Hendrickx, Frank

Working Paper

Protection of workers' personal data: General principles

ILO Working Paper, No. 62

Provided in Cooperation with:
International Labour Organization (ILO), Geneva

Suggested Citation: Hendrickx, Frank (2022) : Protection of workers' personal data: General principles, ILO Working Paper, No. 62, ISBN 978-92-2-036891-6, International Labour Organization (ILO), Geneva, https://doi.org/10.54394/VBKR9991

This Version is available at:
https://hdl.handle.net/10419/263125

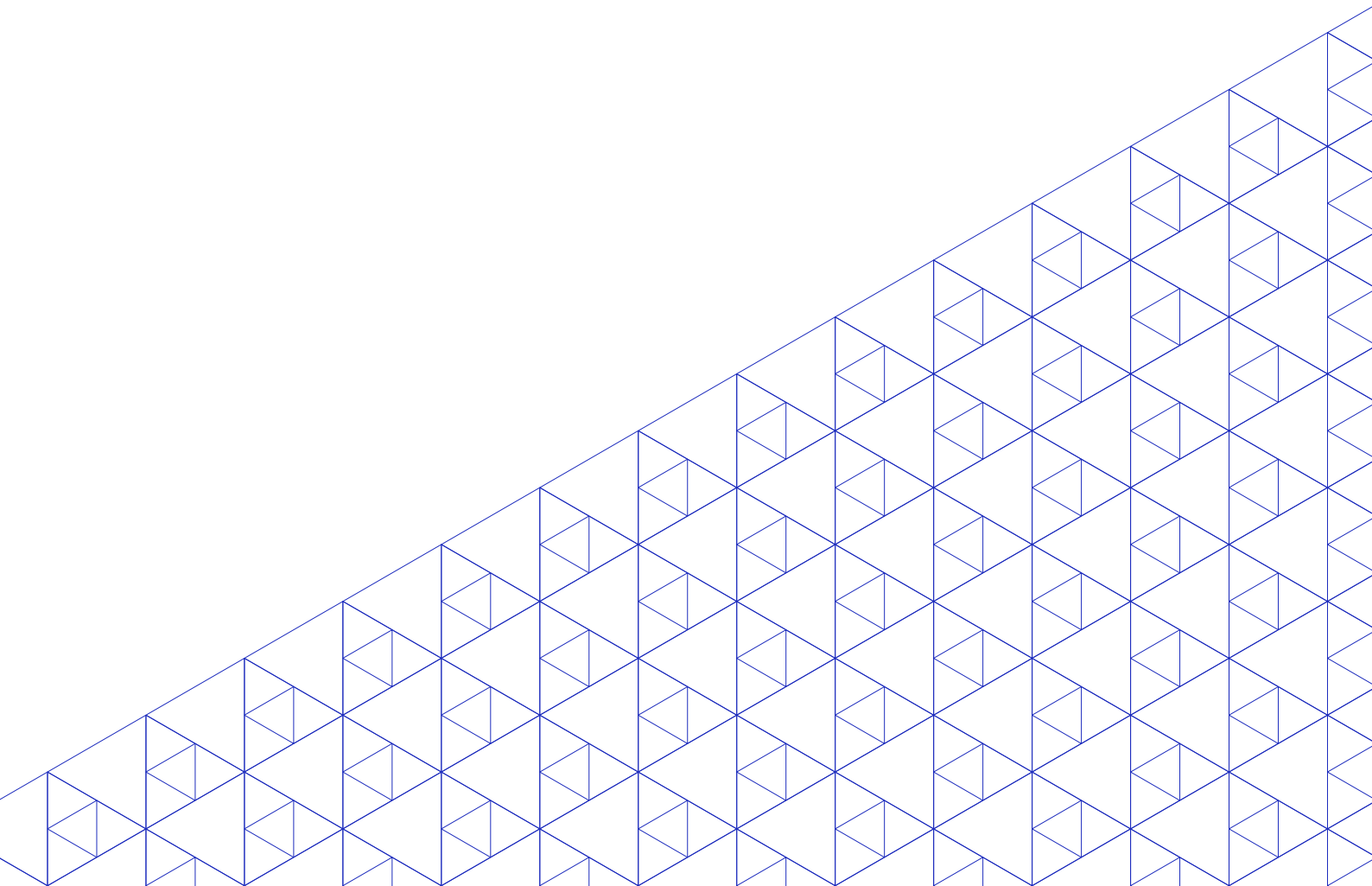
International Labour Organization

ILO Working Paper 62

May / 2022

Protection of workers' personal data: General principles

Author / Frank Hendrickx



ISBN: 9789220368909 (print)
ISBN: 9789220368916 (web-pdf)
ISBN: 9789220368923 (epub)
ISBN: 9789220368930 (mobi)
ISBN: 9789220368947 (html)
ISSN: 2708-3446

https://doi.org/10.54394/VBKR9991

ILO Working Papers summarize the results of ILO research in progress, and seek to stimulate discussion of a range of issues related to the world of work. Comments on this ILO Working Paper are welcome and can be sent to inwork@ilo.org.

Authorization for publication: Philippe Marcadent, Chief, Inclusive Labour Markets, Labour Relations and Working Conditions Branch

ILO Working Papers can be found at: www.ilo.org/global/publications/working-papers

Suggested citation:
Hendrickx, F. 2022. *Protection of workers' personal data: General principles*, ILO Working Paper 62 (Geneva, ILO).

Abstract

This working paper gives an overview of legal standards related to personal data protection. It explores trends, principles and good practices and brings them in relation to the world of work. The aim of this working paper is to give a global and updated outlook of the leading and basic legal principles and standards in this area. The focus is on data protection principles which have a general nature and which can be embedded in a global approach. This working paper attempts to expose and clarify general data protection principles, having in mind that these principles are applicable in the context of the evolving employment relationship, taking into account technological evolutions. An understanding of general data protection principles is considered necessary to comprehend their application in the work environment and to build further towards principles that relate to more specific areas and problem fields.

About the authors

Frank Hendrickx is full professor of labour law at the Law Faculty of KU Leuven (Belgium). He specialises in national, European and comparative labour law, workplace privacy law and sports law. He is the General Editor of the International Encyclopaedia of Laws, Editor of the International Encyclopaedia of Labour Law and Industrial Relatoins, Editor of the Bulletin of Comparative Labour Relations and Editor-in-chief of the European Labour Law Journal.

This paper was written with collaboration of: Elena Gramano (Bocconi University), David Mangan (Maynooth & York University) and Simon Taes (KU Leuven), assisted by Stan Bruurs (KU Leuven) and Sara Huybrechts (KU Leuven).

Table of contents

Introduction

Aim and scope

This study on "the legal protection of workers' personal data" aims to develop the knowledge base on this subject in light of legal and technological developments.

The purpose of this working paper is to give an overview of legal standards related to workers' personal data protection and, from both a global and regional point of view, to explore trends, principles and good practices.

The legal landscape in the field of personal data protection has strongly evolved over time. Many global and regional initiatives have led to standards on personal data protection. The European Union came with a 'General Data Protection Regulation' (GDPR) in 2016. Twenty years earlier, the ILO adopted its Code of Practice on the protection of workers' personal data.[1] Other forms of standards developed both within regional organisations as well as in many countries around the world.

The aim of this working paper is to give a global and updated outlook of the main and basic principles in this area, taking into account legal sources and principles from a comparative perspective. In light of this, the focus will be on data protection principles which have a *general* nature and which can be embedded in a *global* approach of 'the basics', laying ground for a variety of circumstances. Against this background, this working paper attempts to expose and clarify general data protection principles, having in mind that these principles are applicable in the context of the employment relationship. An understanding of the general data protection principles themselves is considered necessary in order to comprehend their application in the work environment.

With this approach in mind, this working paper has limitations. The relevance and importance of specific areas of workers' personal data protection should not be neglected. However, with a view to limit this working paper to basic principles, more specific or complementary principles related to electronic or digital monitoring and surveillance, or specific rules in relation to health data, will not be fully elaborated. Based on the research undertaken for this work paper, the finding is not only that these specific areas are extremely important for the update of the international knowledge base, but the suggestion is that this requires an in-depth follow-up study in its own worth.

A similar approach is undertaken with regard to the discussion on artificial intelligence, robotisation and similar forms of automation. These developments bring new regulatory challenges for the world of work and for data protection law. While this area is sufficiently vast and specific to deserve a separate in-depth study, this report will, within its limits, remain sufficiently sensitive to capture the legal data protection issues arising from them.

Methodology

This study uses a multiple set of legal research methods and sources, mainly involving desk research, including library searches and official websites (specific attention to government departments for justice, labour and data protection), applying key-terms based on the study outline. This involves available and relevant

[1] This code of practice was adopted by a meeting of experts on workers' privacy of the ILO, convened in Geneva from 1 to 7 October 1996 (ILO 1997).

sources of regulation, including legislation, governmental decrees, collective agreements, recommendations, case law, as well as legal scholarship.

In addition, the study used an expert questionnaire with a view to receive input from experts around the world in the cross-sectional field of employment and data protection law. It delivered more precise country related information or clarified selected information. The questionnaire is available with the author of this working paper. The involved expert respondents have been mentioned in the acknowledgment.

Structure

The structure of the report follows the logic of the aims and scope of the working paper. The working paper departs from a main introduction, with a chapter providing a brief setting of the scene, with references to the legal evolution of the privacy and data concepts and standards. A specific chapter discusses the global and regional standard setting in the field of data protection, paying attention to both the global and regional outlook, but also to their mutual influence, their general perspectives as well as, for some, their specific relation to the work context. The issues of AI and 'Industry 4.0.' developments are mentioned in a specific chapter, seen the various and complex challenges in relation to data protection standards and in light of the evolvement of AI related standard setting initiatives.

▶ 1 Understanding general principles

This working paper relies on legally relevant and grounded principles of personal data protection. However, before entering into the relevant global and legal sources in relation to general principles, it is proper to pay attention to their context and to indicate important frameworks of understanding.

1.1. Privacy and data protection

This working paper considers (the right to) personal data protection. The focus of analysis on data protection law follows a logic. The employment environment is a main source of data processing. Contractual obligations, personnel administration and human resources are legitimate motives for – and areas of – data collection and processing. However, an approach to personal data protection needs the broader horizon of the right to privacy. The need for this embedded context has different reasons.

The first reason is that privacy and data protection are overlapping and strongly interdependent legal notions. It is accepted that the right to privacy covers the right to data protection, even outside automatic or semi-automatic data processing.[2] The European Human Rights Court's (ECtHR) case law is an example where rules on data protection have been conceived under the concept of the right to privacy.[3] South Africa is another good example of this broader contextual approach. In this country, the right to personal data protection is seen as a derivative of the constitutional right to privacy.[4] Also other regional perspectives, such as the Indian approach, show that the right to privacy is construed as protection of personal data.[5]

The second reason is that privacy is a reinforcing notion for personal data protection. The right to privacy was defined in 1890 by Warren and Brandeis as "the right to be let alone".[6] Since then, privacy protection strongly evolved over time. It increasingly provided important and various ways of protection in the employment context. It not only covers 'private life', or the 'life away from the public', but a much wider field, including the more 'public' context as well as the workplace and human interaction in a work context. The privacy notion has appeared as flexible, responsive and adaptive to new circumstances. The right to privacy fits with a human-in-command approach, which shows its relevance in discussions on AI and robotisation.[7] In this respect, the report of the Commission on the Future of Work confirms the link between privacy risks, the generation of "large amounts of data on workers" as well as "algorithmic accountability in the world of work".[8]

A third reason, related with the open-textured and responsiveness of the right to privacy, is its connection to the societal and economic context in which that right is promoted or protected. While the right to privacy, and data protection, is universally accepted as a human right, its understanding remains connected with a social and cultural, even politico-historical bind.[9] It may mean that international level principles may need to take into account possible different jurisdictional approaches, though with a common baseline.[10]

2 Some speak about "data privacy", cf. Navarro-Arribas and Torra 2015.
3 See *Leander v. Sweden*, ECtHR 26 March 1987, Series A No 116, p. 22, § 48.
4 Abdulrauf 2020, p. 351.
5 *Shri S. K. Chaurasiya vs Central Vigilance Commission* [2010], cited in Walters et al. 2019, p. 151.
6 Warren and Brandeis 1980.
7 Hendrickx 2019a.
8 ILO 2019, p. 44.
9 Whitman 2004, pp. 1151-1153.
10 Krotoszynski 2016, p. 9; Makulilo 2016, p. 4.

1.2. The employment context

In this study, we aim to take both the legal nature of privacy and data protection as well as the specific context of the employment relationship into account. Based on an international and regional human rights perspective, workers have a right to privacy. However, this legal departure point needs some further qualification for the employment relationship.

An employment relationship implies, in a widely applied view, a relation of subordination or dependency.[11] This implies that the worker's personal freedom is limited to the extent that the employer is in principle entitled to manage and direct the work and thus to have a say over its workers' personal behaviour, to obtain information and to control and discipline workers. Whereas the right to privacy encompasses the 'right to be let alone', the employment relationship gives the employer the 'right not to leave alone' its workers.

