wide-ranging data breaches, companies reported that the effort required is multiple times higher, but no data breaches of this type have been reported by the interviewed companies in France.

According to the interviewees, the burden incurred from Art. 33 GDPR in France is first related to the online platform for reporting a data breach, available through the French supervisory authority's website. This platform was described as not user-friendly and non-optimal. For instance, it is impossible to save a draft during the notification process or to return to previous pages for modifications. Thus, reporting a data breach to the supervisory authority requires finding a slot of several hours, typically approximately 5. Moreover, gathering all the information required for reporting a data breach within the 72 hours set by of Art. 33 (1) was reported as a major burden by the companies interviewed. Indeed, companies stated that 72 hours is far from sufficient to collect enough information regarding the incident and for conducting a risk assessment on the data breach. Therefore, notifications sometimes include approximate numbers, and companies chose to do pre-notification only, which is a possibility given by the supervisory authority in France.

Table 43: Effort for Art. 33 in France

Art. 33 GDPR	Average time spent in hours	Average number of reported data breaches	Average time per reported data breach in hours	Personnel costs per data breach in EUR	Total costs in EUR
Notification of data protection breach[500]	25	5	5	257	1,174

Considering the reported data privacy violations in France[501] over the last three years, Table 44 shows the extrapolated data for France.

Considering the increasing number of cases in France over the last years (except for 2022), further research could analyse underlying causes of this trend.

500 This includes the internal process of the notification of data protection breaches, the gathering of information regarding the incident, the internal risk assessment and decision of whether a notification to the supervisory authority is necessary and the notification to the data protection authority (via the country-specific options).

501 Government data on data breaches reported to the French supervisory authority, CNIL. Source files available at https://www.data.gouv.fr/fr/datasets/notifications-a-la-cnil-de-violations-de-donnees-a-caractere-personnel/ (online, accessed 2 April 2023).

Due to the sample in France, a further differentiation of the effort with regard to a company's size and business model is not possible.

Table 44: Extrapolation of efforts to report data privacy breaches in France

Year	Reported data breaches in France	Costs per breach in EUR	Total costs in EUR
2022	4,088		1,050,616
2021	5,037	257	1,294,509
2020	2,821		724,997

b) Qualitative burdens

In addition to the quantitative estimation of GDPR-related burdens described in the previous section, the qualitative statements of the respondents can be used to further specify the process of implementing the GDPR and the associated perceived burdens.

In France, familiarisation with the requirements of the GDPR was carried out in the companies surveyed as part of a project with a duration ranging from several weeks to 8 months. The associated effort was predominantly rated as high even for the companies which already had an RPA because of the required revisions. All previous processing activities had to be reviewed regarding the new requirements. Especially smaller companies often lacked the appropriate resources, both financial and human. Therefore, these companies often involved external consulting services to create/revise and implement the RPA.

Translating the new legal basis into practice was often carried out by companies with external consulting services, and not only by the smaller ones. Even the companies which had already dealt with the implementation of the previous Data Processing and Civil Liberties Act and prepared the RPA often used external consulting services to comply with the new requirements imposed by the GDPR.

Much like in Germany, creating or revising an existing RPA also represented a high level of effort for companies. However, all companies interviewed for France stated that creating or revising an RPA brought significant benefits as it provided the business owners or the managers with a wide overview of what has been done or needs to be done as regards personal data processing. Several interviewees also stated that the RPA was then used as an internal tool for decision-making, either by managers or by the company's executive. Furthermore, all interviewees (including experts) reported that implementing the RPA, and GDPR requirements

in general, within companies allows raising awareness and interest in personal data protection in businesses.

The creation of the directories was usually managed within a project structure, coordinated by an appointed data protection officer (or by company owners in smaller businesses). The DPO was then in charge of coordinating the information collection with each different department of the company and of creating or revising the directory. In France, official templates provided by the CNIL were widely used for the creation of the RPA, especially by smaller companies which do not have the internal human and financial resources to create templates themselves, or to use templates provided by an external consultancy.

Moreover, the RPA must be updated if changes to the records occur. Thus, new processing activities are continuously being added. As reported during the interviews, the directories are updated on a regular basis, usually once per year, through interviews involving the DPO and the managers of the different relevant departments of the companies. Art. 30 therefore imposes a permanent task; the effort for updating and maintaining the directory depends on the company's development, size, sector of activity and business model (e.g. higher efforts for B2C business models). Overall, according to the surveyed companies in France, the recurring tasks for the maintenance of the RPA were reported as the main burden in complying with Art. 30 GDPR. Three main reasons have been reported by interviewees to explain the high effort of maintaining the RPA. First, since the maintenance of the RPA requires knowledge of which data processing must be added into the record, or revised, interviews involved DPO and members from the different departments concerned with data processing. However, it seems quite difficult for DPOs and members from departments to find common time slots. Second, the DPOs interviewed reported that it was extremely difficult to motivate colleagues to conduct activities related to the maintenance of the RPA. Although members of companies in France are quite aware of the importance of personal data protection, they do not seem particularly involved in and concerned by the GDPR requirements and required tasks. Finally, the interviews necessary for the maintenance of the RPA were reported as highly time-consuming, taking between 2 and 4 hours. This is the main reason members of company are reluctant to cooperate with DPOs for interviews related to directory maintenance.

Unlike in Germany, interviewed companies in France have not established an internal standardised notification process for data breaches under Art. 33. Data protection breaches are usually directly reported to the data protection officer who then reports the incident to the supervisory authority if necessary, using the online notification platform. In most cases, companies interviewed for France stated that they only made a preliminary notification first to comply with the 72 hours set by Art. 33 (1). Then, in the following days, they usually complete the preliminary notification as they have sufficient time to collect enough information regarding the incident

and to conduct a risk assessment on the data breach. The effort for reporting a data breach to the supervisory authority highly varies depending on the type of case and internal resources of the company, but reporting to the authority is always barely time-consuming.

6. Proposals for reducing bureaucratic costs

Interviewees provided suggestions on how data protection procedures and the GDPR could be improved for businesses. It should be noted that all companies interviewed for France accepted to participate in this study provided proposals for reducing GDPR-related bureaucratic costs.

It can be stated that besides potential for improvement, companies also emphasised positive aspects of the GDPR. Creating or revising the RPA in particular was reported as providing businesses owners and managers with a wide overview of what has been done or needs to be done as regards personal data processing. Some respondents also stated that the RPA is used in their companies as an internal tool for decision-making, either by managers or by the company's executive. Moreover, all interviewees (including experts) reported that implementing GDPR requirements in companies significantly contributes to raising awareness and interest in personal data protection among employees.

Nonetheless, some points of criticism and potential for improvement were raised regarding the GDPR in general and Art. 30 and 33 specifically. Some companies requested better support from the supervisory authority as regards the GDPR implementation in general, for instance through the diffusion of recommendations and best practices. Moreover, all respondents among businesses stated that they had never received any feedback from the supervisory authority after making a notification. However, according to them, receiving such feedback is essential for improving future notifications and better protecting personal data. According to the experts interviewed, this contributes to the lack of interest of French enterprises in the GDPR as the companies are never worried by the supervisory authority, never heard of it, and the sanctions seem abstract and irrelevant for them.

Some respondents also suggested the supervisory authority to be more decentralised and present. Indeed, the French supervisory authority only has one office, located in Paris. According to the experts and some of the companies interviewed, the geographic distance from the authority of companies located elsewhere in France highly correlates with the lack of interest of businesses in the GDPR.

Another criticism brought forward several times is that the GDPR could be better adapted to SMEs and mid-caps. Several companies stated that the regulation, in its current form, imposed too heavy an administrative burden on SMEs and mid-caps and that its requirements are far too

high compared to the internal financial and human resources of those businesses. Therefore, it was suggested to better differentiate GDPR requirements according to company's size, making them less sophisticated for smaller businesses and better tailored to companies' resources.

Furthermore, an expert especially highlighted the specific case of companies located in French overseas territories. According to her, an important communication effort is required from the French supervisory authority for companies located in these territories as a significant part of them are wholly unaware of the GDPR. In addition, this expert suggested simplifying the GDPR, especially as regards Art. 30 requirements, as a majority of SMEs and mid-caps located in overseas territories still do not have a digitalised database for personal data.

Likewise, some experts suggested differentiating GDPR requirements, not with regard to the company's size or geographical location, but to their sector of activity. Indeed, overlaps and contradictions were reported between GDPR and other French regulations requirements, especially for the health and defence sectors. Should the differentiation of requirements be unfeasible, providing guidelines or legislative clarifications on which provisions to apply for specific instances of data breaches was an alternative suggestion.

Contradictions with requirements of other regulations as well as too heavy administrative needs on SMEs burden French companies

V. Germany

1. Transposition in national law

Prior to the General Data Protection Regulation (GDPR), the Federal Data Protection Act ("Bundesdatenschutzgesetz", BDSG) was already applicable for the processing of personal data by public and private entities. On 5 July 2017, the new Federal Data Protection Act (BDSG-neu) was published and came into force at the same time as the GDPR on 25 May 2018. The BDSG-neu supplements the provisions of the GDPR and specifies various requirements from the GDPR for Germany, especially opening and specification clauses in the GDPR. In addition, there are the jurisdictions of the federal states (e.g. "Landesdatenschutzgesetz Baden-Württemberg", LDSG-BW).

The record of processing activities (RPA) according to Art. 30 was introduced as part of the GDPR and replaced the directory of procedures ("Verfahrensverzeichnis") that previously existed under the BDSG. Art. 33 concerns the notification of personal data breaches to the supervisory authority and superseded the duty to inform in case of illegal acquisition of data ("Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten") according to the former BDSG § 42a. Since both Art. 30 and 33 do not contain any opening clauses, there is no deviating national interpretation in Germany.

In Germany, the responsibility for monitoring and enforcing compliance with the GDPR is delegated to the data protection authorities of the individual federal states. There are 16 data protection authorities, each of which is responsible for overseeing companies and organisations in their respective state and additionally the Federal Commissioner for Data Protection and Freedom of Information (BfDI) as a supervisory authority at federal level.

2. Creation of records of processing activities

To comply with the requirements of Art. 30, companies must familiarise themselves with the requirements, (initially) create the RPA and regularly maintain it with regard to changes in responsibilities or processing activities that have been added (see Table 31). No deviations from that process were reported in Germany.

As there is no official definition of the notion of a "processing activity" and the required level of detail in the RPA, companies used and are still using templates to create or revise their RPA. In Germany, these are made available via the data protection authorities in the federal states. Due to the decentralised organisation of data protection in Germany, the templates are also heterogeneous. Some companies reported that they had used the templates of the authorities from Baden-Württemberg or Bavaria in particular. A systematic pattern could not be identified.

Compared to Austria, the official templates in Germany in general provide more details as to what information to include in the RPA, e.g. contact details of the controller, necessary details for the processing activity and additional information that is not explicitly required by the GDPR. The templates are comparable to their counterparts in France and Italy (see Part A – Chapter III).

3. Notification of a personal data breach to the supervisory authority

Art. 33 GDPR is implemented as an online notification to the local data protection authority. In Germany, an online form is predominantly used, but notifications by phone and e-mail are also possible (see Part A – Chapter IV). No deviations from the standard process (see Table 31) were reported in Germany.