The right to privacy and data protection is, in principle, guaranteed for all workers, regardless of the type of employment relationship. The employment relationship must, therefore, also be envisaged in its most modern forms and privacy and data protection considerations must be taken into account in different contexts of employment. The issues of privacy and data protection are, for example, increasingly challenged in the context of 'place and time independent' forms of employment, (such as telework)[12] or in the platform economy. As the analysis will take into account these diverse contexts of work, it may form a stepping stone towards the effective recognition that "*all workers, regardless of their contractual arrangement or employment status, must equally enjoy adequate labour protection to ensure humane working conditions for everyone*".[13]

The European Working Party,[14] in its Opinion N° 2/2017, confirms this broad approach towards the application of the EU's GDPR:

> "Where the word "employee" is used in this Opinion, WP29 **does not intend to restrict the scope of this term merely to persons with an employment contract** recognized as such under applicable labour laws. Over the past decades, new business models served by different types of labour relationships, and in particular employment on a freelance basis, have become more commonplace. This Opinion is intended to cover all situations where there is an employment relationship, regardless of whether this relationship is based on an employment contract."[15]

In addition to this, it can be pointed out that rights of data subjects are able to be respected by employers, but the provisions also imply respect by other parties, such as governments, HR providers, colleagues, subcontractors, workers' organisations, and so on.

Beyond the employment relationship, an employment context involves a variety of rights and interests which are broader than purely those of the contracting parties. Legitimate interests of colleagues, clients or the wider public may exercise an influence on the way how the right to privacy or the right to data protection are approached and they may also limit the exercise of this right in a work context. The worker's right to privacy and data protection is therefore qualified by the employment relationship.[16] This will require that the opposition of rights will be part of the discussion, requiring a reconciliation of rights and interests in the employment context. In an employment privacy discourse, reasonable privacy expectations have to be taken into consideration.

---

11 Cf. Paragraph 12, ILO Employment Relationship Recommendation (15 June 2006), R198. The Recommendation, nevertheless, indicates this as an example and mentions, in section 13, the indicators of the existence of an employment relationship that Member States may use.

12 Eurofound and ILO 2017.

13 ILO 2019, p. 38.

14 This independent and advisory Working Party was set up under Article 29 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Its activities ended following the entry into force of the GDPR on 25 May 2018.

15 Article 29, Working Party (2007), *Opinion 4/2007 on the concept of personal data*, WP 136, 20 June 2007, p. 4.

16 Hendrickx 1999, pp. 47 and 51.

1.3. Role of technology

The world of work is confronted with an increasing attention for privacy and data protection. The role of technological development is apparent. Automation and new technologies have not only challenged the world of work, they also have influenced the evolution of the right to privacy and data protection. More recent developments and technological evolutions, such as digitalisation, big data, the internet of things, artificial intelligence and robotisation are affecting the world of work in such a way that attention to privacy and data protection grows with an increased pace and relevance. It has been argued that the dynamic privacy concept has adapted itself over time on the pace of new technological challenges, and the idea of "privacy 4.0"[17] has been seen as a response to 'industry 4.0.' and other disruptive models that attempt to explain the complex future of the world of work.[18] It not only marks the right to privacy as a 'layered' concept, it also confirms its technological responsiveness in a broader perspective.

Various (international) regulators have started to address the issue of personal data protection since the 1980's and 1990's, as will be shown below. Data protection laws and principles have originated in a time that computerisation and electronic databases stood central. During the last decennia of the 20th Century, technological evolutions not only brought computers, but also the internet, with enormous potential of data processing and new electronic communication possibilities. Some of the data protection principles of today still resonate this background, although in a modernised context.

With the paradigm of data protection law evolving over time, there is still room for new evolutions. Increased attention for data protection has come in a world concerned about increased and ultimately unlimited possibilities of data processing, the centralisation and interconnection of data, the fast flow of data and disclosure of information, the ease of manipulation, information asymmetry, and so on. While the 'big brother' metaphor has often been used, it may be noted that data protection problems of the future need to take into account additional approaches, for example as a problem of vulnerability, powerlessness and dehumanisation.[19]

1.4. Changing work-life relations

Another crucial dimension for the future approach of privacy and data protection law in the employment context is the fast evolving and changing world of work and its impact on the work-life context. This goes along with technological innovation allowing new ways of working. A few developments have increased a blurring of boundaries between the sphere of work and the sphere of private life. They lead to a new 'privatisation' of the workplace.

A first evolution is the rise of digital and online communication, such as e-mail and internet. In the employment context, issues have arisen with regard to workers using professional communication systems for personal reasons or bringing personal communication systems into the workplace (including because of 'bring your own device' policies). This mix of private and professional communication not only causes discussion with regard to the monitoring of communication but also to the limits to the (personal) use of communication means in an employment context.

A second development concerns the rise of the virtual workplace. For a number of years, the workplace is gradually shifting towards a more digital workplace. It has come with a new way of looking at the employment relationship, allowing for work to be organised and performed digitally and sometimes in a more

17 Hendrickx 2019b.
18 K. Schwab, The fourth industrial revolution: what it means and how to respond, World Economic Forum, (January 14, 2016); Schwab 2017, 1-128.
19 Cf. Solove 2001.

autonomous way on the side of the worker. It has given rise to a fast growth of home work in the form of telework, with new challenges for work-life boundary management, as confirmed by an ILO/Eurofound study.[20]

A third element is the impact of the use of social media on the work context or the employment relationship. Not only have businesses shown an interest in online recruiting and social media presence. The impact of the use of social media by workers on the employment relationship creates additional tensions and new forms of work-private life interactions.

1.5. New privacy expectations

Along with the technological (r)evolution, work relations have to be understood, more than ever, in terms of privacy relations.[21] The environment of work has developed in such a way, that it becomes hard to escape from various forms of data processing, monitoring, tracking or generally connecting to the digital world. Furthermore, the idea that the workplace delivers a relatively simple context of employers supervising workers, has to be left behind. Not only do management and supervision of work (and workers) come in new digital ways, it may also be in the hands of different actors and even with a complex of automated systems beyond individual or even the employer's full control. The impact on privacy expectations is thus potentially significant. However, at the same time, legal developments towards privacy protection, in light of privacy expectations, are also broadening privacy protection in the work environment.

Since the right to privacy and data protection is to be seen as a fundamental human right, it is protected as such in many instruments and constitutions around the world. This 'fundamental' character brings the rights discourse to the level that justifications of privacy interferences should be dealt with along the lines of human rights protection mechanisms. As the employment context will bring a variety of opposing rights and interests to the right to privacy and data protection, principles of human rights protection will be relevant. An interference or limitation of a fundamental right can be expected to at least require the respect of principles including legitimacy, lawfulness, transparency and proportionality.[22]

However, specific issues of limitations arise in the employment context, due to the increasingly relevant presence of reasonable expectations of privacy. The employment relationship is a context in which the worker's personal freedom and privacy are almost per definition exposed. This does not mean, self-evidently, that a worker cannot have a right to privacy. However, in an (employment) context, reasonable privacy expectations have to be taken into consideration. This concept arises on the horizon due to developments in (North) American as well as European legal systems.[23]

---

20 Eurofound and ILO 2017, p. 5.
21 Moore 2020, p. 32.
22 Hendrickx 2014.
23 S. Nouwt and B.R. de Vries, "Introduction" in Nouwt et al. 2005, p. 3; Finkin 2003, p. xxix; Silva 2020, pp. 627-628; Raepsaet 2011, pp. 145, 147 and 153.

▶ 2 Global sources development

The search for general principles of personal data protection in a global perspective requires a focus on their relevance to the work environment, whereby both international, regional and country perspectives and sources need to be taken into account. The legal source framework will be developed, taking into account the global dynamics in international, regional and national instruments with regard to the right to privacy and data protection and the common grounds on which they may be based.

2.1. Global perspective

As mentioned before, the right to privacy and data protection is a result from a complexity of developments, including technological evolution, but also socio-political as well as legal change. It makes privacy approaches partly universally, partly culturally driven. Whereas privacy and data protection, as notions, have first arisen in Western legal systems, they have evolved throughout the globe. The notion of privacy appeared first in the U.S. legal system, but it has later on been conceptually imported, elaborated and adapted in Europe, where approaches on human dignity and personality rights pre-existed.[24]

While the right to privacy further developed in the North American legal system, European jurisdictions became strongly influenced by the case law of the European Court on Human Rights, under the European Convention on Human Rights (1950), which steadily expanded the number of issues as well as the privacy concept itself.

One of the first international organisations to take up the lead in the increasing regulatory attention to data processing and the concerns of privacy protection was the OECD. The OECD guidelines (see section 3.3) were strongly based on the American 'FIPPS',[25] but they were the first international legal instrument in the field.

During the decennia that followed, regulation of data protection gained momentum, mainly in Europe. The Council of Europe followed up with the adoption of Convention 108 with regard to personal data protection on 28 January 1981.[26] As national European responses were somewhat diffused, and seen the growing impact of the rising digital society, the European Union took the initiative to adopt legislation in 1995. The new millennium, with various challenges, including technological evolution, brought the European Union to modernise its legislation with the adoption of the General Data Protection Regulation (GDPR) in 2016.

In the meantime, the development of the right to privacy and data protection slightly evolved in other regions of the world. Yet data protection laws have been a more recent phenomenon in other parts of the world, such as in Asian and African countries, or within the broad Latin America and Pacific region. While member States of the OECD like Australia already had data protection legislation since the eighties, most Central, Southeast and East Asian countries, would only come rather recently with regulatory interventions.[27] Many African countries have more recently drafted data protection legislation, or are in the process of making it.[28] The initiatives these other parts of the world also brought new driving forces in transnational coop-

[24] Whitman 2004.
[25] Fair Information Practices based on Fair Information Practices Principles; For a recent state of U.S. frameworks, see Baker McKenzie (2018) *Global Privacy and Information Management Handbook*, available at: https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/global_privacy_handbook-_2018.pdf?la=en
[26] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Strasbourg, 28 January 28, 1981, ETS no 108).
[27] Walters et al. 2019, p. vii.
[28] https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf

eration on standard-setting in the field. As will be explained below, various regional initiatives have been taken in Africa, Asia and Latin America. It should be noted, however, that many of these initiatives either resonate, reflect or take the model of the OECD or European data protection standards.

Against the background of these dynamics and global legal development, the European Union legislation, and mainly the GDPR, has been influencing data protection legislation around the world. It often stands as an example or benchmark for new data protection legislation.[29]

While the influence of the European standard setting model seems to attract attention, this study will inevitably relate to the latest developments in the various parts and regions of the world, knowing that European legal sources related to privacy and data protection give a strong and important benchmark.

At the same time, the main international instrument with a focus on data protection in the employment context is the ILO Code of Practice (1996). This document remains a central reference of data protection principles and will be referred to and used throughout this study.

2.2. Human rights sources

The human rights dimension of the issue of privacy and data protection cannot be overlooked. Various international documents make reference to it. The right to privacy is guaranteed by Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.

Most regions in the world would now also recognize the right to privacy and/or data protection. The most important **European** instruments context are the European Convention on Human Rights (ECHR) and the Charter on Fundamental Rights of the European Union (CFREU). Article 8 of the ECHR guarantees the right to respect for private and family life. Articles 7 and 8 CFREU guarantee the right to private life and the right to data protection respectively. The Explanations on these articles of the CFREU provide that the rights guaranteed in this article correspond to those guaranteed by the ECHR. There is a vast area of case law of the European Court on Human Rights (ECtHR) with respect to Article 8 ECHR.

Article 11 of the **American Convention on Human Rights** (1969)[30] relates to the right to privacy. ASEAN, the Association of South-East Asian countries, protects the right to privacy, including the right to data protection, through section 21 of the **ASEAN Human Rights Declaration**. While the African Charter on Human and Peoples' Rights (African Charter) does not expressly refer to the right to privacy, this right is nevertheless inferred from other fundamental rights in the Charter, such as the right to life and human dignity.[31] Furthermore, the African Commission on Human and Peoples' Rights (the African Commission) adopted the "Declaration of Principles of Freedom of Expression and Access to Information in Africa" (**African Declaration**), in 2019, referring to the right to privacy.

2.3. Sources on data protection

Different international or regional organisations have addressed the right to data protection. The various initiatives give shape to general data protection principles. Furthermore, taking into account the need to give more guidance in this regard, data protection in the employment relationship has received specific attention.

[29] Lee A. Bygrave, "Prospects for global consensus", in Bygrave 2014, p. 208, citing Greenleaf 2012.
[30] The Convention is open for signature and ratification by or adherence of any member state of the Organisation of American States. https://www.oas.org/dil/access_to_information_American_Convention_on_Human_Rights.pdf.
[31] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

a. UN instruments

The United Nations do not have a specific standard with regard to data protection, although it follows the subject very closely and has taken various initiatives. On 14 December 1990, the UN General Assembly adopted the **Guidelines for the Regulation of Computerized Personal Data Files**[32], which established minimum guarantees that should be provided in national legislations and were designed to apply to personal data files kept by governmental international organisations. On 18 December 2013 the UN's General Assembly adopted resolution nr. 68/167 on the right to privacy in the digital age,[33] in which it expressed its concern about the evolution of technology making possible "surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights." On 18 December 2014 the General Assembly adopted resolution nr. 69/166 on the right to privacy in the digital age,[34] which encourages the Human Rights Council to remain seized of the debate. The Human Rights Council appointed a special rapporteur on the right to privacy.[35]

b. OECD

The OECD has been one of the first organisations to respond to the increase of automated data processing and the concern to address the issue of data protection with an international instrument. On 23 September 1980, the OECD adopted a **Recommendation concerning guidelines governing the protection of privacy and transborder flows of personal data**. As the title of this recommendation suggests, it concerns a set of guidelines with basic principles of data protection.[36] The OECD updated the guidelines on 11 July 2013.[37] The OECD Guidelines have exercised an influence on the making of national data protection laws around the world.[38]

c. Europe

The European legal order has to be seen both from the perspective of the European Union as well as the Council of Europe.