4. State of research on bureaucratic burdens arising from the GDPR in Germany

The state of research in Germany provides limited insights into the bureaucratic burdens imposed by the GDPR. There are only a few studies addressing bureaucratic burdens of the GDPR for companies[502]. The results of these surveys indicate that the implementation of the GDPR is associated with a high level of effort. In two different studies, for example, almost

502 E.g. Bitkom e.V. (2021); Engels, B., Scheufen, M. (2020); Schricker, J. (2018).

two-thirds of the companies surveyed stated that implementing the requirements of the GDPR would involve a significant amount of time and effort[503]. In another survey of around 500 companies, 42 per cent of the respondents criticised that the effort incurred was high[504]. For example, identifying, analysing and, if necessary, changing the processes in the company that involve personal data is time-consuming[505]. A lack of personnel resources and ongoing legal adjustments to the GDPR also make the implementation more difficult[506]. The studies moreover show differences regarding the type and size of the company. On the one hand, larger companies face higher effort because they have more corporate processes than smaller companies. On the other hand, larger companies have more financial and human resources to implement the GDPR. In addition, the number of data processes often increases with the degree of digitalisation of a company, and with it the data protection requirements[507].

The studies show that the bureaucratic burden arising from the GDPR is a relevant issue for companies in Germany. However, the studies provide little detail or do not quantify the costs associated with the effort of complying with the GDPR. Therefore, this study includes 15 interviews with both companies and experts in the field of data protection in Germany to provide indepth insights into the implementation and the resulting bureaucratic burdens in relation to Art. 30 and 33.

5. Perceived burdens and compliance costs

a) Measurable burdens

To determine the effort involved, the responsibility for compliance with data protection requirements was first surveyed in the interviews. In the companies surveyed, the role of the data protection officer was held by executives in the legal or compliance department. In general, external service providers can also be appointed as data protection officers, but this was not the case for the companies interviewed in Germany. In addition to the data protection officer (DPO), in multinational corporations, so-called data protection coordinators (DPCs) support the data protection officers on local premisses. As activities related to Art. 30 and 33 GDPR were conducted by managers in the companies interviewed, for Germany, an hourly labour cost of 60.22 euros is applied to calculate the financial burden of conducting the standard activities.

503 Engels, B., Scheufen, M. (2020), p. 13; Schricker, J. (2018), p. 36.

504 Bitkom e.V. (2021), p. 1.

505 Engels, B., Scheufen, M. (2020), p. 5.

506 Bitkom e.V. (2021), p. 2.

507 Engels, B., Scheufen, M. (2020), pp. 14, 15.

Effort for Art. 30

The companies interviewed stated that the main effort of complying with Art. 30 GDPR was incurred at the time of implementation. The majority reported that a project structure was created either in the year before or with the introduction of the GDPR to coordinate the implementation of the GDPR in general. The familiarisation and initial creation of the RPA was then also managed within this structure with the DPO responsible for the process. In some cases, RPAs already existed to comply with the former BDSG; those were then updated or subjected to a complete revision. Therefore, the efforts of creation and revision are not further distinguished. Since the creation of the RPA requires knowledge of all business processes, department representatives were also involved in the process, represented by their department managers. The interviews and the assessment therefore always referred to the overall burden on the company. As the familiarisation with the GDPR and the creation of the RPA are the responsibilities of managers, they particularly affect the financial evaluation of the effort as they are paid higher salaries than clerical or skilled workers.

The average time required for familiarisation with the requirements was estimated to be 142.5 hours. These estimates refer to the total time needed to become familiar with the GDPR; only few companies could estimate the effort required for Art. 30 separately. It should be noted that the interviewed companies in Germany already had legal and compliance knowledge; therefore, the effort needed for the familiarisation with the new requirements related to the GDPR is probably lower than for companies that do not have these competencies.

After the initial familiarisation phase, companies reported that trainings were conducted to create awareness of the implications of GDPR among the employees. An exact estimate was not possible for the companies. Therefore, the expenses are not included in the table below.

Table 45: Effort for familiarisation in Germany

Standard activity	Average time spent in hours	Average costs consulting in EUR	Personnel costs in EUR	Total costs in EUR
Familiarisation	142	89,108	8,579	97,687

To create the RPA, companies stated that they used templates, which were either provided by an external consultant or prepared by the company itself. No company reported using the official templates of the authorities.

Based on the size and structure of the companies interviewed, the average costs for consulting services in the familiarisation phase is significantly higher than in Austria, France or Italy. Interviewees reported that these costs are still considered comparatively low. Due to the company's own competences and/or the selection of service providers, interviewees mentioned that it was even possible to save costs, as it was planned with mid-six-figure budgets.

The average time required for the creation of the RPA within the companies interviewed in Germany was estimated to be 2,047 hours. A special characteristic for the sample in Germany is the high number of processing activities, due to the size of the companies interviewed. With an average of 379 activities, the average record is significantly larger than in Austria, France or Italy. This results in an average of 5 hours and 325 euros of personnel costs for the creation of one RPA entry. Based on the average number of processing activities, this results in total costs of 123,296 euros for the initial creation.

Companies in Germany stated that the entire RPA is reviewed once per year and updated if necessary. The following expenses are therefore reported as annual costs. As a result of digitalisation, companies reported that they are increasingly having to create new processing activities but could not quantify the amount or the effort required in the interviews. The following estimates therefore refer only to maintenance; the creation of new processing activities follows the logic described above.

The average time required for the maintenance of the RPA was estimated to be 425 hours. Based on the average of 379 processing activities, this results in roughly 1 hour and 68 euros of personnel costs for the maintenance of one processing activity. Based on the average size of the RPA in Germany, this results in total costs of 25,582 euros per year.

Table 46 summarises the standard activities to comply with Art. 30 GDPR.

Table 46: Effort for Art. 30 GDPR in Germany

Standard activity Art. 30 GDPR	Average time spent in hours	Average number of processing activities	Average time spent per processing activity in hours	Personnel costs per processing activity in EUR	Total costs in EUR
Creation or revision	2,047	379	5	325	123,296
Maintenance	425	379	1	68	25,582

Personnel costs were determined using the average time per standard activity multiplied by the hourly labour costs. The total cost is calculated by multiplying the average cost per case (processing activity) by the average number of processing activities.

In addition to internal efforts, the companies interviewed also use consulting services regarding the GDPR in general, for example, to obtain advice on legal changes or contract updates. In this regard, companies reported an average of 76,031 euros of annual costs for consulting services. The companies interviewed were not able to differentiate the services with reference to Art. 30.

Extrapolation

A representative study by Bitkom e.V. states that at least 62 per cent of companies in Germany have implemented the GDPR in full or to a great extent. Another 33 per cent have partially implemented it. Only 2 per cent stated that they had just started the implementation process, and none reported having not yet begun[508]. For the extrapolation of the data for Germany, it can therefore be assumed that only the maintenance effort has to be considered. In the case of new processing activities, approximately 5 hours would be added in the individual case according to the above-mentioned data. In 2021, there were a total of 3.4 million legal entities in Germany, 0.49 per cent of them with more than 250 employees, for which the above data can be applied[509]. However, over half of the revenues (52 per cent) were generated by those companies (with more than 250 employees)[510].

Table 47: Extrapolation of efforts for maintaining an RPA in Germany

Year	Number of legal entities in Germany in million	Share of entities matching sample in %	Number of comparable entities	Annual costs in EUR
2021	3.4	0.49	16,660	421,597,960

Further research should focus on micro- and small enterprises, which account for the majority (87 per cent) of all legal entities in Germany. Medium-sized companies should also be considered in further research to further specify and distinguish the burden arising from the GDPR in Germany.

508 Bitkom e.V. (2022).

509 Statistisches Bundesamt (Destatis) (2023).

510 Statistisches Bundesamt (Destatis) (2023).

Effort for Art. 33

In the companies interviewed, the responsibility for reporting a data breach is assigned to the data protection officer.

Given the individuality of data breach cases, it is difficult to determine an estimate required to meet the requirements of Art. 33 in general. To obtain an estimate at all, companies were asked for the effort of "a typical" case. Those cases are generally less complex and thus to be considered standard cases.

The average time for the entire process (see Table 31) required to report a data breach was estimated to be 15 hours. On average, companies reported 3 data breaches per year, which results in an average of 5 hours and 309 euros per data breach case. Multiplied by the average number of reported cases, this results in total costs of 880 euros. For more serious or wide-ranging data breaches, companies reported that the effort required is multiple times higher. The effort of obtaining and evaluating the relevant facts and details was described as very time- and resource-consuming. The notification itself was reported to require little effort and was estimated to take half to one hour to complete. It was confirmed that the reason for the relatively low effort is the implementation as an online form by the relevant authorities of the federal states.

Table 48: Effort for Art. 33 in Germany

Art. 33 GDPR	Average time spent in hours	Average number of reported data breaches	Average time per reported data breach in hours	Personnel costs per data breach in EUR	Total costs in EUR
Notification of data protection breach[511]	15	3	5	309	880

Extrapolation

Considering the reported data privacy violations in Germany[512] over the last three years, Table 49 shows the extrapolated data for Germany:

511 This includes the internal process of the notification of data protection breach, the gathering of information regarding the incident, the internal risk assessment and decision of whether a notification to the supervisory authority is necessary and the report to the data protection authority (via the country-specific options).

512 https://www.dsgvo-portal.de/.

Table 49: Extrapolation of efforts to report data privacy breaches in Germany

Table 49: Extrapolation of efforts to report data privacy breaches in Germany

Year	Number of reported data breaches in Germany	Costs per breach in EUR	Total costs in EUR
2022	8,802	309	2,719,818
2021	13,890		4,292,010
2020	26,057		8,051,613

Further research could analyse the underlying effects of the decreasing number of cases in Germany. The interviewed companies reported that the report to the authority also included proof of elimination, which leads to an overall increase in security and thus fewer reported data security cases.

Due to the sample in Germany, further differentiation of the effort with regard to a company's size and business model is impossible.

b) Qualitative burdens

In addition to the estimated quantitative burdens of the GDPR described in the previous section, the qualitative statements of the respondents can be used to further specify the process of implementing the GDPR and the associated perceived burdens.

Familiarisation with the requirements of the GDPR was conducted within a project structure with a duration of several months to 2 years. The associated effort was predominantly rated as high. All business processes had to be reviewed regarding the new requirements. Smaller companies often did not have the resources. To translate the new legal requirements into practice, the companies used external consulting services. In contrast, companies that had already handled the implementation of the BDSG and therefore possessed the corresponding knowledge rated the introduction phase of the GDPR as less time-consuming.

The implementation of the RPA also represented a high level of effort for companies during the implementation phase of the GDPR due to the involvement of several stakeholders in its creation. The interviews also showed that companies that were not aware of their business processes and data considered the implementation of the RPA to be more time-consuming. In contrast, companies that had already recorded their business processes in a management system or in a directory of procedures under the BDSG ("Verfahrensverzeichnis") were able

to use this as preliminary work to prepare the RPA, although they also carried out a complete revision of existing RPAs. The creation of the directory was usually coordinated centrally by the DPO located in the compliance department. The respective processing activities were identified and documented together with each department. Official templates from the authorities were not used. If external templates were used, they were provided by external consultancies.

Moreover, the RPA must be updated if changes occur. New processing activities (e.g. cloud applications) are continuously being added, particularly due to increasing digitalisation. Usually, the directory is reviewed once per year, initiated by the DPO, and conducted by the departments. Art. 30 is therefore a permanent task, the effort of updating and maintaining the directory depends on the company's development and business model (e.g. high effort for changing B2C business models). Companies with a pre-existing systematic process management system often also created internal processes for updating the RPA in case of new processing activities. Overall, according to the companies surveyed, the continuous effort regarding the RPA is rather low, especially compared to the initial creation.

The majority of the companies surveyed have established an internal standardised notification process for data breaches under Art. 33. Data protection breaches are usually first reported to the DPO, who then reports the case to the authorities if necessary. At this point, it should be noted that the data breach process reported during the interviews does not strictly align with the legal requirements. The companies interviewed did not make use of the possibility of a preliminary notification, but rather submitted their final report in the first place. Typical data breaches mentioned by the companies interviewed were mostly related to incorrect dispatch of personal information and cybercrime. Lost devices, on the other hand, played a less important role due to increasing technical protection and encryption.

Within our sample, only a small number of cases have been reported to the authorities. In addition, the internal processes (information gathering as well as the clarification, evaluation and resolution of the case) are particularly described as a burden. The effort varies widely depending on the type of case, but reporting to the agency was described as hardly time-consuming at all. Finally, two other relevant aspects regarding Art. 33 were mentioned by the companies. First, raising employee's awareness of data breaches, for example, in the form of training courses, constitutes a costly but relevant issue. Second, the notification of the persons affected by a personal data breach in accordance with Art. 34, which is associated with the notification of data breaches to the authorities, was stated to be very time-consuming.

6. Proposals for reducing bureaucratic costs

Respondents' feedback on optimising data protection procedures and regulations for businesses is as follows. First, it can be stated that besides potential for improvement, companies also

Assessment: wide range from "GDPR as competitive advantage" to demand for more support by authorities

emphasised positive aspects of the GDPR. For example, some respondents value the GDPR as a beneficial law and cited benefits beyond the mere compliance with the law, e.g. data protection compliance as a competitive advantage. Nevertheless, some points of criticism and potentials for improvement were raised regarding the GDPR in general as well as Art. 30 and 33:

- several of the companies surveyed requested better support from the authorities in implementing the GDPR and particularly Art. 30, for example, in the form of templates, recommendations and best practices. In addition, improved communication by the authorities was suggested. For instance, feedback from the authorities was often missing and the inability to ask questions was criticised.
- On a general level, another point of criticism concerns the different interpretations of the GDPR at both national and European level. The deviations of individual requirements (e.g. fines, opening clauses) lead to legal uncertainty and make it more difficult for companies to implement the requirements of the GDPR, especially for companies operating in different countries across Europe.
- Furthermore, companies criticised the strict treatment of software from American companies such as Microsoft, as their software is indispensable for the work of companies. Interviewees suggested that instead of the companies, the software providers should be held accountable for ensuring data protection.
- There was also support for adapting the GDPR to different business models, as companies with a B2B business model often work less with personal data than B2C companies.
- Documentation was mentioned as a time-consuming topic in general. However, the effort could be reduced by providing appropriate tools.

Regarding Art. 30, respondents suggested clearer guidelines and terminology. In particular, information on the scope of the RPA could be improved to clarify the required level of detail. It was also criticised that the directory has little to no benefit to the business other than compliance with Art. 30. Accordingly, the RPA is rarely used by companies for other data protection issues or business processes.

Concerning Art. 33, several companies expressed uncertainty as to how to correctly apply the 72-hour threshold. The interviews showed that many respondents interpret the notification process as a fixed deadline. Thus, Art. 33 (4) – the option to submit information to the authority incrementally – was not used by the interviewed companies in Germany. The correct interpretation of the data breach notification rule should therefore be accurately defined and communicated. Furthermore, the lack of feedback from the authorities on data protection notifications was repeatedly reported by the interviewees. This led to uncertainty among the

companies that reported a data protection breach. In particular, the question of whether a case should be considered closed was identified as useful feedback or information.

Moreover, it was pointed out several times that other aspects of the GDPR besides Art. 30 and 33 are also perceived as time-consuming and bureaucratic burdens (e.g. data subject rights, deletion periods, information obligations).

VI. Italy

1. Transposition in national law

In Italy, the first regulation addressing the issue of personal data protection was the so-called Privacy Law (Law No 675 of 31 December 1996[513]), which established the Italian data protection authority (DPA), called *"Garante per la protezione dei dati personali"* or *"Garante della Privacy" (hereinafter "Garante")*. The first Personal Data Protection Code was introduced by Legislative Decree No 196 of 30 June 2003[514], which subsequently regulated the role of the Italian DPA.

In 2018, the existing national legislation was harmonised with the new European legislation, the General Data Protection Regulation (GDPR 679/16), by Legislative Decree No 101 of 2018[515]. It added to Legislative Decree No 51 of 2018[516], by which the Italian legal system implemented Directive 2016/680 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection and prosecution of criminal offences, completing the transposition of the so-called EU Data Protection Package. Numerous regulatory interventions[517] have been made to address the COVID-19 epidemiological emergency that affected issues related to the protection of personal data, some of which remain in force even after the end of the state of emergency.

The notion of a record of processing activities (RPA) was first introduced in Italy by Art. 30 GDPR as well as the notification of personal data breaches to the supervisory authority by

513 Law No 675 of 31 December 1996 – Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/28335.

514 Legislative Decree No 196 of 30 June 2003, stating the "Codice in materia di protezione dei dati personali" (in S.O n. 123 alla G.U. 29 luglio 2003, n. 174), available at https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29.

515 Legislative Decree No 101 of 10 August 2018, available at https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg; https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9042718.

516 Legislative Decree No 51 of 18 May 2018, available at https://www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/sg.

517 Available in the section "Personal data protection and Covid" of the Camera dei deputati, Servizio Studi (30 September 2022), Protezione dei dati personali, p. 10, available at https://www.camera.it/temiap/documentazione/temi/pdf/1115552.pdf?_1679491785128.

Art. 33 GDPR. Since both Art. 30 and 33 do not contain any opening clauses, there is no deviating national interpretation in Italy.

In Italy, the responsibility for monitoring and enforcing compliance with the GDPR is delegated to the Garante as an independent administrative authority that is subject to the Italian parliament.

2. Creation of records of processing activities

To comply with the requirements of Art. 30, companies have to familiarise themselves with the requirements, (initially) create the RPA and regularly maintain it with regard to changes in responsibilities or processing activities that have been added (see Table 31) No deviations from that process were reported in Italy.

As there is no official definition of the notion of a "processing activity" and the required level of detail in the RPA, companies use templates to create their RPA. Compared to France or Germany, the template provided by the Italian authority is quite basic and, de facto, only used by micro- or small companies.

3. Notification of a personal data breach to the supervisory authority

Art. 33 GDPR is implemented as an online notification to the local data protection authority. In Italy, starting from 1 July 2021, the notification of a personal data breach must be submitted to the DPA through a specific electronic proceeding, made available on the authority's website[518], as stated in the Provision of 27 May 2021[519]. No deviations from the standard process (see Table 31) were reported in Italy.

4. State of research on bureaucratic burdens arising from the GDPR in Italy

The state of research in Italy provides limited insights into the bureaucratic burdens imposed by the GDPR. Most academic studies focus on the harmonisation of the Italian legislation to the European regulations[520]. The same topic is also covered by several public authorities and international organisation publications[521]. Other studies and reports focus on facilitating the compliance of companies, especially SMEs, with personal data protection laws[522]. A small number of surveys and studies assessing the level of compliance of Italian companies have

518 https://servizi.gpdp.it/databreach/s/.

519 Provision of 27 May 2021 – Procedura telematica per la notifica di violazioni di dati personali (data breach) https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9667201.

520 E.g. Panetta, R. (2017); Cassano, G. et al. (2018); Angelini, M. et al. (2020).

521 Blogdroiteuropeen (2019); Garante (2018); IAPP (2018); Camera dei deputati (2022).

522 Garante (2007, 2013); Confartigianato (2021).

been conducted over the years[523]. The results of these surveys indicate that Italian companies began familiarising themselves with GDPR requirements as early as in 2016. However, from a survey of around 160 companies, it emerges that their awareness of the topic was mainly driven by the fear of sanctions rather than by a clear perception of the risks in case of data breach[524]. Another study, conducted one year after the implementation of the GDPR in Italy, shows that more than half of the over 100 companies surveyed are compliant with the GDPR requirements[525]. The same study also reported that 45 per cent of the companies interviewed had increased their GDPR budget, 85 per cent had created an RPA and 68 per cent had developed a data breach notification procedure. Another report highlighted that Italian companies were the most sanctioned in Europe in 2021[526]. The increase in the number of sanctions was associated with a surge in the number of inspections conducted by the DPA, which doubled between 2020 and 2021. Out of 75 companies interviewed, 43 per cent had established a detailed internal system to handle inspections, while only 7 per cent had no procedure at all. The surge of inspections, on the other hand, did not correlate with a correspondent increase in data breach notifications. Between 2018 and 2021, the number of reported data breaches in Italy corresponded to 3,460 – a very low number compared to the 77,747 notifications reported in Germany. According to the study, this evidence does not indicate a higher data security among Italian companies but rather a reluctance to report the data breach despite this being mandatory by law. The fear of sanctions is identified as a possible cause. In fact, Italy ranks as the fourth country by the total sum of fines[527] (almost 123 million euros by March 2023) and the second by number (248 by March 2023) in Europe.

The studies show the level of compliance with the GDPR among companies in Italy. However, the studies provide little detail or do not quantify the costs associated with the effort to comply with the GDPR. Therefore, this study includes 15 interviews with both companies and experts in the field of data protection in Italy to provide further insights into the implementation and the resulting bureaucratic burdens in relation to Art. 30 and 33.

5. Perceived burdens and compliance costs

a) Measurable burdens

In the first step of the interviews, the responsibility for complying with data protection requirements was assessed to determine the burden. It was observed that in the companies surveyed, the role of the data protection officer (DPO) is often outsourced to external service

523 GCSEC and Europrivacy (2016); Osservatorio Cybercecurity & Data Protection (2020); DLA Piper and IPTT (2021).

524 GCSEC and Europrivacy (2016).

525 Osservatorio Cybersecurity & Data Protection (2020).

526 DLA Piper and IPTT (2021).

527 Data about fines are collected by the international law firm CMS and available in their open database GDPR Enforcement Tracker at https://www.enforcementtracker.com/?insights.

providers, frequently the same firm that provided the initial consultancy. While it is possible for executives from legal or compliance departments to be appointed as DPOs, this was not the case for the companies interviewed in Italy.