The origins of EU data protection legislation can be found in the Data Protection Directive 95/46/EC on 24 October 1995,[39] with which the EU created a major legal instrument on the subject. In 2012, the European Commission took the initiative to reform the data protection legislation, taking into account considerations of new technological developments and the effective exercise of rights.[40] This led to the adoption of the '**General Data Protection Regulation'**, known as the **GDPR**, on 27 April 2016.[41] The regulation is applica-

---

32 UN General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*, (December 14, 1990), available at: https://www.refworld.org/docid/3ddcafaac.html.

33 http://undocs.org/A/RES/68/167.

34 Resolution adopted by the General Assembly on 18 December 2014 [on the report of the Third Committee (A/69/488/Add.2 and Corr.1)] 69/166. The right to privacy in the digital age; http://dag.un.org/bitstream/handle/11176/158167/A_RES_69_166-EN.pdf?sequence=3&isAllowed=y.

35 Resolution adopted by the Human Rights Council 28/16. The right to privacy in the digital age; http://repository.un.org/bitstream/handle/11176/311688/A_HRC_RES_28_16-EN.pdf?sequence=3&isAllowed=y.

36 See for the full text: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

37 See for the full text: http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

38 http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

39 Directive 95/46/EC of the European Parliament and of 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, OJ 23 November 1995, L281/31.

40 COM/2012/09 final.

41 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) *OJ* L 119, 4.5.2016, 1-88.

ble as from 25 May 2018 and replaces the 1995 Directive. The new GDPR is, furthermore, complemented with a new directive.[42]

The Council of Europe adopted **Convention 108** with regard to personal data protection on 28 January 1981,[43] in order to bring more unity in the national legal systems and to protect human rights on a higher level.[44] Also the Council of Europe decided to modernise Convention 108.[45] The modernised convention, adopted on 18 May 2018, is now referred to as "**Convention 108+**". With this instrument, the Council of Europe sought to create a 'global' convention and promotes accession by countries outside Europe. In addition to the 47 European participating states, eight countries outside Europe have become parties, including – at this time of writing – Uruguay, Mauritius, Senegal, Tunisia, Cape Verde, Mexico, Argentina and Morocco, with further outreach to Burkina Faso.[46]

d. Asia-Pacific

In the Asia-Pacific region, different initiatives with regard to privacy and data protection have been taken.

On 16 November 2016, an **ASEAN "Framework on Personal Data Protection"** was adopted, containing a set of principles to guide the implementation of data protection measures at national and regional level.[47] However, also APEC, the Asia-Pacific Economic Cooperation, developed data protection norms. This was done through the **APEC Privacy Framework**, first adopted in 2005 and updated in 2015. This Framework is modelled upon the OECD data protection guidelines[48] but, when drafted, it had due consideration for the different legal features and context of the APEC region.[49]

APEC also adopted the "**Cross Border Privacy Rules system" (CBPR)** in 2011, a voluntary and accountability based system of rules, to facilitate the respect of privacy and personal data protection in information flows among APEC economies.[50] Seen the different initiatives in this region, attempts are made to bridge the initiatives from ASEAN and APEC[51] in order to reach a single and more coherent framework for the whole region.

For the APEC region, it is relevant to mention the Asia Pacific Privacy Authorities (APPA), a forum for privacy authorities in the Asia Pacific region.[52]

It gives privacy authorities in the region an opportunity to form partnerships, discuss best practices and share information on emerging technology, trends and changes to privacy regulation.[53]

---

42 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ* L 119, 4.5.2016, p. 89-131.

43 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Strasbourg, 28 January 28, 1981, ETS no 108).

44 It has been, moreover, ratified by countries outside the Council of Europe. See: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=mScbc290.

45 Explanatory Memorandum, to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Series No. 223.

46 Status April 2020: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures; Greenleaf and Cottier 2020.

47 https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf.

48 For a comparison between the APEC Privacy Framework and the GDPR: https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/.

49 APEC Privacy Framework 2015, Section 5; file:///C:/Users/u0009915/Downloads/217_ECSG_2015%20APEC%20Privacy%20Framework.pdf.

50 APEC Privacy Framework 2015, Section 12; file:///C:/Users/u0009915/Downloads/217_ECSG_2015%20APEC%20Privacy%20Framework.pdf.

51 https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf.

52 https://www.appaforum.org/.

53 https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf.

e. Africa

The legal notions of privacy and data protection have gradually shown up in the African region. While the concept of privacy may be rather new to the cultural and legal traditions of African countries, the value of a regulatory approach has increased over the years. Different African countries have taken initiatives of regulating data protection and various African constitutions have adopted a right to privacy.[54] These legislative initiatives have been promoted, supported and underpinned by African regional initiatives, partly in response to a need for benchmarking and harmonisation.

An important initiative came from ECOWAS, the intergovernmental organisation of Western African countries. The "**ECOWAS Data Protection Act**" was adopted on 16 February 2010.[55] It can be seen as the first real sub-regional initiative to develop a framework of personal data protection law in Africa. Additionally, in 2013, a Model Law on Data Protection was drafted as an initiative from Sub-Saharan Africa.[56]

The African Union (AU), covering 55 African states, followed with a wider African initiative. It adopted in 2014 the **African Union Convention on Cyber Security and Personal Data Protection**. The convention has a rather broad scope, including electronic commerce and cybersecurity, but includes an important part on personal data protection.[57] In order for the Convention to enter into force, 15 ratifications are needed. Only eight have – at this time of writing – done so.[58] The 2014 Convention has been completed by personal data protection guidelines in 2018 in order to facilitate the further promotion of the instrument.[59]

Another relevant African regional document is the revised **Declaration of Principles of Freedom of Expression and Access to Information**, adopted by the African Commission on Human Rights in 2019.[60] This declaration gives guidance on surveillance, privacy and data protection.

f. Latin America and the Caribbean

Latin American countries are slowly coming to a regional development of common standards on privacy and data protection. Countries in this region have been working on data protection law reforms. Some of the major national reforms have been inspired by, or modelled on, the European GDPR, such as the cases of Argentina and Brazil, with a number of countries, such as Chile, Mexico and Uruguay going in the same direction.[61]

Within the **Ibero-American Data Protection Network**, a network of cooperation set up on the initiative of the Spanish data protection authority,[62] adopted on 20 June 2017 a document with **Data Protection**

---

54 Alunge 2020, p. 46; For an overview of enacted data privacy laws in Africa (status February 2020 – with more and other African countries underway with new laws): Cape Verde (2001, amended 2013), Seychelles (2003), Burkina Faso (2004, under revision), Mauritius (2004, revised 2017), Tunisia (2004, under revision), Senegal (2008, under revision), Benin (2009 revised 2017), Morocco (2009, under revision), Angola (2011), Gabon (2011), Lesotho (2011), Ghana (2012), Ivory Coast (Cote d'Ivoire, 2013), Mali (2013), South Africa (2013), Madagascar (2014), Chad (2015), Malawi (2016), Equatorial Guinea (2016), Sao Tome e Principe (2016), Guinea (Conakry) (2016), Mauritania (2017), Niger (2017), Algeria (2018), Botswana (2018), Nigeria (2019), Uganda (2019), Kenya (2019), Congo-Brazzaville (Republic of Congo) (2019), Togo (2019) and Egypt (2020)", Zimbabwe (2002), see Greenleaf and Cottier, 2020 (cf. p.3).

55 Supplementary Act A/SA.1/01/10 Personal Data Protection within ECOWAS, http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf.

56 https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf.

57 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

58 Status 18 June 2020: Angola, Ghana, Guinea, Mauritius, Mozambique, Namibia, Rwanda and Senegal, https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf.

59 Personal Data Protection Guidelines for Africa A joint initiative of the Internet Society and the Commission of the African Union 9 May 2018; https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN-1.pdf.

60 https://www.achpr.org/legalinstruments/detail?id=69.

61 https://www.lexology.com/library/detail.aspx?g=b62b37fd-54dc-4fd4-9c81-36b32767a101.

62 http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA-D1-30-Dec-2014.pdf (cf. p.128).

Standards of the Ibero-American States.[63] The document aims to promote and contribute, through a set of guidelines, regulatory initiatives on personal data in the Ibero-American region. Reflecting the EU's GDPR model, it has served as a blueprint for data protection law reforms and initiatives in the countries of this region.[64] A 2019 study, commissioned under the supervision of the Economic Commission for Latin America and the Caribbean (ECLAC), showed that Latin American countries have tried to establish own initiatives, resonating a combination of the GDPR, the OECD and APEC's regulatory model.[65]

2.4. Sources on data protection in the work environment

While general data protection instruments are in principle applicable in the employment context, some initiatives have been taken to create more specific guidance for the work environment. Three main organisations have to be mentioned.

a. ILO

Due to the need to develop data protection principles that specifically address the use of workers' personal data, the ILO published a Code of Practice concerning the protection of workers' personal data adopted in a Meeting of Experts on Workers' Privacy of the ILO in 1996.[66] The Preamble of the Code points out that the purpose is to provide guidance on the protection of workers' personal data. The instrument was not adopted as a Convention or Recommendation. It is not designed to replace national laws, regulations, or international labour standards or other accepted standards, but should be used in the development of legislation, regulations, collective bargaining agreements, work regulations, policies and other practical measures.

b. EU

The EU made attempts to legislate in the area of employment data protection. Based on comparative work[67], the European Commission initiated the consultation process under the Treaty's social policy title with the social partners on this subject. The initiative, however, ultimately did not succeed.[68]

Under the (former) 1995 European Data Protection Directive, the European 'Data Protection Working Party'[69] adopted some guidance on data protection in the employment context. The Working Party adopted Opinion 8/2001 of 13 September 2001 on the processing of personal data in the employment context.[70] Another instrument is the EU Working Document of 29 May 2002 on workplace communications.[71] On 8 June 2017, the Working Party issued Opinion 2/2017 on data processing at work (WP Opinion 2/2017).[72] Under the GDPR and its new governance model, the Working Party was replaced by the 'European Data Protection Board'. The opinions of the Working Party nevertheless remain relevant and valid.

---

63 For the text: https://iapp.org/media/pdf/resource_center/Ibero-Am_standards.pdf.

64 Cf. https://ec.europa.eu/fpi/sites/fpi/files/ann8_international_digital_cooperation_personal_data_protection_and_flow.pdf.

65 https://repositorio.cepal.org/bitstream/handle/11362/44629/1/S1900395_en.pdf ; Lehuedé 2019, p. 58.

66 ILO 1997.

67 Freedland 1999, Hendrickx 2003 and Hendrickx 2002.

68 See https://ec.europa.eu/social/main.jsp?pager.offset=10&advSearchKey=data+protection&mode=advancedSubmit&catId=22&doc_submit=&policyArea=0&policyAreaSub=0&country=0&year=0.

69 The Working Party is an advisory group composed by representatives of the data protection authorities of the Member States, which acts independently and has the task, inter alia, of examining any question covering the application of the national measures adopted under the Data Protection Directive in order to contribute to the uniform application of such measures.

70 Opinion 8/2001 of 13 September 2001 on the processing of personal data in the employment context, 5062/01/EN/Final, WP 48, 28 p; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf.

71 Data Protection Working Party, *Working Document on the Surveillance of Electronic Communications in the Workplace*, May 29, 2002, 5401/01/EN/final, 35 p.

72 See: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

c. Council of Europe

The desirability of adapting these data protection principles to the particular requirements of the employment sector led to the adoption of Recommendation No. R(89)2 on the Protection of Personal Data Used for Employment Purposes. This Recommendation was adopted by the Committee of Ministers on 18 January 1989. On 1 April 2015, the Committee of Ministers adopted a new Recommendation on the processing of personal data in the employment context (CM/Rec(2015)5),[73] motivated due to changes in the employment context and new technologies.[74]

[73] https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a.
[74] See the preamble of Recommendation CM/Rec(2015)5.

3 Data protection principles

3.1. Introduction

As the world-wide growth of data protection regulation is unstoppable and a logical follow-up from technological evolutions and societal needs, it is clear that, mainly, regional data instruments attempt to give their respective responses. It has been indicated above, however, that with the creation of different regional instruments, mutual inspiration and benchmarking has taken place. This implies that, while the different instruments have their own language and choices, it is important to recognise and appreciate their global dimension and the common elements of data protection standards.

Only few studies have been conducted that compare and synthesise major data protection standards on a global scale. A leading study came in 2020 from the **Global Privacy Assembly**, a composition that groups data protection authorities world-wide (formerly known as International Conference of Data Protection and Privacy Commissioners - ICDPPC). The study produces a comparative inventory of the main and globally shared principles of data protection.[75] Ten regional or global standards were analysed, including, besides the assembly's own 'Madrid Resolution', the OECD Privacy Guidelines, the APEC Privacy Framework, the Council of Europe (CoE) Convention 108 and Convention 108+, the Standards for Personal Data Protection for Ibero-American States, the African Union Convention on Cyber Security and Personal Data Protection, the ECOWAS Act on Personal Data Protection, the EU data protection standards (GDPR) and the UN Guidelines for the Regulation of Computerized Personal Data Files. From the comparison of these instruments, the following global key-principles come out:[76]

1. **Fairness:** personal data should be processed fairly (with links to non-discrimination, transparency, absence of fraud).
2. **Legitimacy: (also known as lawfulness)** personal data should be processed for legitimate purposes, or should be processed lawfully.
3. **Purpose specification:** personal data should be processed only for specified, defined, explicit and legitimate purposes.
4. **Proportionality:** personal data should be processed taking into account general requirements of proportionality, data minimisation requirements, requirements of non-excessive processing, or requirements of relevance to purpose.
5. **Data quality:** personal data should be accurate, complete and up to date.
6. **Openness/transparency:** the inclusion of some degree of openness or transparency can be found in all frameworks. Degrees range from general requirements to have transparent policies, and to ensure information about personal data processing is made available, to specific lists of information that must be provided directly to data subjects.
7. **Security:** there should be appropriate (or sufficient) measures to secure personal data (processing).
8. **Data retention:** personal data should not be retained longer than what is necessary for the purposes of processing.