Typically, the team responsible for GDPR compliance consists of one or more internal resources and one or more consultants (at least during the initial implementation of the compliance procedures). The size and composition of the team varies significantly depending on the dimension and the activity of the company. Based on the interviews with Italian enterprises, the team size ranges from 2 employees and one consultant from a business association (providing support only during the initial implementation phase) for small and medium-sized enterprises (SMEs) to a team of 7 professionals, including 2 managers, 2 external consultants for DPO tasks and 3 external consultants for other legal and IT matters related to GDPR compliance.

Activities related to Art. 30 and 33 GDPR are typically conducted by managers and manager-level professionals in the companies interviewed. Therefore, an hourly labour cost of 59.57 euros is applied to calculate the financial burden of carrying out standard activities in Italy.

Effort for Art. 30

The companies interviewed have reported that the primary effort of complying with Art. 30 GDPR was incurred during the implementation phase. Most of them indicated that a project structure was established either when the GDPR was introduced in 2016 or when existing national legislation was aligned with the GDPR in 2018. The process of familiarisation and initial creation of the RPA was managed by the GDPR team, as previously described. Since the creation of the RPA requires knowledge of all business processes, all departments participated in the process, represented by their department managers. The interviews and assessments therefore considered the overall burden on the company. Consequently, the familiarisation and creation of the RPA became the responsibility of managers, which particularly affected the financial evaluation of the effort.

The average time estimated for familiarisation with the requirements of the GDPR was 431 hours, which corresponds to personnel costs of 25,658 euros. These estimates encompassed the total time needed to achieve familiarity with the GDPR, as only a small number of companies were able to estimate the effort required specifically for Art. 30.

Following the initial familiarisation phase, companies reported conducting trainings to raise awareness among employees about the implications of the GDPR. Training is mandatory by law, although it lacks standardisation in terms of hours allocated. Enterprises adopt varying

approaches to this practice, influenced by their size and perception of the significance of training. Consequently, the training programmes are tailor-made for each company. The training curriculum for a labourer, for instance, will differ from that designed for an administrative manager, encompassing distinct modules and timeframes. The training duration ranges from a minimum of 3–4 hours to as much as 12 hours per employee, contingent upon their position within the organisational hierarchy of the company. However, detailed estimates of expenses related to these trainings were impossible to obtain from the companies and therefore are not included in the figures.

Table 50: Effort for familiarisation in Italy

Standard activity	Average time spent in hours	Average costs consulting in EUR	Personnel costs in EUR	Total costs in EUR
Familiarisation	431	3,372	25,658	29,030

To create the RPA, companies often rely on templates provided by external consultants or created in-house. Average costs for consulting services amounted to 3,372 euros. While some countries, such as France, offer structured templates through their national authorities, the Italian authority provides a basic Excel template with columns but no rows. Consequently, the official template in Italy is predominantly utilised by small and micro-companies, whereas larger companies opt for tailor-made templates.

The average time required to create the RPA in the Italian companies surveyed was estimated to be 180 hours, with an average of 45 activities per RPA. This overall record size is notably smaller than that of Germany or France. However, this difference can be attributed to the size of the companies surveyed rather than a structural national disparity. Accordingly, the average personnel costs for creating one processing activity amount to 4 hours and 237 euros. Italian companies spend an average of 1,124 euros on consulting services to create the RPA. Based on the average number of processing activities and the costs for consultation in the creation phase, the total costs for creating the RPA in Italy amount to 11,868 euros.

Half of the Italian companies surveyed reported reviewing and updating their entire RPA once or twice per year, while the remaining companies exhibited a high heterogeneity in their review frequency, ranging from once per quarter to once per month to 3 times per week. This disparity can be explained by the varying significance of GDPR compliance to the core business of each company. For example, the company that reviews its record of processing activities 3

times per week is a software house that handles medical data and requires GDPR compliance for its business contracts.

The following expenses are reported as annual costs. As a result of digitalisation, companies reported that they are increasingly having to create new processing activities but could not quantify the amount or the effort required in the interviews. Therefore, the following estimates only pertain to maintenance costs, with an average of 49 hours estimated for RPA maintenance. Based on the average of 45 processing activities, this translates to 1 hour and 64 euros of personnel costs for maintaining one processing activity. Based on the average size of the RPA, the total annual maintenance costs for the RPA in Italy amount to 2,893 euros.

Table 51 summarises the standard activities to comply with Art. 30 GDPR.

Table 51: Effort for Art. 30 GDPR in Italy

Standard activity Art. 30 GDPR	Average time spent in hours	Average number of processing activities	Average time spent per processing activity in hours	Personnel costs per processing activity in EUR	Total costs in EUR
Creation or revision	180	45	4	237	11,868[528]
Maintenance	49	45	1	64	2,893

In addition to internal efforts, the companies interviewed also used consulting services for general GDPR compliance, such as obtaining advice on legal changes and contract updates. The companies reported an average annual cost of 16,682 euros for these consulting services. The expert interviewed noted that the annual fees varied significantly based on the size of the company, ranging from little to no cost for small companies to 50,000 euros for larger ones. Most of the interviewed companies were unable to differentiate the services specifically related to Art. 30 GDPR.

Extrapolation

According to a representative study conducted by Osservatorio Cyber Security & Data Protection, as of 2020, at least 85 per cent of the companies in Italy have implemented an RPA. Extrapolating this data to Italy, it can be inferred that only the maintenance effort needs to be

528 This includes an average of 1,124 euros which could be directly attributed to the creation of the RPA.

considered. In the case of new processing activities, approximately 4 hours would be added on an individual basis, as per the above-mentioned data. In the year 2020, Italy recorded a total of 4.4 million registered legal entities[529], with approximately 85 per cent of them adhering to the regulatory requirement of having an RPA. This translates to approximately 3.8 million compliant enterprises and to an estimated annual expenditure of 10.9 billion euros dedicated to the maintenance of RPAs.

However, it is important to note that there are differing opinions among experts regarding the level of compliance among Italian companies. According to interviews conducted with experts, the estimated rate of compliance ranges from 50 to 70 per cent on average. When specifically considering micro-enterprises, which constitute 95 per cent of all legal entities in Italy[530], the compliance rate drops significantly, namely to only 10 to 25 per cent.

If micro-enterprises are excluded from the calculations, the annual cost of maintaining an RPA would amount to 551 million euros. Therefore, further research in Italy should delve into the level of compliance, with a particular focus on micro- and small enterprises, which combined account for the vast majority (99 per cent) of all legal entities in Italy[531].

Table 52: Extrapolation of efforts for maintaining an RPA in Italy

Table 52: Extrapolation of efforts for maintaining an RPA in Italy[532]

Year	Number of legal entities in Italy	Share of RPA-compliant entities in %	Number of compliant entities	Annual costs in EUR
2020	215,692	85	183,338	551,113,501

Effort for Art. 33

In the companies interviewed, it was observed that companies typically seek the assistance of their consultants when a data breach occurs. Nevertheless, the responsibility for reporting a data breach is usually assigned to the data controller.

529 Imprese e addetti (Istat), 2023.

530 Imprese e addetti (Istat) (2023).

531 Imprese e addetti (Istat) (2023).

532 Excluding micro-enterprises.

Due to the unique nature of data breach cases, it was challenging for the interviewees to estimate the effort required to meet the requirements of Art. 33 GDPR in a general sense. To obtain an estimate, companies were asked to provide information on the effort required for a "typical" data breach case, which is generally less complex and thus considered a standard case.

The average time for the entire process (see Table 31) required to report a data breach was estimated to be 13 hours. On average, companies reported experiencing one data breach, resulting in an average of 10 hours and 617 euros of costs per data breach case. When multiplied by the average number of reported cases, this results in a total cost of 749 euros. Companies reported that for more serious or extensive data breaches, the effort required is multiple times higher. Obtaining and evaluating the relevant facts and details was described as time- and resource-consuming. The actual notification process was reported as requiring little effort, estimated to take between half to one hour to complete. Additionally, the procedures for notifying all affected users whose data was compromised, as well as the backup and controls of IT systems, were described as lengthy and resource-intensive activities, significantly increasing the time and cost of the overall procedure.

Table 53: Effort for Art. 33 in Italy

Art. 33 GDPR	Average time spent in hours	Average number of reported data breaches	Average time per reported data breach in hours	Personnel costs per data breach in EUR	Total costs in EUR
Notification of data protection breach[533]	13	1	10	617	749

Extrapolation

Considering the reported data privacy violations in Italy[534] over the last two years, Table 54 shows the extrapolated data for Italy.

Despite the increasing number of cases in Italy, the findings from the interviews align with the existing literature, revealing that the number of reported data breaches in Italy is much

533 This includes the internal process of the notification of a data protection breach, the gathering of information regarding the incident, the internal risk assessment and decision of whether a notification to the supervisory authority is necessary and the notification to the data protection authority (via the country-specific options).

534 DLA Piper (2022).

lower compared to the number of notifications reported in other countries, such as Germany and France. However, this does not necessarily indicate a higher level of data security among Italian companies, but rather a reluctance to comply with the legal requirement of data breach notifications. Interviews with experts and companies further corroborated this observation, revealing distinct variations in the approach to risk reporting across different countries, which can be attributed to historical and cultural factors. Italy has a well-established tradition of small and medium-sized family-owned businesses in which reputation holds paramount importance. Consequently, there is a prevalent perception that reporting data breaches could tarnish the company's image, leading to a hesitancy to disclose such incidents.

Table 54: Extrapolation of efforts to report data privacy breaches in Italy

Year	Number of reported data breaches in Italy	Costs per breach in EUR	Total costs in EUR
2021[535]	1,782	749	1,334,718
2020[536]	1,574		1,178,926

Due to the sample in Italy, a further differentiation of the effort with regard to a company's size and business model is impossible.

b) Qualitative burdens

In addition to the estimated quantitative burdens of the GDPR described in the previous section, the qualitative statements of the respondents can be used to further specify the process of implementing the GDPR and the associated perceived burdens.

Familiarisation with the requirements of the GDPR was conducted in the companies surveyed as part of a project with varying durations, ranging from a few days to a few years. This heterogeneity is dependent on multiple factors, such as the size of the companies, their organisational structure, level of internal organisation and cooperation among the involved managers and consultants. Consequently, the associated effort also varies but was predominantly rated as high. All business processes were subjected to review considering the GDPR requirements. Smaller companies often faced challenges due to limited resources. To implement the European legal framework, the companies surveyed frequently used external consulting services.

535 From 28 January 2021 to 27 January 2022 (DLA Piper, 2022).

536 From 28 January 2020 to 27 January 2021 (DLA Piper, 2022).

The implementation of the RPA posed significant challenges for companies during the implementation phase of the GDPR, as it required substantial effort involving multiple individuals. Based on the interviews conducted, it was found that the cost of creating an RPA accounted for 10 to 50 per cent of the overall implementation burden. One of the major challenges faced by the companies interviewed was the initial assessment, which involved mapping internal processes and data chains. This proved to be particularly challenging when companies had limited knowledge of their internal organisation. Additionally, difficulties arose when managers responsible for providing the required documentation were not prompt or efficient, lacked competence and were not transparent in identifying all the necessary data and processes. To create an RPA, most Italian companies outsourced the task to external consultants who worked in collaboration with internal resources or a team of company employees, especially in the case of large enterprises. The processing activities were acquired from each department individually. As mentioned above, official templates from authorities were generally not used. When templates were used, they were often provided by external consultancies. The choice of adopting either an Excel or a software format for the RPA was evenly distributed among the companies interviewed. SMEs generally preferred the Excel solution, as it is easier to update even without IT-trained personnel. Large companies, however, often opted for software solutions, as they allowed handling multiple activities and automatically generated documents and procedures after entering company data, minimising the risk of errors.