[75] Another interesting comparison departing from the African instruments: Greenleaf and Cottier 2020.

[76] Global Privacy Assembly, Policy Strategy Working Group 1: Global frameworks and standards, October 2020, https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

9. **Accountability:** (a slightly less generally shared principle, with six out of ten frameworks) requiring that data controllers (and where applicable, processors) are accountable for the personal data they process.
10. **Access:** data subjects have the right of access to their personal data and have these data rectified and/or deleted or erased, with (for some instruments) additional guarantees of objecting or contesting the data processing.

In this working paper, these general principles will be further discussed, but with some re-arrangement for reasons of logic and discussion. Some of the general data protection principles are strongly intertwined or form part of a wider cluster. Their relevance may also vary in light of arising issues in the employment relationship. Hereafter, the analysis will focus on all aforementioned principles, under the following headings:

1. Legitimacy
2. Proportionality
3. Purpose limitation
4. Transparency
5. Data quality
6. Access
7. Accountability and governance
8. Collective rights

Before doing so, however, it is proper to give a short reflection on the definitions and scope of data protection standards.

3.2. Definitions and scope

The **ILO Code of Practice** gives the following definitions:

> 3.1. The term "personal data" means any information related to an identified or identifiable worker.
>
> 3.2. The term "processing" includes the collection, storage, combination, communication or any other use of personal data.

a. Personal data

The definitions used make clear that the material scope of personal data protection is very broad, regardless of the used technology. Personal data can be considered to relate to computer files, data involving a person's name, image, address, professional status, family status, health information, education, career, income, behaviour, opinions, etc., displayed through paper based or electronically produced texts, images, and so on.

It does not matter whether personal data or sensitive or not, nor whether they are 'private' or 'public'. The CJEU has made clear, for example, that also data relating to activities of a *professional* nature are covered by the right to data protection.[77]

[77] CJEU, 9 November 2010, Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen,* para. 59.

b. Personal data processing

The different global instruments define 'processing' with some differences, but the concept of 'processing' of personal data is generally understood in a very broad sense. It may refer (cf. example article 4, 2 GDPR) to any operation or a set of operations, performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. This broad interpretation is significant for the employment context. Also the *collection* of personal data is thus covered by data protection standard. In principle, and certainly when automated or semi-automated means are applied, it is not required that personal data have to be stored and further processed after they have been collected, in order for the regulation to apply.

However, the scope of application remains often limited to automated or partly automated processing activities, or to processing activities which are purely manual but which (are destined to) form part of a filing system or are intended to form part of a filing system. Manual processing of personal data outside the scope of a filing system is then not covered. This is, for example, the regime of the GDPR, where following article 4, 6 GDPR, a filing system is "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis". Although this is a quite abstract definition and open for discussion, it may have practical results. For example, when a recruiter makes notes during a selection interview with a job applicant, these personal notes would not be covered by the GDPR when the notes are taken on paper and if the notes are not (meant to be) kept in a structured way. Would the notes be taken with a stylus pen on a tablet, or would the notes be scanned afterwards, the situation would be covered by the GDPR.

Other instruments make similar limitations to the scope of personal data protection. For example, in section 2 of **CoE Recommendation CM/Rec(2015)5**, where no automated processing is used, data processing means "the operations carried out within a structured set established according to any criteria which allows for the search of personal data". Nevertheless, the Council of Europe Convention nr. 108 limits, in principle, its scope of application to "automated personal data files and automatic processing of personal data-",[78] although it does not exclude member states to decide for a wider scope.[79] The **2013 OECD Guidelines** on data protection are not, in principle, limited to any technological intervention. The Guidelines are to be applied whenever their processing poses a danger to privacy and individual liberties. Automatic methods are only one of the problems raised in the Guidelines.[80]

c. Legal persons

A matter of discussion is whether the right to data protection can also be enjoyed by **a *legal* person** and not only by a *natural* person. According to the European Working Party Opinion 4/2007 only a human being is granted protection.[81] In its definition of personal data, article 4 GDPR also limits its scope to data concerning a natural person.

However, it could be questioned whether this limitation would follow from a fundamental rights logic. It is evident that also legal persons, including an organisation or a business, may enjoy fundamental rights, such as, for example, the right to collective bargaining or the freedom to conduct a business. This means that the right to data protection could also cover protection, for example, with regard to the processing of confidential information of a legal person. It would also imply that, in principle, trade unions may enjoy the right to personal data protection.

78 Article 3, 1 Convention 108.
79 Article 3, 2, c Convention 108.
80 *Cf.* Section 38 OECD Guidelines on data protection 2013.
81 Article 29 Working Party (2007), *Opinion 4/2007 on the concept of personal data*, WP 136, 20 June 2007, p. 22.

The Council of Europe's **Convention 108+** is open for the application of personal data protection to legal persons. In the Explanatory Report, it can be read that "the Parties may extend the protection in their domestic law to data relating to legal persons in order to protect their legitimate interests".[82] Also the **2013 OECD Guidelines** on data protection mention the possibility to apply data protection to legal persons, groups and similar entities, but leaves this to the member states due to a lack of consensus on the level of the OECD. The OECD explains that country experiences show "that it is difficult to define clearly the dividing line between personal and non-personal data. For example, data relating to a small company may also concern its owner or owners and provide personal information of a more or less sensitive nature. In such instances it may be advisable to extend to corporate entities the protection offered by rules relating primarily to personal data."[83] The **UN Guidelines** seem to go in a similar direction, indicating that "states can opt to extend all or part of the principles to files on legal persons, particularly when they contain some information on individuals".

3.3. Legitimacy

Personal data must be processed on a legitimate basis. In other words, personal data processing has to be justified on the basis of a legitimate ground, reason or purpose. A legitimate basis requires, above all, that it is lawful.

The **ILO Code of Practice** provides:

> 5.1. Personal data should be processed lawfully and fairly, and only for reasons directly relevant to the employment of the worker.

a. Principle

This principle of lawfulness or legitimacy stands central in data protection law and has been further specified in different data protection instruments around the globe.

Some will refer to this as a data collection limitation principle. As the **OECD Guidelines** (2013) put it:

> 7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

There is a similar reference in the **APEC Privacy Framework**. As will be shown below, it is connected with data quality and proportionality.

The principle of lawfulness is explicitly provided in some of the data protection standards, for example in the **GDPR** and in the **ECOWAS** data protection act. The evaluation of this legitimacy principle will be much dependent on the context and circumstances of data processing. However, it must be clear that the employment relationship is recognised as a legitimate basis for personal data processing under data protection law. Obviously, the link with the employment relationship should be established in a proper way.

However, while the contract may be a strong and legitimate basis for data processing, the instruments, such as the **GDPR**, show that employers who want to process personal data of employees, may ground the

[82] Explanatory Report, para. 30, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.
[83] The OECD Privacy Framework, 2013, p. 49, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

legitimacy of the processing on a wide variety of grounds. Under the GDPR's article 6, processing is considered to be lawful when necessary:

- for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- for compliance with a legal obligation to which the controller is subject;
- in order to protect the vital interests of the data subject or of another natural person;
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for the purposes of the legitimate interests pursued by the controller or by a third party.

Similar references can be found in the **ECOWAS Data Protection Act**. According to article 23 of this act, processing is legitimate when the processing is necessary:

- for performance of a contract to which the data subject is party or for the application of precontractual measures at their request;
- to comply with a legal obligation;
- for implementation of a public interest mission or relevant to the exercise of public authority vested in the controller;
- for safeguarding the interests or rights and fundamental liberties of the data subject.

The instruments show that personal data processing is not only legitimate when employers are required or obliged to process these data, based on legal obligations, but also in case where employers have a contractual or other "legitimate interest". Justifications may come from the employer's legitimate interests in areas such as: recruitment and selection; the exercise of his rights, such as the right to exercise authority and control, or to direct the enterprise and plan the work, under the employment contract; payroll, administration and human resources services; health and safety obligations and actions; diversity policies, and so on.

In the **APEC Framework**, this aspect is rather found in the principle on 'use of information', where reference is made to the condition that personal data should be collected:

- when necessary to provide a service or product requested by the individual;
- or by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.

This seems to be somewhat stricter than the GDPR or ECOWAS instrument. In the commentary to the **APEC Framework** provision, it is explained that "the use of personal information for 'compatible or related purposes' would extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner" and "the processing of employee payrolls by a third party."[84]

Also a public interest reason could be envisaged by an employer. It means that external circumstances to the business, such as for example a pandemic, might determine the necessity to collect some data from employees.

[84] Cf. Commentary to article 25 APEC Privacy Framework.

The **GDPR** gives a set of employment related purposes when referring to employment related data processing in article 88. It seems evident the explicit reference means that the European legislator considers these as legitimate purposes:

> The purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

Some countries have further specified the issue of legitimate or lawful processing for employment purposes.

The **Finnish** Act on the Protection of Privacy in Working Life has used an adapted wording for the employment relationship and provides that:

> The employer is only allowed to process personal data directly necessary for the employee's employment relationship, which is connected with managing the rights and obligations of the parties to the employment relationship or with the benefits provided by the employer for the employee or which arises from the special nature of the work concerned.[85]

This is the case in **Germany** where the legislator, making use of art. 88 GDPR, and through its Federal Data Protection Act (the "BDSG"), adopted specific rules regarding data processing for employment-related purposes. Employment-related processing of personal data has to follow the purposes set out in the BDSG. Besides some special cases, the processing of personal data can be justified on the following grounds:

- data processing is necessary for the decision on the establishment of an employment relationship or after the establishment of the employment relationship for its execution or termination or for the exercise or fulfilment of the rights and obligations of the representation of the interests of the employees resulting from a law or a collective bargaining agreement, a works agreement, or a service agreement;
- data processing is necessary to detect criminal offences (but only if there is document reason to do this);
- data processing necessary to comply with a works council agreement which conforms with art. 88 GDPR;
- data processing can be allowed, some cases, when it is based on the worker's consent.[86]

Another leading example is **France**, where the national data protection authority ("CNIL") has listed a number of legitimate purposes for data processing in the employment context:[87]

- Recruitment;
- Administrative management of personnel;
- Management of remuneration and completion of related administrative formalities;
- Provision of professional tools to staff;
- Organisation of work;
- Career and mobility monitoring;
- Training;

---

85 Section 3, Act on the Protection of Privacy in Working Life *(759/2004; amendments up to 347/2019 included),* https://www.finlex.fi/fi/laki/kaannokset/2004/en20040759.pdf.

86 Cf. also: DLA Piper, "Germany", in *Data Protection Laws of the World*, DLA Piper, 2020, p. 278.

87 Decision n ° 2019-160 of 21 November 2019 adopting a framework relating to the processing of personal data implemented for the purposes of personnel management (Guideline by CNIL) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041798580/.

- Keeping of compulsory registers, relations with employee representative bodies;
- Internal communication;
- Management of social assistance;
- Performing audits, managing litigation and pre-litigation.

These examples show that the requirement of legitimacy or lawfulness, in light of purposes related to the employment context, offers still quite open justifications for the processing of personal data, including not only the necessity for the employment contract but also "legitimate interests pursued by the controller". The **German** example shows that the concrete application of the legitimacy principle, laid down in legislative standards, will still rely on case law, from which a broader reasonableness test may result, allowing to see necessary processing also in light of the employers' economic business efficiency or for the application of IT policies.[88] Further below, this relevance is elaborated and examples are given in combining the legitimacy requirement with the proportionality principle, in order to assess which personal data can be seen as 'necessary' and thus can be lawfully processed in the employment context.

b. Non-discrimination

In light of legitimacy or lawfulness, the processing of personal data should also brought into connection with the principle of non-discrimination. It is clear that discriminatory motives, purposes or effects have to be rejected in light of the legitimacy principle.

The ILO Code of Practice provides:

> 5.10. The processing of personal data should not have the effect of unlawfully discriminating in employment or occupation.

The language of the ILO Code is particularly interesting, as it does not refer to discriminatory purposes as such, but to discriminatory 'effects'. This is particularly relevant in light of algorithmic decision-making instruments, such as in artificial intelligence, people analytics or in the gig economy, where software may be used, although with biased and even unintended discriminatory effects.

The issue of discrimination is also of key-importance the use of data analytics and algorithmic based data processing.[89]

c. Consent

A specific ground of justifying personal data processing is consent. It is widely referred to in data protection instruments. However, the freedom of consent is an important issue in data protection law. Consent is obviously only a valid ground if it is, or can be, given freely. In light of this, in the employment context, a major question exists on whether consent can be a legitimate ground for personal data processing. The **ILO Code of Practice** refers to "informed and explicit consent".

An instrument that has paid much important to the freedom of consent, with subsequent and additional guidance, is the GDPR. Article 4, 11 GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". The GDPR provides furthermore that, when assessing whether consent is given freely, utmost account shall be taken

---

88 German Expert Response.

89 Global Privacy Assembly Report, Policy Strategy Working Group 2, Digital Economy, October 2020, https://globalprivacyassembly.org/wp-content/uploads/2020/10/GPA-PSWG2_Digital_Economy_Working_Group_Report_public.pdf (p.15).

of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[90] Furthermore, the GDPR provides that data subjects have the right to withdraw their consent at any time.[91] The European Working Party has referred to the problematic nature of freedom of consent in employment relationships and is of the opinion that, "unless in exceptional situations, employers will have to rely on another legal ground than consent – such as the necessity to process the data for their legitimate interest".[92] It furthermore states that default settings on devices or the application of software cannot qualify as consent, as consent would require an "active expression of will".[93] This is not a purely European approach. The Data Protection Authority of the **Philippines**, for example, extensively referred to the EU Working Party in taking a similar position on consent.[94]

The **APEC Privacy Framework** refers to this matter as a dimension of "choice". In the commentary to its article 26, it provides that "in certain situations, it would not be practicable for employers to provide a mechanism to exercise choice related to the use of the personal information of their employees when using such information for employment purposes. For example, if an organisation has decided to centralize human resources information, that organisation should not be required to provide a mechanism to exercise choice to its employees before engaging in such an activity".[95] The issue of consent also becomes increasingly relevant in African legal systems, where default consent is becoming less apparent compared to 'opt-in' consent.[96] In the **African ECOWAS Act**, consent is defined as a manifestation of specific, unequivocal, free, informed and express will of a data subject.[97]

Examples can also be found in **Germany**, which needs to fit within the GDPR approach. The German Federal Data Protection Act (BDSG) seems to assess the freedom of choice in light of the circumstances. For example, there may be an opening for free choice, for example, if a legal or economic advantage is obtained for the employee or if the employer and the employee pursue similar interests.[98] Examples may be supplementary services, such as in car policies or IT policies, birthday lists, and so on.[99]

The data protection authority ("CNIL") of **France** has considered the possibility of consent also in a very limited way. The CNIL clarified that in the phase of recruitment, job applicants cannot be considered to be free to give their consent to the processing of personal data. However, on the other hand, the CNIL is of the opinion that consent can be lawfully given by employees, for example, for appearing in a promotional video-clip of the business, but still only on the condition that the choice is real and refusal does not have negative effects on the employee's working conditions.[100] Also for the legal system of **Senegal**, it has been reported that for the online publication of a worker's photograph, consent is not only possible, but also required.[101]

The **2015 Council of Europe Recommendation** gives less indication to the overall issue of consent.[102] **CoE Convention 108+** refers to "free, specific, informed and unambiguous consent" (art. 5.2.) while the **African** instruments refer to the need for consent to be 'specific, unequivocal, free, informed and express'.[103]

90 Article 7, 4 GDPR.
91 Article 7, 3 GDPR.
92 WP Opinion 2/2017, 4.
93 WP Opinion 2/2017, 7.
94 https://www.privacy.gov.ph/wp-content/files/attachments/advopn/2019/AdOps_2019-034.pdf.
95 Commentary to article 26, APEC Privacy Framework.
96 https://www.jdsupra.com/legalnews/recent-developments-in-african-data-7141556/
97 http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf.
98 In addition in principle a written form requirement exists for the consent § 26 (2) sentence 3 BDSG and an obligation to inform about the right of revocation (Article. 7 (3) GDPR) in accordance to § 26 (2) sentence 4 BDSG.
99 DLA Piper, "Germany", in *Data Protection Laws of the World*, DLA Piper, 2020, p. 278.
100 Commission nationale de l'informatique et des libertés Délibération no 2019-160 du 21 novembre 2019 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en oeuvre aux fins de gestion du personnel, CNIL2009233X, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041798580/
101 Boshe 2016, p. 263.
102 Section 9.3. CoE Recommendation 2015.
103 See the African instruments on data protection.

The limited possibilities to obtain an employee's consent for personal data protection stand in contrast with the wide range of legitimate grounds for employers to process personal data. The issue of consent may become more relevant in cases where data protection laws do not explicitly refer to general employment relevant legitimate purposes of data processing, which is for example the case in **Japan**.[104] Consent may be relevant as additional safeguard, for example as a condition to communicate personal data to third parties, as is illustrated in the system of **Mozambique**.[105]

3.4. Proportionality

a. Principle

Conditions of relevancy, adequacy, necessity, or proportionality of data processing are all related to the additional requirements and limitations of data processing, beyond lawfulness or legitimacy.

Proportionality would seem the most general and over-arching of those principles. It allows to understand the term 'necessary' and to distinguish it from 'legitimacy', since the legitimacy principle is also referring to necessity, such as in "necessary for the performance of a contract" (cf. (art.6,1,b) **GDPR**). While the lawfulness or legitimacy criteria refer to grounds, reasons or purposes of data processing, the requirements of relevance, adequacy and so on, would rather point at the relationship of the personal data that are collected and processed, with those purposes. As necessity should be evaluated in light of the aim pursued,[106] the processing has to remain proportionate to the legitimate purposes.[107] In the words of the European Working Party: "Regardless of the legal basis for such processing, a proportionality test should be undertaken prior to its commencement to consider whether the processing is necessary to achieve a legitimate purpose".[108] As the **OECD's Explanation** to the Guidelines phrases it: "The requirements in this respect are linked to the purposes of data, i.e. they are not intended to be more far-reaching than is necessary for the purposes for which the data are used".[109] It requires a rather careful, judicious and prudent use of data in light of the pursued purposes.

This proportionality principle is explicitly mentioned as a principle in **CoE Convention 108+** and in the **Ibero-American Standards for Personal Data Protection** the 18th principle. In some instruments, proportionality is seen to be included in the principle of "data quality", such as in the **OECD Guidelines** (2013). But all instruments use one or more of the principles of relevance, adequacy, non-excessiveness, and so on. The **CoE Recommendation** (2015), relating to employment, provides:

> 5.2. Personal data collected by employers for employment purposes should be relevant and not excessive, bearing in mind the type of the employment as well as the changing information needs of the employer.

The principle of proportionality is inherent to human rights protection mechanisms. While different approaches of proportionality could be envisaged, three main explanations are broadly accepted as constituting a test of proportionality in the context of data protection law:[110]

- Suitability (or adequacy): is the data processing suitable or relevant to realising the legitimate goals?
- Necessity: is the data processing required for realising the legitimate goals? Such necessity requirement may be connected to an alternative means test: are there alternative means to realise the legitimate goals.

104 Expert Response Japan.
105 Traça and Neves 2016, pp. 365-366.
106 Section 4.1 CoE Rec 2015.
107 WP Opinion 2/2017, 7.
108 WP Opinion 2/2017, 4.
109 Explanation 53, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum.
110 Lee A. Bygrave, "Core principles of data privacy law", in Bygrave 2014, p. 148.

– Non-excessiveness: does the measure go further than is necessary to realise the legitimate goals?

Proportionality plays also a role in the area of electronic monitoring. The European Working Party has explained the relevance of this in its **Opinion 2/2017**: "monitoring every online activity of the employees is a disproportionate response and an interference with the right to secrecy of communications. The employer should first investigate other, less invasive, means to protect the confidentiality of customer data and the security of the network".[111] The **Philippines** Data Protection Advisory Opinion (No. 2018-048) on monitoring of employees requires "an assessment of the necessity and proportionality of the monitoring", and recommends that "less privacy-intrusive means of monitoring should be considered rather than excessive and disproportionate mechanisms".[112] In the case of Barbulescu, however, the ECtHR "considers that proportionality and procedural guarantees against arbitrariness are essential".[113]

b. Data minimisation

A new notion connected with proportionality in data protection law is data minimisation.

The **Ibero-American Standards for Personal Data Protection**'s 18th principle, referring to proportionality, demands that personal data should be "appropriate, pertinent and limited to the minimum necessary for the purpose." The **CoE Recommendation** (2015) provides:

> 4.1. Employers should minimise the processing of personal data to only the data necessary to the aim pursued in the individual cases concerned.

The principle is also recognised in article 5, 1, c **GDPR**, providing that the processing of personal data should be:

> "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')"

The application of this principle is relevant for different employment context issues. It may, for example, be particularly relevant in the context of electronic monitoring. Data protection instruments usually do not offer a straightforward answer to the question of whether and, if so, to what extent, employers may monitor workers in the workplace. But excessive monitoring is usually ruled out.

In light of this, the ILO Code of Practice provides that "continuous monitoring should be permitted only if required for health and safety or the protection of property" (section 6.14, 3).

c. Necessary data

Both the open grounds of lawfulness and legitimate purposes of data processing (under the 'legitimacy principle') and the proportionality or necessity test in light of these purposes, do not take away that a wide series of personal data can be processed in the context of employment.

The European Working Party, in its **Opinion 8/2001** mentioned the following data as possible relevant data in the employment context[114]: application forms and work references; payroll and tax information-tax and social benefits information; sickness records; annual leave records; unpaid leave/special leave records; annual appraisal/assessment records; records relating to promoting, transfer; training, disciplinary matters;

---

111 Working Party Opinion 2/2017 on data processing at work, p. 13.

112 SyCip Salazar Hernandez & Gatmaitan, *Data Privacy: NPC Addresses Return-to-Work and WFH Questions*, 8 June 2020, https://www.lexology.com/library/detail.aspx?g=0ea8d164-011f-48aa-9003-d629eab6efdc

113 *Barbulescu*, ECtHR (Grand Chamber) judgement of 5 September 2017, §121.

114 Working Party, Opinion 08/2001 on the processing of personal data in the employment context, WP 48, 13 September 2001, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2001/wp48_en.pdf.

records relating to accident at work; information generated by computer systems; attendance records; family members; reimbursement of expenses, e.g. travel.

The need to collect and further process personal data in the employment relationship, and the establishing of all kinds of employee records, is followed in different systems. In **Australia** the Fair Work Act 2009 and Fair Work Regulations 2009 require employers to maintain records of various matters, including identification, employment and wage data.[115] In the **Philippines**, the necessity for employment related purposes may include data on careers, human resource management functions, or all information needed to comply with statutory and regulatory requirements of government agencies.[116]

Some jurisdictions apply a broader reasonableness test. For example in **Japan**, employers can collect personal information (including their credit records and background checks) to a reasonable extent. Only when it comes to sensitive information (such as criminal records), consent has to be given.[117] In **Singapore**, based on the Personal Data Protection Act 2012, the processing of personal data of employees can be legitimate if it is reasonable for the purpose of "managing or terminating an employment relationship". Examples of this are: bank account details (salary administration); monitoring of the use of the computer network resources; posting photographs in the staff directory intranet; or managing staff benefit and training schemes.[118]

d. Essence of a right

Related to proportionality is the idea that data protection cannot lead to such a limitation of the right to data protection, that it would compromise the essence of that right. One could also translate this into the idea that workplace privacy cannot be reduced to 'zero', which should not be seen as incongruent with reasonable privacy expectations or with notice or consent requirements in case of monitoring.[119]

The idea that an individual cannot lose the enjoyment of the essence of a right can also be connected to the limitations on individual (or collective) consent as a ground or technique to process personal data. The ILO's reference is interesting in this regard. The **ILO Code of Practice** mentions:

> 5.13. Workers may not waive their privacy rights.

In the Commentary to section 5.13 the ILO Code it is pointed out that "in view of the dependence of workers on their employment and the fundamental nature of privacy rights, the code states that workers may not waive their privacy rights. It is, nevertheless, recognized that privacy rights are not absolute and are balanced with competing public interests according to national law."

While the waiver of rights has to be addressed in a nuanced way,[120] restrictions to applying it have to be seen in light of the proportionality principle, as well against the background of the issue of free consent in employment relationships. Some legal systems have opted expressly to make waivers in the employment context legally impossible. For example in **Brazil**, under the Data Protection Act, employment contracts clauses that provide for a waiver by the worker of the right to clear, accurate and easily accessible information on the processing of personal data relating to it, are considered to be null and void.[121]

115 Expert Response Australia.
116 Republic of the Philippines NATIONAL PRIVACY COMMISSION, PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2017-50; https://www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-050.pdf.
117 https://www.lexology.com/library/detail.aspx?g=e4dd9d42-2235-40d2-b306-8aea9da92f03.
118 https://www.lexology.com/library/detail.aspx?g=b80f3cd9-6f19-4e14-ad75-6d8896f8a5e7.
119 Mangan 2019, p. 568.
120 Purtova 2017.
121 Expert Response Brazil.

3.5. Purpose limitation

a. Principle

The purpose limitation principle is a widely recognised principle of data protection. This general requirement comes back in most data protection instruments. The different international data protection standards share the rule that personal data should be processed for specific (or specified), explicit, legitimate (or lawful) purposes. Furthermore, personal data should not be further processed in a manner incompatible with those purposes.

Some data protection standards give more detailed obligations such as the **OECD Guidelines** (2013) providing that:

> 9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

The **ILO Code of Practice** provides:

> 5.2. Personal data should, in principle, be used only for the purposes for which they were originally collected.
>
> 5.3. If personal data are to be processed for purposes other than those for which they were collected, the employer should ensure that they are not used in a manner incompatible with the original purpose, and should take the necessary measures to avoid any misinterpretations caused by a change of context.

This important data protection principle is related to verifiability and transparency of personal data processing. It also contributes to the fairness of data processing. The principle not only requires that the original purpose of data collection needs to be legitimate and clear, but also that subsequent data processing activities remain compatible with the original purposes. It means that 're-purposing' is, in principle possible, but this should be compatible with the original purpose of collection.