Moreover, the RPA must be updated if changes to the records occur. New processing activities (e.g. micro-marketing) are continuously being added, particularly due to increasing digitalisation. Typically, the record is reviewed periodically, initiated by the responsible DPO and conducted by the specialist departments in the case of large enterprises or by the administrative personnel overseeing GDPR compliance for SMEs. Art. 30 is an ongoing obligation, as the effort required to update and maintain the record depends on the company's growth and business model. Overall, based on the feedback from the companies surveyed, the continuous effort in maintaining the RPA is relatively low, particularly when compared to its initial creation. However, there are exceptions, such as companies whose core business revolves around GDPR compliance, e.g. software houses and security companies. For them, the maintenance costs are comparable to the initiation ones.

The majority of companies surveyed have implemented an internal standardised process for reporting data breaches in accordance with Art. 33. Typically, data protection breaches are initially escalated to the DPO or external consultants. The established procedures involve assessing the scope of the breach, estimating the potential impact of the damage and implementing risk-mitigation measures. Subsequently, the data controller, as stipulated in Art. 33, is responsible for notifying the supervisory authority within the prescribed timeframe.

Data breaches are reported to occur frequently, although not all of them must be reported to the data protection authority. The companies interviewed mentioned that common types of data breaches are often related to the inadvertent disclosure of personal information and cybercrime, while incidents involving lost devices are less frequent due to increased technical safeguards. Additionally, there is a general tendency to underestimate the severity of breaches. One issue that has been identified is that company owners are often unaware of the extent of the breach suffered by their organisation. Moreover, in Italy, companies tend to refrain from publicly disclosing data breaches unless mandated by legal requirements to report them to the relevant authority.

Overall, only a small number of data breaches have been reported to the authorities according to the companies surveyed. Furthermore, it is exclusively the processes that take place beside the actual reporting to the authorities – the clarification, assessment and resolution of the case – that constitute a burden. Although the risk assessment, which must be conducted within 72 hours to determine the data exposed and assess the need for notification under Art. 33, can be complex and time-consuming, reporting to the authority itself is often perceived as burdensome. The effort involved varies highly depending on the type of case, but reporting to the authority was always considered to be less time-consuming. In some cases, the indirect costs can be substantial as well. They involve the use of IT consultants and in some cases require the suspension of some company processes to carry out the required security checks.

6. Proposals for reducing bureaucratic costs

The feedback provided by respondents regarding the optimisation of data protection procedures and regulations for businesses can be summarised as follows. First, it is noteworthy that companies not only highlighted areas for improvement but also acknowledged the positive aspects of the GDPR. Compliance with the GDPR was recognised as offering numerous benefits to organisations, including enhanced data security, improved risk management, increased accountability, strengthened customer trust and a better understanding of their data landscape. Despite the initial effort and resources required, organisations often realise the long-term value of GDPR compliance.

However, several critical issues were also raised in relation to the GDPR in general and Art. 30 and 33 in particular:

- many companies surveyed expressed the need for better support from authorities in the implementation of the GDPR. They recommended establishing a more accessible and structured consultative process by the data protection authority to provide guidance and support to companies in complying with GDPR requirements.

- Companies also suggested a clearer regulation and interpretation of rules related to retention times, consent and other interpretative issues that companies frequently encounter. They recommended promoting consistency in interpretation across different national data protection authorities within the European Union.
- Interviewees also mentioned the need for simplification of the compliance process and alignment of GDPR requirements with the practical realities of companies' organisational structure and business activities, to facilitate compliance.

Call for economic incentives for SMEs to comply with the GDPR

- The experts interviewed highlighted the lack of economic incentives for small and medium-sized companies in Italy to adapt to GDPR compliance. The only incentive currently available is the threat of sanctions, which may not be sufficient to motivate businesses to comply. They recommended providing specific regional and national tenders or incentives to assist Italian companies in their GDPR adaptation efforts, which could encourage companies to invest in necessary changes and raise awareness about the importance of compliance.
- The sanctions for GDPR violations were noted to vary greatly depending on the nature and severity of the violation, ranging from low fines to significant penalties. The lack of certainty in the punishment for non-compliance and variations across countries were identified as factors that could impact companies' decision-making and competitiveness.
- One suggestion was to implement peer-to-peer incentives that could encourage compliance through requests from customers, suppliers and employees whose personal data are processed. Incorporating privacy as a part of the quality of products and services offered by companies, and making reporting procedures for privacy violations more accessible, could make it easier for individuals to report non-compliance.
- Improved communication by the data protection authority was recommended, with a responsibility to communicate the importance of GDPR compliance to the public, including individuals and businesses. Communication should be accessible and use understandable terms to raise awareness about privacy and data protection.

Respondents also assessed that while Art. 30 and 33 are the most burdensome activities, they are also the most regulated principles of the entire Regulation, with numerous guidelines and standards available. However, concerning Art. 30, respondents stated that there is a lack of information on the scope of the RPA. It was also criticised that the RPA provides no benefit beyond fulfilling the requirements of Art. 30. Moreover, it was noted that RPAs are often not properly filled in or updated after the implementation phase, which exposes companies to liability during controls, especially in cases of data breaches.

Regarding Art. 33, there is a general tendency to underestimate violations. One of the problems identified is that company owners are often unaware of the data breaches suffered by

their organisations. Additionally, in Italy, companies tend to underreport cases of data breaches due to concerns about potential damage to their brand reputation.

Finally, the companies surveyed mentioned a wide range of other points of criticism regarding the GDPR in general, which could not be elaborated further due to the scope of the study. It was also noted multiple times that aspects of the GDPR beyond Art. 30 and 33 also impose a burden on companies.

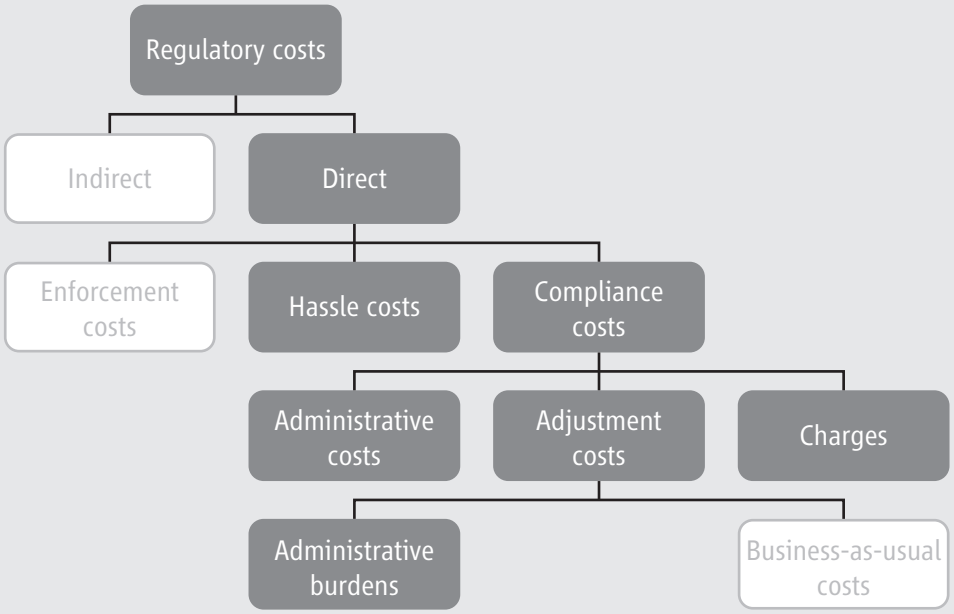
VII. Study approach

1. Methodology

The methodology is based on the concept of "compliance costs" used by the German Federal Government in its regulatory projects.[537] Compared to the EU Standard Cost Model (EU-SCM), this concept is a more comprehensive measure of bureaucracy. To align the concept of compliance costs with EU studies, the cost types are defined following the better regulation toolbox of the European Commission. The methodological approach of the EU-SCM only assesses the costs of the administrative burdens: costs arising from compliance with information obligations under legal regulation. For a comprehensive assessment of the regulatory burdens resulting from Art. 30 and 33 GDPR, the methodological approach must include hassle costs, charges and adjustment costs. Business-as-usual costs, i.e. costs resulting from information obligations that companies must comply with regardless of the existence of the regulation, are not considered in any of the methodological approaches.

537 Bundesregierung (2023), Leitfaden zur Ermittlung und Darstellung des Erfüllungsaufwands in Regelungsvorhaben der Bundesregierung.

Typology of costs[538]



Regulatory costs are a general term. They consist of **indirect costs** incurred in related markets that are not directly affected by regulation (e.g. changes in consumer prices in the regulated sector due to increased compliance costs and in the quantity of goods and services available). Direct costs, on the other hand, are specifically associated with regulation.

Direct costs include:

- **Hassle costs:** costs arising from unnecessary delays, redundancy or corruption during the regulatory process. Due to their broad definition and qualitative nature, they are not included in the methodological approach of the EU-SCM. In this study, they are captured qualitatively to identify additional burdens due to complications.
- **Enforcement costs:** costs associated with activities related to the implementation of a regulation borne by public authorities, such as monitoring, inspection and litigation. They are not included in the EU-SCM model or in this assessment.
- **Compliance costs:** costs borne to comply with the provision of regulation.

The focus of this study is on compliance costs. These consist of:

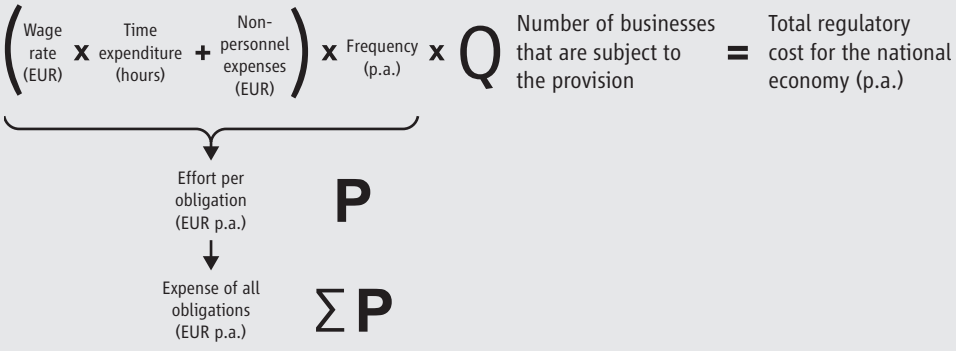
538 All definitions originate from the better regulation toolbox of the European Commission (2021), https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox_en.