Part of the respect of secondary (re-purposed) use of personal data of workers can be the respect for transparency and information to the worker concerned. For example, the **CoE Recommendation** (2015) provides:

> 6.3. Under exceptional circumstances, where data are to be processed for employment purposes other than the purpose for which they were originally collected, employers should take adequate measures to avoid misuse of the data for this different purpose and inform the employee. Where important decisions affecting the employee are to be taken, based on the processing of that data, the employee should be informed accordingly.

b. Specifications

The purpose limitation is often illustrated in cases of monitoring or evaluation of workers. In this context, the **ILO Code of Practice** provides:

> 5.4. Personal data collected in connection with technical or organizational measures to ensure the security and proper operation of automated information systems should not be used to control the behaviour of workers.

The European Working Party, in **Opinion 2/2017**, gives the example of mobile device management systems, allowing employers to locate devices remotely (including the workers using them). As they enable employers to record real-time activities, including working time, and allow them to pursue security purposes, employers must "ensure that the data collected as part of this remote location capability is processed

for a specified purpose and does not, and could not, form part of a wider programme enabling ongoing monitoring of employees."[122]

3.6. Transparency

a. Principle

According to article 8 CFREU, everyone has the right to fair personal data processing. Fairness can be seen broadly and interpreted in many ways. It is certainly connected with the question of legitimacy and with the purpose-limitation principle.

Fairness also implies transparency. This is made clear in the Council of Europe's 2015 Recommendation which brings transparency of processing in direct relation with the need to guarantee a fair processing.[123]

The **OECD Guidelines** (2013) provide that:

> 12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
>
> 13. Individuals should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;

The **ILO Code of Practice** provides:

> 11.1. Workers should have the right to be regularly notified of the personal data held about them and the processing of that personal data.
>
> 6.2. If it is necessary to collect personal data from third parties, the worker should be informed in advance, and give explicit consent. The employer should indicate the purposes of the processing, the sources and means the employer intends to use, as well as the type of data to be gathered, and the consequences, if any, of refusing consent.

The commentary to this article in the ILO Code mentions that:

> Workers will want to know what happens to their data only if they have at least a rough idea of the kind of data collected, the purposes for doing so and the potential users.

The CoE **Recommendation (2015)** provides that "persons concerned should be properly and periodically informed in application of a clear privacy policy" (section 14.1).

b. Specifications

In data protection law, this principle is also brought in connection with monitoring and surveillance.

---

122 Working Party, Opinion 2/2017 on data processing at work, p.17.
123 Section 10.1. CoE Recommendation 2015.

The **ILO Code** requires that, in case of electronic monitoring, workers should be *informed in advance* of various aspects of the monitoring (section 6.14,1). This is strongly connected to the need to give prior notice of monitoring and the assessment of reasonable privacy expectations.

> The principle of prior notice is found in almost all studied legal systems although the manner in which notification is required may still differ. Some countries will refer to the need for having clear policies at company level, others explicitly require prior and/or written notification. Relying on comparative information, the **European** Court on Human Rights (ECtHR), in its *Barbulescu*-judgement, requires 'prior notice' in case of electronic monitoring, meaning that "the warning from the employer must be given before the monitoring activities are initiated, especially where they also entail accessing the contents of employees' communications".[124] In the comparative outlook in this judgement, it is reported that "with regard to monitoring powers, thirty-four **Council of Europe** member States require employers to give employees prior notice of monitoring".[125] In **Hungary**, for example, the Labour Code (2019) provides that employers are allowed to monitor the behaviour of workers with the use technical means, but he must notify the workers in advance and in writing.[126]

In the GDPR, transparency requirements are provided for in articles 13 to 15, granting data subjects the right to be informed about whether personal data regarding him or her are being collected and the identity of the controller, the purposes, whether data are being transferred to recipients and so on. According to the **European** Working Party, it means that workers "*must be informed of the existence of any monitoring, the purposes for which personal data are to be processed and any other information necessary to guarantee fair processing*".[127]

3.7. Data quality

Data quality is a concept that may be conceived in different ways. According to the **European Data Protection Supervisor**, data quality refers to a set of principles, including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.[128] For the purpose of discussing principles in relation to the employment context, the data quality is limited hereafter as including *accuracy* and *storage limitation*, as the other principles have been taken separately, taking into account the manner in which the studied international data protection standards are structured. These two elements are recognized as principles in the main international data protection instruments.

Also the **ILO Code of Practice** encompasses the principles of accuracy and storage limitation:

> 8.4. Employers should verify periodically that the personal data stored is accurate, up to date and complete.
>
> 8.5. Personal data should be stored only for so long as it is justified by the specific purposes for which they have been collected unless:
>
> (a) a worker wishes to be on a list of potential job candidates for a specific period;
>
> (b) the personal data are required to be kept by national legislation; or
>
> (c) the personal data are required by an employer or a worker for any legal proceedings to prove any matter to do with an existing or former employment relationship.

---

124 *Barbulescu*, ECtHR 5 September 2017, Grand Chamber, para. 133.
125 *Barbulescu*, ECtHR 5 September 2017, Grand Chamber, para. 53.
126 Expert Response Hungary.
127 WP Opinion 2/2017, 8.
128 https://edps.europa.eu/data-protection/data-protection/glossary/d_en.

a. Accuracy

It is obvious that accuracy of personal data in an employment or business context should be correct. This is strongly intertwined with the rights, obligations and liabilities under employment laws, including the identification of workers, the registration of performed working hours, the calculation of pay and determination of other benefits, social security and tax obligations, keeping information on training, and so on.

Three additional remarks have to be made in light of accuracy, seen the specificity of the employment context.

The first concerns the accuracy of evaluation data. The European Data Protection Supervisor has indicated that "*information intended to evaluate staff consists largely of subjective judgments of their professional performance. It is therefore difficult to assess the accuracy of such information*".[129] Staff evaluation data may, however, also contain objective elements. But this will be more relevant for the data subject's right to access and rectification, as explained below.

A second remark concerns the increasing importance of data quality in light of the use of artificial intelligence and algorithms. For example, it is clear that the accuracy of personal data, and their further processing, will play an important role in avoiding or regulating undesired outcomes, oversimplification, or discriminatory effects of algorithmic programmes.

A third aspect, related to accuracy, concerns the so-called 'right to lie'. The **ILO Code of Practice** provides that "if a worker is asked questions that are inconsistent with the main principles of the Code, and the worker gives an inaccurate or incomplete answer, the worker should not be subject to termination of the employment relationship or any other disciplinary measure". In its commentary, the ILO Code explains:

> (6.8) Although workers are expected to provide truthful information, the code shares the view of many national courts that, especially in connection with hiring procedures, workers are justified in refusing to answer questions that are incompatible with the code. In such cases, the employer bears the responsibility for incomplete or inaccurate responses and, consequently, is not entitled to impose sanctions. Moreover, the employer should not profit from a misunderstanding on the part of the worker as to what is being asked if the worker provides additional or irrelevant information (6.9).

There are different signs that this is still a controversial point. Providing untruthful information, or providing no information, can be a problematic issue, both under contract law as under employment law, often departing from mutual information duties and good faith obligations. Nevertheless, there are nuances. Scholarship has paid some attention to it. For example, a "defensive" (permissible) right has been described and grounded, as a way to avoid an (impermissible) serious wrongdoing.[130] Similarly, the use of the right to lie of a job applicant has been legitimised 'a shield' in response to discriminatory questions of an employer in the recruitment phase.[131] According to other research, in the **French** legal system there is a right to lie, or to remain silent, under certain conditions. This is for example the case when job applicants are asked to respond to questions concerning their health status (which is information to be gathered by the occupational physician).[132]

b. Storage limitation

The principle that personal data should not be kept or stored longer than necessary is connected to the data quality principle, but it can also be clustered within the proportionality principle. The 'storage limitation'

---

129 https://edps.europa.eu/data-protection/data-protection/reference-library/evaluation-staff_en.
130 Stewart 2019.
131 Hendrickx 1999.
132 Fantoni-Quinton and Laflamme 2017.

principle covers the idea that personal data need to be – and have to remain – relevant and cannot be processed for "longer than is necessary", seen the purposes for which the personal data are processed (cf. article 5, 1, e GDPR).

In addition to the ILO references, mentioned above, the **CoE Recommendation** (2015) establishes some further guidance for the employment relationship:

> 13.2. Personal data submitted in support of a job application should normally be deleted as soon as it becomes clear that an offer of employment will not be made or is not accepted by the job applicant. Where such data are stored with a view to a further job opportunity, the data subject should be informed accordingly and the data should be deleted if he or she so requests.
>
> 13.3. Where it is essential to store data submitted for a job application for the purpose of bringing or defending legal actions or any other legitimate purpose, the data should be stored only for the period necessary for the fulfilment of such purpose.
>
> 13.4. Personal data processed for the purpose of an internal investigation carried out by employers which has not led to the adoption of negative measures in relation to any employee should be deleted after a reasonable period, without prejudice to the employee's right of access until such deletion takes place.

Storage limitation has, according to the European Working Party **Opinion 2/2017** an effect on recruitment related personal data. According to the Working Party, "data collected during the recruitment process should generally be deleted as soon as it becomes clear that an offer of employment will not be made or is not accepted by the individual concerned".[133] A case in **New Zealand** has pointed out that personal data relating to (unsuccessful) job applicants cannot be kept indefinitely for future recruitment purposes.[134] Some countries have specific limits for the retention of data. For example, in **Bulgaria**, personal data of job applicants may not be kept longer than six months, unless the candidate would agree with a longer storage period.[135]

3.8. Access

All major data protection instruments provide that everyone has the right of access to personal data (concerning him or her) and the right to have the data rectified. Under these principles, a set of additional data protection rights for data subjects are provided in nearly all frameworks:

- **Access**: the right to obtain access to personal data is universally acknowledged;
- **Rectification**: often a follow up right of the right to access and recognized in all data protection instruments;
- **Deletion/erasure**: strongly connected to access and rectification and is also a universally accepted right;
- **Data portability**: much less generally recognized. It appears in the Ibero-American Standards and the GDPR.

a. Access

The right to have access to personal data will inevitably play a role in the employment context, seen the number of data and records kept for reasons of personnel administration, HR and other purposes.

---

133 Working Party, Opinion 2/2017 on data processing at work, 11.
134 Expert Response New Zealand.
135 DLA Piper, « Bulgaria », in *Data Protection Laws of the World*, DLA Piper, 2020, pp. 115-116.

According to the **ILO Code of Practice**:

> 11.2. Workers should have access to all their personal data, irrespective of whether the personal data are processed by automated systems or are kept in a particular manual file regarding the individual worker or in any other file which includes workers' personal data.

The right to have access to personal data processing may, additionally, involve a right to receive a copy of the personal data undergoing processing.[136]

According to the **ILO Code of Practice**:

> 11.3. The workers' right to know about the processing of their personal data should include the right to examine and obtain a copy of any records to the extent that the data contained in the record includes that worker's personal data.

The **ILO Code of Practice** provides for additional guarantees:

> 11.4. Workers should have the right of access to their personal data during normal working hours. If access cannot be arranged during normal working hours, other arrangements should be made that take into account the interests of the worker and the employer.
>
> 11.5. Workers should be entitled to designate a workers' representative or a coworker of their choice to assist them in the exercise of their right of access.
>
> 11.6. Workers should have the right to have access to medical data concerning them through a medical professional of their choice.
>
> 11.7. Employers should not charge workers for granting access to or copying their own records.

Most data protection instruments would allow for some limits towards the right to have access, or would accept conditions or a rule of reasonableness in applying the right. In some legal systems, this may be more specified for the employment context. From the data protection system in **Australia**, a number of relevant limitations can be reported, such as reasons relating to public health or safety; access would have an unreasonable impact on the privacy of another person; the request to access is frivolous or vexatious; reasons related to law enforcement or legal action; the information is commercially sensitive; or granting the request would be unlawful.[137]

b. Rectification

Data subjects have generally the right to obtain the rectification of inaccurate personal data concerning them. This also has a logical relevance for the employment context. However, some discussions may arise, certainly with regard to whether data are complete or whether evaluation data can be rectified.

The **ILO Code of Practice** provides:

> 11.9. Workers should have the right to demand that incorrect or incomplete personal data, and personal data processed inconsistently with the provisions of this code, be deleted or rectified.
>
> 11.10. In case of a deletion or rectification of personal data, employers should inform all parties who have been previously provided with the inaccurate or incomplete personal data of the corrections made, unless the worker agrees that this is not necessary.

[136] Cf. article 15, 3 GDPR.
[137] Expert Response Australia.

> 11.11. If the employer refuses to correct the personal data, the worker should be entitled to place a statement on or with the record setting out the reasons for that worker's disagreement. Any subsequent use of the personal data should include the information that the personal data are disputed, and the worker's statement.

The ILO's principle that the worker should be entitled to put a statement in the relevant record, with an indication of the worker's disagreement with the personal data, finds support in article 16 of the GDPR, which guarantees "the right to have incomplete personal data completed, including by means of providing a supplementary statement".

c. Evaluation data

A point of discussion relates to evaluation data. One may understand the issue in terms of worker evaluations made by employers or supervisors, or test results, are often kept in personnel files.

The international data protection standards do not seem to give a direct answer on how to treat evaluation data, while different *national* laws do qualify opinions as personal data.[138] The question is whether a person's opinion (e.g. an assessment) concerning another individual can be seen as personal data, and whose personal data.

The **ILO Code of Practice** is rather clear and straightforward and refers to "judgmental" data under its personal data protection principles for workers:

> 11.12. In the case of judgmental personal data, if deletion or rectification is not possible, workers should have the right to supplement the stored personal data by a statement expressing their own view. The statement should be included in all communications of the personal data, unless the worker agrees that this is not necessary.

The **CoE Recommendation** (2015) provides:

> 11.3. The right of access should also be guaranteed in respect of evaluation data, including where such data relate to assessments of the performance, productivity or capability of the employee when the assessment process has been completed at the latest, without prejudice to the right of defense of employers or third parties involved. Although such data cannot be corrected by the employee, purely subjective assessments should be open to challenge in accordance with domestic law.

Under the data protection law of **New Zealand**, an employer can decide not to give access to information that would unjustifiably reveal private information about another person. This can be e.g. when information is protected under legal professional privilege or when evaluations are obtained under a promise of confidentiality (e.g. job references, external referees for a promotion etc.).[139] Also the data protection authority of the **Philippines** approves access to worker performance evaluation, but refers to the possibility for employers to provide a summary of ratings without identifying the source in order to uphold the duty of confidentiality.[140] A possible limitation might also be that, in an HR context, evaluations may imply information of other employees (colleagues) who have a right and interest of not having their information disclosed.

In the case of *Nowak v. Data Protection Commissioner,* the **European Court of Justice** (CJEU) was of the opinion that the comments of an examiner with respect to a candidate's answers, no less than the answers

---

138 Cf. Bygrave 2014, p. 134.

139 Privacy Commissioner, *Privacy at work. A guide to the Privacy Act for employers and employees,* 2008, https://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-at-Work-2008.pdf, 19.

140 Republic of the Philippines, National Privacy Commission, Privacy Policy Office Advisory Opinion No. 2018-042; https://www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/AONo_2018-042.pdf.

submitted by the candidate at the examination, constitute information relating to that candidate.[141] Seen the fact that those comments are liable to have effects for the candidate, a right of access to these data may be exercised. The Court recognises that this does not imply a right to change the exam answers afterwards, but the right to access enables the data subject to obtain, depending on the circumstances, rectification (e.g. material mistakes by the examination authority), erasure or blocking of the data (e.g. when communication to third parties is intended).

d. Erasure

The right to erasure implies the right to have data removed. This could mean different things in an employment context. It could imply that some data have to be partly removed, so that another and more proper picture is given of the available information.

Closely connected with the right to access and rectification is the 'right to be forgotten'. This right was recognised, though in a specific context, by the European Court of Justice (CJEU) in the widely known *Google*-case, with reference to article 8 CFREU.[142] Under the right to erasure,[143] a data subject should have a right to be forgotten "where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed".[144]

This right to erasure and to be forgotten could be explored as a right for employees to demand that information about their past employment would not be brought under wide (public) attention after a certain period of time, as was illustrated by the ECtHR in the case of *Sõro v. Estonia.* However, the EU Working Party is of the opinion that a distinction between private and professional life has to be made and suggests that professional life exposure is less problematic.[145]

e. Data portability

Data portability refers to the right to receive personal data from a data controller and/or to transfer those data to another controller. It has become relevant with the rise of information networks and the network economy, where not only networks of enterprises, people and services are strongly interconnected.[146]

Notwithstanding its growing relevance, the principle of data portability has not yet been expressed in specific terms in many international data protection standards. Only the **Ibero-American Standards** and the **GDPR** appear to explicitly include it. However, the approach of the **Declaration of Principles of Freedom of Expression and Access to Information in Africa (2019)** is also interesting in this respect, stressing the informational autonomy of data subjects:

> Principle 42. 4. Every person shall have the right to exercise autonomy in relation to their personal information by law and to obtain and reuse their personal information, across multiple services, by moving, copying or transferring it.

141 CJEU, Judgement of 20 December 2017, No. C-434/16, *Nowak v Data Protection Commissioner*, ECLI:EU:C:2017:994.
142 CJEU (GC), 13 May 2014, No. C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD).*
143 Article 17, 1 GDPR.
144 GDPR, Preamble 65.
145 Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on *Google Spain and Inc v. Agencia Espanõla de Protección de Datos (AEPD) and Mario Costeja González* C-131/12, adopted on 26 November 2014, 16 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf - consulted 20 November 2017).
146 Shapiro and Varian 1998.

The GDPR (article 20(1)) states that:

> "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided".

Data portability may for example be relevant in cases of evaluation data, which could be relevant for new employment positions that workers take up with other employers. It may also be relevant specifically in the context of the gig economy and platform work, where workers have an interest in moving rating and ranking systems from one platform to another.[147]

3.9. Accountability and governance

a. Principle

Not all international data protection standards refer to the accountability principle, although a majority do so in one way or another. The accountability principle can be widened as a data protection governance principle, in order to group a number or a set of connected data protection principles.

The **Ibero-American Standards**, **CoE Convention 108+** and the **GDPR** provide, for example, obligations with regard to the data protection officers, training or audits in the accountability principles.

The GDPR provides that data controllers must be held responsible and demonstrate compliance for living up to standards on lawfulness of data protection (cf. art. 5.2 GDPR). The accountability principle is also brought forward in the **OECD Guidelines** (2013):

> 14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

However, accountability should not be understood in a too narrow sense. An interesting concept added to accountability is that of "privacy management", explicitly referred to in the **OECD Guidelines** (2013):

> 15. A data controller should: a) have in place a privacy management programme.

The idea is that data controllers must give effect to data protection principles and provide for appropriate safeguards based on privacy risk assessment, ongoing monitoring and periodic assessment. A broader notion of data protection governance can be construed. Data controllers and other involved parties thus bear a wider responsibility which requires them to be accountable, to provide for sufficient security measures related to data processing activities, as well as to manage and regularly assess data processing activities.

b. Security

The **OECD Guidelines** (2015) refer to the "security safeguards principle":

> 11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

---

147 Uni Global Union, Top 10 Principles for Workers' Data Privacy and Protection, (cf. point 1.c.), http://www.thefutureworldofwork.org/media/35421/uni_workers_data_protection.pdf?utm_campaign=revue_fortnightly_newsletter&utm_.

c. Specifications

The following references in the **ILO Code of Practice** could be seen in relation to this:

> 5.7. Employers should regularly assess their data processing practices: (a) to reduce as far as possible the kind and amount of personal data collected; and (b) to improve ways of protecting the privacy of workers.
>
> 5.9. Persons who process personal data should be regularly trained to ensure an understanding of the data collection process and their role in the application of the principles in this code.
>
> 7.1. Employers should ensure that personal data are protected by such security safeguards as are reasonable in the circumstances to guard against loss and unauthorized access, use, modification or disclosure.

Also the **CoE Recommendation** (2015) provides a number of aspects of this broader principle:

> 4.2. Employers should develop appropriate measures, to ensure that they respect in practice the principles and obligations relating to data processing for employment purposes. At the request of the supervisory authority, employers should be able to demonstrate their compliance with such principles and obligations. These measures should be adapted to the volume and nature of the data processed, the type of activities being undertaken, and should also take into account possible implications for fundamental rights and freedoms of employees.
>
> 20.1. Employers or, where applicable, processors, should carry out a risk analysis of the potential impact of any intended data-processing on the employees' rights and fundamental freedoms and design data processing operations in such a way as to prevent or at least minimise the risk of interference with those rights and fundamental freedoms.
>
> 20.2. Unless domestic law or practice provides other appropriate safeguards, the agreement of employees' representatives should be sought before the introduction or adaptation of ICTs where the analysis reveals risks of interference with employees' rights and fundamental freedoms.

Part of the broader accountability and management principle is that not only the employer, but also other parties, either part of the larger organisational setting, or third parties, have respect for the data protection principles. As the **OECD Explanatory Memorandum** indicates, it is essential that not only data controllers but also those parties that processing data on behalf of the controller, including service organisations, are held accountable for respecting the principles of data protection, including confidentiality.[148]

Accountability is also a matter of the internal operations of a data controller, such as an employer. In an HR context, the treatment of personal data should involve the accountability of different involved actors. The principle is thus directed to a wide range of addressees.

The **CoE Recommendation** (2015) provides:

> 12.3. The personnel administration, as well as any other person engaged in the processing of the data, should be kept informed of such measures, of the need to respect them and of the need to maintain confidentiality about such measures as well.

The **ILO Code of Practice** provides:

> 5.12. All persons, including employers, workers' representatives, employment agencies and workers, who have access to personal data, should be bound to a rule of confidentiality consistent with the performance of their duties and the principles in this code.

[148] Cf. Explanatory Memorandum 62, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum.

> 13.1. If the employer uses employment agencies to recruit workers, the employer should request the employment agency to process personal data consistently with the provisions of this code.

d. Impact assessment

The data protection impact assessment (DPIA) has been promoted as an important component of some personal data protection instruments. It is often relate to data processing with 'high risk' impact. An example of 'high risk', according to the European Working Party's **Opinion 2/2017** is "a case of systematic and extensive evaluation of personal aspects related to natural persons based on automated processing".[149]

For example, the **Ibero-American Standards** mention that the person responsible shall perform an impact assessment prior to implementation of treatment of personal data that probably entails a data protection high risk. Article 35(1) of the **GDPR** provides that:

> Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

Such 'DPIA' may be relevant in the context of the employment relationship, for example in cases where employers are intending extensive monitoring of workers.[150]

An assessment of data protection practices is also mentioned in the **ILO Code of Practice**:

> 5.7. Employers should regularly assess their data processing practices: (a) to reduce as far as possible the kind and amount of personal data collected; and (b) to improve ways of protecting the privacy of workers.

e. Privacy by design and default

Privacy by design and by default are a specific approach in relation to accountability applied by the GDPR. Article 25.2 of the GDPR provides:

> The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

This means that data controllers have to be proactive and making continuous assessment of the privacy impact of technology.[151] Preamble 78 of the GDPR explains that it entails that appropriate technical and organisational measures are taken to ensure that the requirements of the GDPR are met: "the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations."[152]

---

149 Working Party, Opinion 2/2017 on data processing at work, p 8.
150 Long et al. 2020, p. 9.
151 Jasmontaite et al. 2018.
152 Preamble 78 GDPR.

These principles are clearly still put in general terms and will have to be translated to the own context of the data controller. There is not yet much guidance on the implementation of this principle through the case law of the European courts. However, the Google Spain case of the European Court of Justice (CJEU) has made clear that the principle will likely play a role in the application of algorithmic decision-making processes.[153] In rejecting that search engines or algorithms are value-neutral, the Court confirmed that systems like these should be designed in a privacy friendly way.[154]

An example in the employment context is, according to the European Working Party **Opinion 2/2017**, when an employer would issue (tracking) devices to workers, then "the most privacy friendly solutions should be selected if tracking technologies are involved".[155]

3.10. Collective rights

With regard to collective rights, the **ILO Code of Practice** provides:

> 12. Collective rights
>
> 12.1. All negotiations concerning the processing of workers' personal data should be guided and bound by the principles in this code that protect the individual worker's right to know and decide which personal data concerning that worker should be used, under which conditions, and for which purposes.
>
> 12.2. The workers' representatives, where they exist, and in conformity with national law and practice, should be informed and consulted:
>
> (a) concerning the introduction or modification of automated systems that process worker's personal data;
>
> (b) before the introduction of any electronic monitoring of workers' behaviour in the workplace;
>
> (c) about the purpose, contents and the manner of administering and interpreting any questionnaires and tests concerning the personal data of the workers.

In the employment context, a reference to collective rights may be relevant in different perspectives.

a. Regulation

As data protection laws are generally not designed for, although applicable to, the employment context, the creation of more specific and adapted rules or principles may be envisaged or desirable.

The **ILO Code of Practice** also hints at this:

> 5.11. Employers, workers and their representatives should cooperate in protecting personal data and in developing policies on workers' privacy consistent with the principles in this code.

The idea of adapting the principles to the employment context has been explicitly suggested by the European data protection legislator. Article 88 of the **GDPR** provides:

> 1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements,

153 Case C-131/12, *Google Spain v Agencia Española de Protección de Datos (AEPD)*, Judgement of 13 May 2014.
154 Bygrave 2017, p.11.
155 Working Party, Opinion 2/2017 on data processing at work, p8.

management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

On 24 June 2020, the **European Commission** issued its first report on the evaluation and review of the General Data Protection Regulation (the 'GDPR').[156] The analysis confirms that the main legislative approach, together with the specifics and challenges of the world of work, leads to a need for more guidance in the employment context of data protection principles.[157] On 22 June 2020, the European social partners adopted an autonomous agreement on the digitalisation of work,[158] addressing different aspects of the digital agenda for work, referring to article 88 GDPR.

It must be noted that also workers' representative bodies may be a forum where the translation and application of data protection rights and principles may be modelled to the relevant context of the work environment.

Some **countries** have used collective bargaining, either additionally or complementary to legislation.

For example, in **Israel**, the social partners concluded a collective agreement on Employees' use of computers in the workplace (2008).[159] It tries to strike a balance between the proprietary rights of the employer and the privacy rights of the employee. The agreement does not apply if the worker owns the computer.[160]

In **Belgium**, national collective agreements have been adopted in the National Labour Council, related to worker privacy and data protection: National Collective Agreement n° 68 (CA 68) concerns camera surveillance in the workplace and provides for the conditions and guarantees under which monitoring via video/camera is possible in the workplace; National Collective Agreement n° 81 (CA 81) van 26 April 2002 concerns the monitoring of electronic communication in the workplace, regulating the guarantees in light of the monitoring of workplace based communication, including internet and e-mail.

b. Legitimisation

Another approach of involving collective rights would concern the sphere of legitimising the processing of personal data in the employment context.