- **Adjustment costs:** the additional costs of complying with a new regula-tion. They include the expenses and investments that companies must bear to adapt to a regulation's requirements.
- **Administrative costs:** these costs stem from the administrative activities necessary to comply with the information obligations of a regulation. They consist of administrative costs and business-as-usual costs.
- **Charges:** e.g. fees, levies and taxes related to the regulation.

a) Compliance costs

Compliance costs are captured at the company level. Rules and regulations force companies to meet certain targets or requirements, e.g. applying for certificates, training to achieve a particular qualification or providing and sharing information (labels, applications, documentation etc.). The companies' tasks to meet such requirements can be modelled in standard activities. To capture the compliance costs, the average time to perform all activities is usually multiplied by the average labour cost in euros. One-off compliance costs are multiplied by their annual frequency to obtain annual values. If material and procurement costs are directly incurred to fulfil a requirement, they are added either once or based on an average annual material cost (for continuous tasks). The results are values for an average company that can be extrapolated to the total economic costs of a Member State based on official statistics. In this study, only the compliance costs for the core activities for the compliance with Art. 30 and 33 GDPR are used for extrapolation to country level.

Figure 13: Calculation of regulatory costs



If a requirement exclusively applies to companies exceeding a certain size or if, for example, small and medium-sized companies fulfil the requirements manually while large companies utilise an automatic procedure, different case groups can be formed. For the calculation of

compliance costs, it is irrelevant whether the differentiation is based on a different design choice or a different underlying standard.

b) Labour costs

The total labour cost per hour is necessary to determine the financial basis required to carry out the steps to create and maintain an RPA as well as notifying the supervisory authority of a personal data breach. Information was collected on who is responsible for these processes (in terms of the type of job or positions in the companies). However, information on the salary of the employees could not be collected to a satisfying degree due to the sensitivity of such data.

To ensure that data on labour costs are coherent across the four countries studied, data from Eurostat was used instead. While national sources would have provided more detailed information (e.g. in terms of economic sector or professional qualification), a database at the European level ensures that the figures cover the same elements and that common definitions are used. This aspect is particularly important as labour costs are dependent on national labour law, tax rules and national contractual arrangements. The use of labour costs makes it possible to overcome the problem of the varying distribution of social contributions paid by employers and employees between countries.

Data on labour costs in the four countries were collected in the following manner:

- data on the gross hourly earnings of professionals by country were extracted from a Eurostat database. These data refer to companies in the industry, construction, and services sectors, having more than 10 employees. The latest available data refer to the year 2018.
- The interviews showed that, in general, managers and/or highly qualified employees are assigned to handle the GDPR requirements. This also includes the creation of an RPA or reporting a personal data breach to the supervisory authority. Companies that do not manage data protection issues within their own organisation generally use external data protection officers, who also charge a high hourly wage as consultants. Hence, "managers" was selected as classification for the mean hourly earnings. The general level of hourly costs is therefore higher than with other activities.
- Data on the share of non-wage labour costs over total labour costs were also extracted from Eurostat database; these data also relate to the year 2018 and companies in the industry, construction, and services sectors, having more than 10 employees.
- To calculate the total hourly labour costs of professionals, gross hourly earnings of managers were divided by the share of wage-related labour costs.

Table 55 illustrates the results by country.

Table 55: Calculation of hourly labour costs

Country	Gross hourly earnings of managers (2018) in EUR	Non-wage labour costs of total labour costs (2018) in %	Wage-related labour costs (2018) in %	Hourly labour cost of managers (2018) in EUR
Austria	36.58	26.7	73.30	49.90
France	31.51	32.9	67.10	46.96
Germany	46.73	22.4	77.60	60.22
Italy	42.59	28.5	71.50	59.57

This dataset, based on a common source with common definitions, provides clear advantages for comparative analysis. Nevertheless, some limitations must be acknowledged:

The weight of non-wage-related and wage-related labour costs can vary depending on the wage level. The use of a single generic share per country, such as the one extracted from Eurostat, may lead to an underestimation or overestimation of the final hourly labour cost.

Similarly, the disaggregation of labour costs can vary in each national context depending on the economic sector.

Despite these caveats, these data represent the most accurate available approximation of labour costs relevant to this study.

c) Transposition in national law

Additional burdens and costs may result from the transposition of EU law in national law, which may lead to additional regulatory and reporting obligations for companies due to the transposition of national law.

2. Data collection

The information collected is based on standardised interviews with company representatives and experts from Austria, France, Germany and Italy to obtain insights into perceived regulatory burdens.

The following is a brief description of the sample for each country:

- in Austria, a total of 12 interviews were conducted. The sample includes several experts who work as consultants and/or as external data protection officers (7). One interview was conducted with a representative of the Austrian Economic Chamber (Wirtschaftskammer Österreich). Furthermore, 5 representatives from small to large companies reported on their experiences with the implementation of the GDPR. Even though a considerable number of companies have been approached for additional interviews, the majority of them rejected the request. According to the expert interviews, this could be due to a low level of acceptance of the GDPR among small and micro-enterprises, which account for the vast majority of the business population in Austria[539].
- In France, a total of 19 interviews were carried out. The sample includes 2 experts from business associations, lawyers specialised in the GDPR and one expert from the French association of data protection officers. As for companies, a total of 15 interviews were carried out: 9 with large, 3 with medium, 2 with micro- and 1 with a small-sized enterprise. Most interviews with companies were conducted with data protection officers. Among all the enterprises interviewed, around a quarter (26.7 per cent) are family-owned.
- A total of 15 interviews were conducted in Germany. One company responded in writing serving as an additional case. In addition, two experts from different consulting firms were interviewed.
- A total of 21 interviews were carried out in Italy, with the majority (14) being company representatives. The sample also included 2 experts from business associations, 2 GDPR specialists and one representing crafts and micro- as well as small enterprises. Furthermore, 4 experts from various consulting and law firms were also interviewed.

Table 56: Overview of interviews conducted per country

	Austria	France	Germany	Italy
Representatives from companies	5	15	13	14
Consultants acting as external data protection officers	3	1	–	4
Chamber of commerce and business associations	1	2	–	3
Other experts	3	1	2	–
Total	12	19	15	21

539 Bundesministerium für Arbeit und Wirtschaft Österreich.

List of tables

List of figures

Bibliography

Administrative Court of Wiesbaden (2022), judgement of 17 January 2022, Court file No. 6 K 1164/21.WI, available at https://openjur.de/u/2391922.html (online, accessed 24 May 2023).

Angelini, M., Ciccotelli, C., Franchina, L., Marchetti-Spaccamela, A., Querzoni, L. (2020), Italian National Framework for Cybersecurity and Data Protection. In: Antunes, L., Naldi, M., Italiano, G. F., Rannenberg, K., Drogkaris, P. (eds.), Privacy Technologies and Policy. APF 2020. Lecture Notes in Computer Science (LNSC), volume 12121. Springer, Cham. https://doi.org/10.1007/978-3-030-55196-4_8.

Art. 29 Working Party (2014), WP 213, Opinion 03/2014 on Data Breach Notification of 25 March 2014, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf (online, accessed 25 May 2023).

Art. 29 Working Party (2017), Working Paper (WP) 243 rev. 1, Guidelines on Data Protection Officers ('DPOs'), available at https://ec.europa.eu/newsroom/article29/items/612048/en (online, accessed 25 May 2023).

Art. 29 Working Party (2017), WP 248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 endorsed by EDPB, available at https://ec.europa.eu/newsroom/article29/items/611236 (online, accessed 25 May 2023).

Art. 29 Working Party (2018), Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30 (5) GDPR, available at https://ec.europa.eu/newsroom/article29/items/624045 (online, accessed 25 May 2023).

Art. 29 Working Party (2018), WP 250 rev.1, Guidelines on Personal data breach notification under Regulation 2016/679, available at https://ec.europa.eu/newsroom/article29/items/612052 (online, accessed 25 May 2023).

Arthur D. Little (2018), Digitale Transformation von KMU in Österreich 2018. Erfassung des Digitalisierungsindex 2018, https://www.wko.at/branchen/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/kmu-digitalisierungsstudie-2018_1.pdf (online, accessed 6 April 2023).

Arthur D. Little (2019), Digitale Transformation von KMUs in Österreich 2018. Erfassung des Digitalisierungsindex 2019, https://www.wko.at/branchen/b/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/kmu-digitalisierungsstudie-2019.pdf (online, accessed 6 April 2023).

BfDI (not dated), Tasks and powers, https://www.bfdi.bund.de/EN/DerBfDI/UeberUns/DieBehoerde/diebehoerde_node.html (online, accessed 24 May 2023)

BfDI (2018), Infoblatt „Meldung von Datenschutzverstößen", available at https://www.bfdi.bund.de/DE/Service/Datenschutzverstoesse/Infoblatt_Datenschutzverstoesse.html (online, accessed 24 May 2023).

BfDI (2019), Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DSGVO available at https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKBeschluessePositionspapiere/98DSK_Erfahrungsbericht-DSGVO-Anwendung.html (online, accessed 24 May 2023).

Bitkom e.V. (2017), Das Verarbeitungsverzeichnis, Leitfaden, available at https://www.bitkom.org/Bitkom/Publikationen/Das-Verarbeitungsverzeichnis.html (online, accessed 24 May 2023).

Bitkom e.V. (2021), Datenschutz setzt Unternehmen unter Dauerdruck, https://www.bitkom.org/Presse/Presseinformation/Datenschutz-setzt-Unternehmen-unter-Dauerdruck (online, accessed 6 April 2023).

Bitkom e.V. (2022), Datenschutz in der deutschen Wirtschaft: DS-GVO & internationale Datentransfers, https://www.bitkom.org/sites/main/files/2022-09/Bitkom-Charts%20Datenschutz%2027%2009%202022_final.pdf (online, accessed 27 March 2023).

Bogendorfer, R. (2022), Commentation on Art. 30 GDPR, in Knyrim, R. (ed.), Der DatKomm.

Bundesministerium für Arbeit und Wirtschaft (2021), KMU im Fokus 2021, https://www.bmaw.gv.at/Services/Zahlen-Daten-Fakten/KMU-in-%C3%96sterreich.html (online, accessed 23 March 2023).

Bundesministerium für Arbeit und Wirtschaft (2023), KMU in Österreich, https://www.bmaw.gv.at/Services/Zahlen-Daten-Fakten/KMU-in-%C3%96sterreich.html#:~:text=Die%20Europ%C3%A4ische%20Kommission%20definiert%20ein,Bilanzsumme%20bis%2043%20Millionen%20Euro (accessed online 28 March 2023)

Camera dei deputati, Servizio Studi, XVIII legislatura (2022), Protezione dei dati personali, https://temi.camera.it/leg18/temi/la_protezione_dei_dati_personali.html (online, accessed 18 April 2023).

Cassano, G., Colarocco, V., Gallus, G.-B., Micozzi, F.-P. (a cura di) (2018), Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101, Giuffrè Francis Lefebvre Editore, Milano.

CJEU (2022), judgment of 28 April 2022, C-319/20 (Meta Platforms), ECLI:EU:C:2022:322, available at https://curia.europa.eu/juris/document/document.jsf;jsessionid=9144610AE75C4914ABA079E95EA5BF11?text=&docid=258485&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=227709 (online, accessed 24 May 2023).

CMS Legal (2023), GDPR Enforcement Tracker, https://www.enforcementtracker.com/ (online, accessed 18 April 2023).

CNIL (not dated), The CNIL's Missions, available at https://www.cnil.fr/en/cnils-missions (online, accessed 24 May 2023)

CNIL (not dated), Le register des activités de traitement, available at https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement (online, accessed 24 May 2023)

CNIL (not dated), Traitement de données personnelles, available at https://www.cnil.fr/fr/definition/traitement-de-donnees-personnelles (online, accessed 24 May 2023)

CNIL (2017), Règlement européen sur la protection des données personnelles – Guide du sous-traitant, available at https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf (online, accessed 24 May 2023).

CNIL (2018), Notifier une violation de données personnelles, available at https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles (online, accessed 24 May 2023).

CNIL (2020), Délibération SAN-2020-014, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042675720 (online, accessed 24 May 2023)

CNIL (2020), Délibération SAN-2020-015 available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042676787 (online, accessed 24 May 2023)

CNIL (2021) Délibération SAN-2021-014, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044043045 (online, accessed 24 May 2023).

CNIL (2023), Les violations de données personnelles, available at https://www.cnil.fr/fr/les-violations-de-donnees-personnelles (online, accessed 24 May 2023).

CNIL (2023), La CNIL publie une nouvelle version de son guide de la sécurité des données personnelles, available at https://www.cnil.fr/fr/la-cnil-publie-une-nouvelle-version-de-son-guide-de-la-securite-des-donnees-personnelles (online, accessed 25 May 2023).

CNIL / Bpifrance (2018), Guide pratique de sensibilization au RGPD pour les petites et moyennes entreprises, available at https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf (online, accessed 24 May 2023).

Confartigianato (2021), Linee guida per l'adeguamento al GDPR delle micro e piccole imprese che presentano un livello di rischio basso/medio.

Confindustria Salerno (2018), Privacy: modello di Registro delle attività di trattamento e Glossario, available at https://www.confindustria.sa.it/privacy-modello-di-registro-delle-attivita-di-trattamento-e-glossario/ (online, accessed 24 May 2023).

Council of State (France) (2022), decision no. 449694, 22 July 22 2022, available at https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-07-22/449694 (online, accessed 25 May 2023).

Decreto legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" (in S.O n. 123 alla G.U. 29 luglio 2003, n. 174), https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29 (online, accessed 18 April 2023).

Decreto legislativo 10 agosto 2018, n. 101, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9042718 (online, accessed 18 April 2023).

Decreto legislativo 18 maggio 2018, n. 51 https://www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/sg (online, accessed 18 April 2023).

Deloitte (2021), Datenschutz in Zeiten von COVID-19, https://www2.deloitte.com/content/dam/Deloitte/at/Documents/risk/cyber-risk/at-datenschutz-umfrage-2021.pdf (online, accessed 28 March 2023).

Deloitte (2022), Deloitte Umfrage zum Datenschutz 2022, https://www2.deloitte.com/content/dam/Deloitte/at/Documents/risk/at-datenschutz-umfrage-2022.pdf (online, accessed 28 March 2023).

DLA Piper and Italian Privacy Think Tank (IPTT) (2021), Italian Privacy Compliance Survey, https://www.dlapiper.com/it-it/insights/publications/2021/05/italian-privacy-compliance-survey (online, accessed 18 April 2023).

DSB (2018), Datenschutzbericht 2018, available at https://www.dsb.gv.at/dam/jcr:508ea4f5-436a-41d6-9cdf-c10ab739bf4d/datenschutzbericht_2018.pdf (online, accessed 25 May 2023).

DSB (2018), decision of 8 August 2018, DSB-D084.133/0002-DSB/2018, available at https://ris.bka.gv.at/Dokumente/Dsk/DSBT_20180808_DSB_D084_133_0002_DSB_2018_00/DSBT_20180808_DSB_D084_133_0002_DSB_2018_00.pdf (online, accessed 25 May 2023).

DSB (2018), Newsletter 4/2018, available at https://www.dsb.gv.at/dam/jcr:c4d92a7b-1c4b-47a2-bba8-2fad7704a7d1/Newsletter_DSB_4-18.pdf (online, accessed 25 May 2023).

DSB (2019), Datenschutzbericht 2019, available at https://www.dsb.gv.at/dam/jcr:c9c2daf9-9746-4088-bced-dc8e296076e0/Datenschutzbericht_2019.pdf (online, accessed 25 May 2023).

DSB (2019), Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO, available at https://www.dsb.gv.at/dam/jcr:81630a55-648b-4689-b849-ce0732f6a1af/Meldung%20von%20Verletzungen%20des%20Schutzes%20personenbezogener%20Daten%20gem%C3%A4%C3%9F%20Art.%2033%20DSGVO%20Notification%20of%20a%20personal%20data%20breach%20(Art.%2033%20GDPR)%20.pdf (online, accessed 24 May 2023).

DSB (2020), Datenschutzbericht 2020, available at https://www.dsb.gv.at/dam/jcr:ad90690f-1d10-4e8f-8ed6-b489e888c30f/Datenschutzbericht%202020.pdf (online, accessed 25 May 2023).

DSB (2021), Datenschutzbericht 2021, available at https://www.dsb.gv.at/dam/jcr:1360e98b-d22a-4a49-b3bd-6afca2f86d4c/Datenschutzbericht_2021.pdf (online, accessed 24 May 2023).

DSB (2022), Leitfaden zur Verordnung (EU) 2016/679, available at https://www.dsb.gv.at/dam/jcr:5fc3b77f-d546-4609-aca0-e34035979549/DSGVO_Leitfaden_2022.pdf (online, accessed 25 May 2023).

DSB (2023), Datenschutzbericht 2022, https://www.dsb.gv.at/dam/jcr:ee7b155a-0a1f-4d00-98e9-902314c7022d/Datenschutzbericht%202022.pdf (online, accessed 17 April 2023).

DSGVO-Portal (2021), Rückblick DSGVO-Bußgeldverfahren und Datenpannen 2020, https://www.dsgvo-portal.de/news/rueckblick_dsgvo_bussgelder_datenpannen_2020.php (online, accessed 27 March 2023).

DSGVO-Portal (2022), Rückblick DSGVO-Bußgeldverfahren und Datenpannen 2021 https://www.dsgvo-portal.de/news/rueckblick_dsgvo-bussgeldverfahren_und_datenpannen_2021.php (online, accessed 27 March 2023).

DSGVO-Portal (2023), Rückblick DSGVO-Bußgeldverfahren und Datenpannen 2022 https://www.dsgvo-portal.de/news/rueckblick_dsgvo-bussgeldverfahren_und_datenpannen_2022.php (online, accessed 27 March 2023).

DSK (not dated), Sample template for an RPA for controllers https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_verantwortliche.pdf (online, accessed 25 May 2023).

DSK (not dated), sample template for an RPA for processors, https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_auftragsverarbeiter.pdf (online, accessed 25 May 2023).

DSK (2018), Kurzpapier Nr. 18 – Risiko für die Rechte und Freiheiten natürlicher Personen, available at https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf (online, accessed 25 May 2023).

DSK (2018), Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO, available at https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf (online, accessed 25 May 2023).

DSK (2018), Kurzpapier Nr. 1 – Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DSGVO, available at https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf (online, accessed 25 May 2023).

EDPB (not dated), Endorsed WP29 Guidelines, available at https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en (online, accessed 25 May 2023).

EDPB (2018), Guidelines 02/2018 of 25 May 2018 on the derogations of Art. 49 under Regulation 2016/679, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf (online, accessed 25 May 2023).

EDPB (2021), Guidelines 07/2020 on the concepts of controller and processor in the GDPR, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en (online, accessed 25 May 2023).

EDPB (2022), Guidelines 01/2021 on Examples regarding Data Breach Notification of 14 December 2021, Version 2.0, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en and https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_en (online, accessed 25 May 2023).

EDPB (2022), Guidelines 09/2022 of 10 October 2022 on personal data breach notification under GDPR, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-92022-personal-data-breach_en (online, accessed 25 May 2023).

Engels, B. and Scheufen, M. (2020), Wettbewerbseffekte der Europäischen Datenschutzgrundverordnung: Eine Analyse basierend auf einer Befragung unter deutschen Unternehmen, IW-Report, No 1/2020, Institut der deutschen Wirtschaft (IW), Köln.

Enichlmair, C., Dorr, A., Hosner, D., Petzlberger, K., Schrammel, J. (2019), Bürokratiebelastung im niederösterreichischen Gewerbe und Handwerk 2019, Endbericht, https://www.kmuforschung.ac.at/wp-content/uploads/2020/01/B%C3%BCrokratie-Gewerbe-und-Handwerk-N%C3%96-2019-Endbericht.pdf (online, accessed 6 April 2023).

European Commission (2021), 'Better regulation' toolbox – November 2021 edition, https://commission.europa.eu/system/files/2023-02/br_toolbox-nov_2021_en.pdf (online, accessed 22 March 2023).

Federal Administrative Court (Austria) (2020), decision of 26 November 2020, W258 2227269-1, available at https://ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20201126_W258_2227269_1_00/BVWGT_20201126_W258_2227269_1_00.pdf (online, accessed 24 May 2023).

Federal Administrative Court (Austria) (2020), decision of 22 December 2020, W258 2225293-1, available at https://ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20201222_W258_2225293_1_00/BVWGT_20201222_W258_2225293_1_00.pdf (online, accessed 24 May 2023).

Federal Constitutional Court (Germany) (2010), decision of 27 April 2010, 2 BVL 13/07, ECLI:DE:BVerfG:2010:lk20100427.2bvl001307.

Federal Labour Court (Germany) (2021), judgment of 16 December, 2021, 2 AZR 235/21, ECLI:DE:BAG:2021:161221.U.2AZR235.21.0, available at https://www.bundesarbeitsgericht.de/entscheidung/2-azr-235-21/ (online, accessed 24 May 2023).

Fiscal Court of Berlin-Brandenburg (2022), judgment of 26 January 2022, 16 K 2059/21, openjur 2022, 7472, available at https://openjur.de/u/2393347.html (online, accessed 25 May 2023).

Garante (not dated), Principi fondamentali del trattamento, available at https://www.garanteprivacy.it/home/principi-fondamentali-del-trattamento (online, accessed 24 May 2023).

Garante (not dated), Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali, available at https://servizi.gpdp.it/databreach/s/self-assessment (online, accessed 24 May 2023).

Garante (not dated), Istruzioni per l'utilizzo della procedura telematica per la notifica delle violazioni dei dati personali, available at https://servizi.gpdp.it/databreach/s/istruzioni (online, accessed 24 May 2023).

Garante (not dated), Effettua la notifica utilizzando la firma digitale, available at https://servizi.gpdp.it/databreach/s/scelta-auth (online, accessed 24 May 2023).

Garante (not dated), Scheda Registro dei Trattamenti del responsabile/sub-responsabile, available at https://www.garanteprivacy.it/documents/10160/0/Modello+di+%E2%80%9Cregistro+semplificato%E2%80%9D+delle+attivit%C3%A0+di+trattamento+del+responsabile+per+PMI.pdf/5a4dfd05-6c79-ff2f-f48f-14e5a3a87817?version=1.1 (online, accessed 25 May 2023).

Garante (not dated), Scheda Registro dei Trattamenti per titolare (contitolare/rappresentante del titolare, available at https://www.garanteprivacy.it/documents/10160/0/Modello+di+%E2%80%9Cregistro+semplificato%E2%80%9D+delle+attivit%C3%A0+di+trattamento+del+titolare+per+PMI.pdf/ca77f44e-0f85-4b01-6135-f3a7fc5182ec?version=1.2 (online, accessed 25 May 2023).

Garante (not dated), Violazioni di dati personali (data breach) in base alle previsioni del Regolamento (UE) 2016/679, available at https://www.garanteprivacy.it/regolamentoue/databreach (online, accessed 25 May 2023).

Garante (2007), Practical guidelines and simplifying measures for SMEs [1435985], https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1435985 (online, accessed 18 April 2023).

Garante (2013), Privacy: working with business. Ten corporate best practices to improve your business, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2676236 (online, accessed 18 April 2023).

Garante (2018), Guida all'applicazione del Regolamento UE 2016 679, available at https://www.privacyitalia.eu/wp-content/uploads/2018/03/Guida-al-Gdpr-2018.pdf (online, accessed 25 May 2023).

Garante (2018), FAQ sul registro delle attività di trattamento, available at https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento (online, accessed 25 May 2023).

Garante (2019), Relazione annuale 2019, available at https://www.garanteprivacy.it/documents/10160/0/Relazione+annuale+2019.pdf/4fcc5ca8-5ca7-432f-c3f8-4e9e69181a23?version=1.1 (online, accessed 24 May 2023).

Garante (2019), Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach), available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9126951 (online, accessed 25 May 2023).

Garante (2020), Relazione annuale 2020, available at https://www.garanteprivacy.it/documents/10160/0/Relazione+annuale+2020.pdf/286a6332-896a-d4b1-a2da-e32d-7d4838c9?version=2.0 (online, accessed 24 May 2023).

Garante (2021), Notifica di una violazione dei dati personali, available at https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni (online, accessed 24 May 2023).

Garante (2021), Relazione annuale 2021, available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9787195 (online, accessed 24 May 2023).

GDD-Praxishilfe DS-GVO (Va) (2022), Verzeichnis von Verarbeitungstätigkeiten-Verantwortlicher, Version 2.2, available at https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ds-gvo-verzeichnis-von-verarbeitungstaetigkeiten/view (online, accessed 25 May 2023).

GDD-Praxishilfe DS-GVO (Vb) (2020), Verzeichnis von Verarbeitungstätigkeiten-Auftragsverarbeiter, Version 1.0, January 2020, available at https://www.gdd.de/downloads/praxishilfen/GDDPraxishilfe_5bVVTAuftragsverarbeiter.pdf (online, accessed 25 May 2023).

GENERAL DATA PROTECTION REGULATION (GDPR), REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:32016R0679 (online, accessed 23 March 2023).

Global Cyber Security Center (GCSEC) and Europrivacy (2016), Survey sul nuovo Regolamento Europeo Privacy.

Gola, P. (2018), Commentation on Art. 33 GDPR, in Gola, P. (ed.) Datenschutz-Grundverordnung, Kommentar. 2nd edition.

Gola, P. (2018), Introduction, in Gola, P. (ed.) Datenschutz-Grundverordnung, Kommentar. 2nd edition.

Gottweis, A. (2018), Das Verzeichnis von Verarbeitungstätigkeiten gem Art 30 DSGVO, in Jahnel, D. (ed.), Jahrbuch Datenschutzrecht 2018, 49.

Higher Regional Court of Stuttgart (2021), judgment of March 31, 2021, 9 U 34/21, openJur 2021, 29387, available at https://openjur.de/u/2354794.html (online, accessed 25 May 2023).

Horn, B. (2017), DS-GVO ante portas: Die Dokumentationspflichten im Verarbeitungsverzeichnis nach Art 30 DS-GVO, jusIT 2017, 106.

International Association of Privacy Professionals (IAPP) (2018), Analysis: Italy's GDPR implementation law, https://iapp.org/news/a/analysis-italys-gdpr-implementation-law/ (online, accessed 18 April 2023).

Jahnel, D. (2020), Kommentar zur Datenschutz-Grundverordnung.

König, G. / Schaupp, A. (2022), Commentation on Art. 33 GDPR, in Knyrim. R. (ed.), Der DatKomm.

Legal Tribune Online (2018), Datenschutzverfahren gegen Knuddels abgeschlossen, available at https://www.lto.de/recht/nachrichten/n/knuddels-datenschutz-hacker-bussgeld-kooperation/ (online, accessed 24 May 2023).

Legge n. 675 del 31 dicembre 1996 – Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/28335 (online, accessed 18 April 2023).

LfDI Baden-Württemberg (not dated), Meldung von Datenpannen, available at https://www.baden-wuerttemberg.datenschutz.de/meldung-von-datenpannen/ (online, accessed 25 May 2023).

LfDI Baden-Württemberg (not dated), Sample template for a processing directory pursuant to Article 30 of the GDPR with deletion concept pursuant to Article 17 (1) of the GDPR (Excel spreadsheet) with sample entries for applicant data available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/11/211129_Arbeitshilfe_VV_und_Loeschkonzept_Tabelle-mit-Bsp-Bewerberdaten.xlsx (online, accessed 25 May 2023).

LfDI Baden-Württemberg (2018), press release of 18 November 2018, available at https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/ (online, accessed 25 May 2023).

LfDI Baden-Württemberg (2018), 34th activity report, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/LfDI-34.-Datenschutz-T%C3%A4tigkeitsbericht-Internet.pdf (online, accessed 25 May 2023).

LfDI Baden-Württemberg (2019), 35th activity report, p. 7, 131, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/01/35.-T%C3%A4tigkeitsbericht-f%C3%BCr-den-Datenschutz-Web.pdf (online, accessed 25 May 2023).

LfDI Baden-Wuerttemberg (2020), Training video „Europaweit geltende Regelungen praktisch umgesetzt, Folge 2: Verarbeitungsverzeichnis nach Art. 30 Abs. 1 DS-GVO", available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/07/Schulung-Verarbeitungsverzeichnis-2020-07.mp4 (online, accessed 25 May 2023).

LfDI Baden-Württemberg (2021), 37th activity report, p. 120, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/02/22020225_Taetigkeitsbericht_TB-Datenschutz_2021_V1.pdf (online, accessed 25 May 2023).

LfDI Baden-Wuerttemberg (2022), Prüfung der Datenpannenmeldung abgeschlossen, available at https://www.baden-wuerttemberg.datenschutz.de/pruefung-abgeschlossen/ (online, accessed 24 May 2023).

LOI n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, (dite "Loi Informatique et Libertés"), https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460 (online, accessed 29 March 2023).

LOI n°2018-493 du 20 juin 2018 relative à la protection des données personnelles, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952 (online, accessed 29 March 2023).

Mc Cullagh, K., Tambou, O., Bourton, S. (eds.) (2019), National Adaptations of the GDPR, Collection Open Access Book, Blogdroiteuropeen, 130 pages, https://iris.unito.it/bitstream/2318/1721974/1/national-adaptations-of-the-gdpr.pdf (online, accessed 18 April 2023).

Medinsoft (2019), Livre blanc RGPD, available at https://medinsoft.com/wp-content/uploads/2019/05/LivreBlanc_LegalInTech.pdf (online, accessed 25 May 2023).

Ministry of Economy, Finance and Industrial and Digital Sovereignty (France) (2022), Le développement de l'assurance du risqué cyber, available at https://medias.vie-publique.fr/data_storage_s3/rapport/pdf/286216.pdf (online, accessed 25 May 2023)

Nguyen, A., Commentation on Art. 51 GDPR in Gola, P. (ed.) Datenschutz-Grundverordnung, Kommentar. 2nd edition.

Osservatorio Cybersecurity & Data Protection (2019), GDPR: lo stato di adeguamento delle imprese italiane, https://www.osservatori.net/it/prodotti/formato/report/gdpr-imprese-italiane (online, accessed 18 April 2023).

Panetta, R. (2017), The data protection reform and its impact on the Italian legal system: Between hopes and expectations. Journal of Data Protection & Privacy, 1(2), pp. 183–192(10).

Piltz, C. (2019), Was ist eine „Verarbeitungstätigkeit" im Sinne der DSGVO?, available at https://www.delegedata.de/2019/03/was-ist-eine-verarbeitungstaetigkeit-im-sinne-der-dsgvo/ (online, accessed 25 May 2023).

Regional Court of Essen (2021), judgment of 23 September 2021, 6 O 190/21, openJur 2021, 32607, available at https://openjur.de/u/2362644.html (online, accessed 25 May 2023).

Regional Labour Court of Schleswig-Holstein (2019), decision of 6 August 2019, 2 TaBV 9/19, available at https://www.iww.de/quellenmaterial/id/211754 (online, accessed 25 May 2023).

Schmiedhofer, H. (2019), Die Datenschutzgrundverordnung 2016 und daraus resultierende Anforderungen an Klein- und Mittelunternehmen in Österreich, https://unipub.uni-graz.at/obvugrhs/download/pdf/3658989?originalFilename=true (online, accessed 6 April 2023).

Schricker, J. (2018), Wie sehen die Unternehmen die neue Datenschutzgrundverordnung, ifo Schnelldienst, ISSN 0018-974X, ifo Institut – Leibniz-Institut für Wirtschaftsforschung an der Universität München, München, 71(15), pp. 35–39.

Statistisches Bundesamt (2023), Statistisches Unternehmensregister. 87 % der Rechtlichen Einheiten mit weniger als zehn Beschäftigten, https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Unternehmensregister/unternehmen-kleine.html (online, accessed 27 March 2023).

Statistisches Bundesamt, Wiesbaden im Auftrag der Bundesregierung und des Nationalen Normenkontrollrates (2022), Leitfaden zur Ermittlung und Darstellung des Erfüllungsaufwands in Regelungsvorhaben der Bundesregierung, https://www.destatis.de/DE/Themen/Staat/Buerokratiekosten/Publikationen/Downloads-Buerokratiekosten/erfuellungsaufwand-handbuch.pdf?__blob=publicationFile (online, accessed 22 March 2023).

Supreme Administrative Court (Austria) (2021), decision of 14 December 2021, Ro 2021/04/0007-4, available at https://ris.bka.gv.at/Dokumente/Vwgh/JWT_2021040007_20211214J00/JWT_2021040007_20211214J00.pdf (online, accessed 24 May 2023).

Unione Industriale Verbano Cusio Ossola (2018), Privacy: modello di registro delle attività di trattamento e glossario available at http://www.uivco.vb.it/web/binary/saveas?filename_field=datas_fname&field=datas&model=ir.attachment&id=4087 (online, accessed 25 May 2023).

Foundation for Family Businesses
(Stiftung Familienunternehmen)

Prinzregentenstrasse 50
80538 Munich
Germany

Phone + 49 (0) 89 / 12 76 400 02
Fax + 49 (0) 89 / 12 76 400 09
E-mail info@familienunternehmen.de

www.familienunternehmen.de/en

Price: 39,90 €

ISBN: 978-3-948850-35-7