This dimension can be connected with the issue of consent. The intermediation or the involvement of a collective institution, such as a workers' representation body or a collective bargaining agreement, may lead to more robust guarantees. For example, **CoE Recommendation** (2015) provides that the agreement of employees' representatives should be sought before the introduction or adaptation of ICTs where the analysis reveals risks of interference with employees' rights and fundamental freedoms (section 20.2.). The **German** Federal Data Protection Act (BDSG) expressly permits the processing of employee data on the basis

156 Brussels, 24.6.2020 COM(2020) 264 final; https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v6_1.pdf.
157 Brussels, 24.6.2020 SWD(2020) 115 final; file:///C:/Users/u0009915/Downloads/090166e5d0c710c3%20(1).pdf.
158 https://www.businesseurope.eu/sites/buseur/files/media/reports_and_studies/2020-06-22_agreement_on_digitalisation_-_with_signatures.pdf.
159 Collective agreement 7003/2008 between the Histadrut and Liskat Hatium (June 25, 2008) http://www.workagreements.economy.gov.il/Agreements/20087033.pdf (Hebrew).
160 Wallach 2011, p. 204.

of collective agreements and works council agreements. Such an agreement can create not only workers' rights, but also workers' obligations.[161]

c. Governance

Another dimension is incorporating worker representative groups in data management and data protection impact assessment. It is referred to by section 12.2 of the ILO Code of Practice, mentioning that "***workers' representatives***, where they exist, and in conformity with national law and practice, should be informed and consulted" about certain aspects of data processing". Also section 5.8. of the ILO Code provides: "workers ***and their representatives*** should be kept informed of any data collection process, the rules that govern that process, and their rights."

The European Working Party **Opinion 2/2017** "recommends that in all cases a representative sample of employees is involved in assessing the necessity of the monitoring, as well as the logic and accessibility of the policy".[162]

The **CoE Recommendation** (2015) provides:

> 21. (...) employers should (...) c. consult employees' representatives in accordance with domestic law or practice, before any monitoring system can be introduced or in circumstances where such monitoring may change. Where the consultation procedure reveals a possibility of infringement of employees' right to respect for privacy and human dignity, the agreement of employees' representatives should be obtained;

Collective governance, with the involvement of workers' representatives, is suggested in light of the rise of artificial intelligence. Seen the impact of technology, including AI systems, on data protection in the work context, it has been recommended that "*worker representative groups must be incorporated into all discussions, design and execution of any data collection, storage, processing and decision-making strategies envisaged and/or incorporated by companies and organisations*".[163]

d. Representation

Another dimension is the role of workers' representatives in the exercise of rights of data subjects. In principle, data protection standards offer individual rights to data subjects. Within this context, workers, as data subjects, may be relying on support and assistance of their representatives.

The **CoE Recommendation** (2015) provides:

> 11.8. Unless provisions of domestic law provide otherwise, an employee should be entitled to choose and designate a person to assist him or her in the exercise of his or her right of access, rectification and to object or to exercise these rights on his or her behalf.

In **Australia**, under the Fair Work Act 2009, both employees as their unions on their behalf have a right to access their employee record and a copy of it.[164]

The data protection standards could also be seen as construing data protection rights for workers' representatives. Instead of individual rights, data protection principles could be designed to foster access to certain data processing activities through collective channels. For example, a need for transparency arises in the field of algorithms used in the work environment ('explaining the algorithm'). At the same time,

---

161 Expert Response Germany.
162 Working Party Opinion 2/2017 on data processing at work, p. 14.
163 Moore 2020, p. 89; https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf.
164 Expert Response Australia.

not only may algorithms be complex, some information may be sensitive or confidential on the part of the employer. Giving algorithmic transparency to worker representatives, rather than to workers individually, may be a pathway to overcome these issues.

A more collective view may be derived from the CoE **Recommendation (2015)** providing:

> 7.1. In accordance with domestic law and practice, or the terms of collective agreements, personal data may be communicated to the employee's representatives, but only to the extent that such data are necessary to allow them to properly represent the employee's interests or if such data are necessary for the fulfilment and supervision of obligations laid down in collective agreements.
>
> 7.2. In accordance with domestic law and practice, the use of information systems and technologies for the communication of data to employees' representatives should be subject to specific agreements that set out, in advance, transparent rules prescribing their use and safeguards to protect confidential communications, in accordance with principle 10.

▶ 4 Artificial intelligence and data protection

4.1. Introduction

The rise of new technologies, based on artificial intelligence and robotics, brings new challenges for both the world of work and data protection law. Data protection standards address the issue of AI. Many data protection concepts and principles take into account new technological developments. However, the future outlook of technology brings new challenges to the key-principles set out in the sections above.

Artificial intelligence raises new issues. AI systems may be working on the premise that massive and combined data are required and applied for different purposes, linked in manners not necessarily limited, for purposes or results not yet known, while data protection relies on purpose limitation, data minimisation and transparency. Artificial intelligent systems are sometimes seen as 'black boxes',[165] running on complex systems, connecting different types and sources of data, with results that remain often opaque. A difficulty is to understand and explain how intelligent machines or decision tools use combined data to infer certain decisions.[166] This explainability problem brings the idea to the fore that data subjects need to be entitled to "meaningful explanations to understand a given decision, grounds to contest it, and advice on how the data subject can change his or her behaviour or situation to possibly receive a desired decision".[167] Digital platforms show the effects of such work-related algorithms.[168]

An important dimension is people analytics: "the use of analytical techniques such as data mining, predictive analytics and contextual analytics to enable managers to take better decisions related to their workforce".[169] Its core lies not only in the collection of data, but in the analysis of these data. Legal scholars have indicated that three main concerns arise in this context, even when departing from personal data which are *a priori* not unlawful to collect.[170] The first is the aggregation and accumulation of data, bringing data to a 'next' and more complicated level, which may give new results, including profiling of persons. A second is the secondary use of personal data, beyond the original purpose of collection in order to explore or apply new purposes and avenues. "Data analytics involve methods and usage patterns which neither the entity collecting the data nor the data subject considered or could have even imagined at the time of collection."[171] A third aspect has to do with the accuracy of personal data in people analytics contexts, since algorithms may be applied and evaluations may result from the combination of data sets, including personal data, and the processing of them.

There are challenges for data protection standards. Questions may arise whether results generated by people analytics are accurate, adequate and reliable. There are also issues with regard to discriminatory effects. It may be that "management-by-algorithm and artificial intelligence" does not lead to more objective and bias-free HR practices.[172] A combination of different conditions may assumed to be required in order to be implemented before making proper use of it, including involvement of workers and data governance.[173]

---

165 Kilhoffer et al. 2020, p. 42; M. Graham and J. Woodcock similarly refer to one common feature among DLPs, namely "*that they offer tools to bring together the supply of, and demand for, labour.*" Graham and Woodcock 2018, p. 242.
166 Strandburg 2019, p. 1852.
167 Wachter et al., p. 844.
168 Berg et al. 2018, p. 8; Also see Drahokoupil and Fabo 2019, p. 46; Choudary 2018.
169 Shrivastava et al. 2018.
170 Cf. Bodie et al. 2017, pp. 998-1001.
171 Opinion 3/2018 EDPS Opinion on online manipulation and personal data, p.15: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.
172 De Stefano 2020, p. 72.
173 Peeters et al. 2020.

Big data processing is another area where data protection standards are challenged. Processing may rely on non-personalised or non-individualised, rather aggregated, data. The question is how this relates to the common legal definitions used in the personal data concept and the scope of data protection law. At the same time, the body of knowledge created by big data may refer to groups of individuals and the right to privacy of these groups, or individuals belonging to it, may need to be covered in other ways.[174] Another issue relates to the data minimisation principle. Big data relies on wide ranging or massive data processing and on accumulation of data, but in terms of volume as well as in time. It may be questioned how this fits into a data quality and data minimisation principle. A third aspect concerns the use of big data. A great deal of big data is connected with smart devices or the 'internet of things', which may leave it open what the future purposes of data uses are, which brings questions in light of the legitimacy and purpose limitation principles.[175]

Wearables, smart watches, smart belts, smart gloves, are part of the new world of work. These features can bring additional value to work. They may contribute to a more healthy and safe workplace. Some smart gloves allow sign language users to communicate with others without the assistance of an interpreter.[176] However, they also may become a feature of total control. For example, socio-metric badges, ID cards with integrated sensors, not only tracking location but also measuring different interpersonal variables, such as speech patterns and body movements, which results in a total picture of human interaction at work.[177] It obviously provides opportunities to assess collaboration, task organisation and productivity. Self-evidently, it poses new privacy problems in light of monitoring and surveillance and the fair processing of personal data.

An additional new level in 'Industry 4.0.' concerns robotics and cyber-physical systems (CPS). It concerns technical systems in which computers, robots and machines interact with the physical world. Smart or intelligent robots, understood as mechanical creatures which can function autonomously[178], create new questions, for example in light of human-machine interaction. When humans and robots work together, there are evident reasons to carefully consider conditions and quality of work. They come with predicted effects such as a "lack of privacy, extra monitoring and surveillance in the workplace, and a new sense of alienation".[179]

4.2. Data Protection Standards and AI

a. Applying or adapting data protection

Data protection standards can be a basis for responding to the above broad outlook and challenges. In some cases, data protection standards have to be re-interpreted, but may appear to be crucial in regulating AI. An example is 'data quality'[180], which may address AI related issues like bias, discriminatory effects, inaccurate or coincidental correlations between data, simplified conclusions, lack of context of data, or merely irrelevant data processing.[181]

Some data protection instruments specifically address or anticipate the phenomenon of algorithmic processes. Data protection law addresses, for example, profiling and/or automated decision-making and the concerns related to the ability to make decisions by technological means without human involvement.

174 Cf. Mittelstadt et al. 2018.
175 White Paper of the Committee of Experts on a data protection framework for India, 2017, https://innovate.mygov.in/wp-content/uploads/2017/11/Final_Draft_White_Paper_on_Data_Protection_in_India.pdf.
176 https://www.wipo.int/wipo_magazine/en/2019/05/article_0005.html.
177 Cf. Kim et al.
178 Murphy 2000, p. 3.
179 Upchurch and Moore 2018, p. 67.
180 Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights, FRA Focus, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf.
181 Future of Privacy Forum, *The Privacy Expert's Guide to Artificial Intelligence and Machine Learning*, 2018, p. 8; https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf.

b. Profiling and automated decision-making

With regard to profiling and automated decision-making, a series of rights of data subjects (workers) are guaranteed in some data protection instruments. Three main rights must be mentioned:

- the right not to be subject to it;
- the right be informed about it;
- the right to have a human interface.

It is mainly the GDPR which provides the most detailed provisions in this field. However, the subject received also attention in other standards, including the Code of Practice from the ILO.

Right not to be subject

The **ILO Code of Practice** contains a reference to this in section 5.5:

> "decisions concerning a worker should not be based solely on the automated processing of that worker's personal data."

Article 22, 1 **GDPR** provides that a data subject has the right not to be subject to a decision based solely on automated data processing (including profiling) which produces legal effects concerning him or her, or similarly significantly affects him or her.

The **CoE Recommendation** (2015) provides:

> 11.4. An employee should not be subject to a decision significantly affecting him or her, based solely on an automated processing of data without having his or her views taken into consideration.

The first important aspect of this is a right not to be subject (thus to object) to profiling. This is at least following from article 21.1 **GDPR**. This provision concerns all forms of data processing involving profiling, including those that are not fully automated. Furthermore, the GDPR provides for a right not to be subject to fully automated decision-making (including profiling). Under the GDPR there are, however, limits in the scope of protection. Article 22, 2 GDPR, related to fully automated decision-making, provides that the right to not being subject does not apply if the decision: a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; b) is authorized by the law to which the controller is subject and which also lays down suitable measures; or c) is based on the data subject's explicit consent (consent of workers being problematic in an EU legal context). A justification is thus possible when based on the (needs of the) employment contract. In principle, the 'necessity for the employment contract' principle requires that submitting workers to solely automated decision-making should be based on a real need.

The European Data Protection Working Party gives the following example:

> A business advertises an open position. As working for the business in question is popular, the business receives tens of thousands of applications. Due to the exceptionally high volume of applications, the business may find that it is not practically possible to identify fitting candidates without first using fully automated means to sift out irrelevant applications. In this case, automated decision-making may be necessary in order to make a short list of possible candidates, with the intention of entering into a contract with a data subject.[182]

The approach of the GDPR is thus that the employment contract can provide for justifications to involve profiling and/or fully automated decision-making. The example of the Working Party shows that a degree

[182] Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, Adopted on 3 October 2017, as last Revised and Adopted on 6 February 2018, 17/EN WP251rev.01, 21.

of leeway is given to employers. A manual processing of this number of candidates is, obviously, not very practical. But the question is from how much job applications onwards it is not necessary anymore to apply automated decision-making.

Right to be informed

The second element of protection is the right to be informed about automated decision-making. It is obviously connected with the principle of transparency.

The **CoE Recommendation** (2015) provides:

> 11.5. An employee should also be able to obtain, upon request, information on the reasoning underlying the data processing, the results of which are applied to him or her.

According to article 15,1,h **GDPR**, a data subject has the right to obtain information about the existence of (fully) automated decision-making, including profiling, and to receive meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing. In its guidelines, the European Working Party explains that:

> "the growth and complexity of machine-learning can make it challenging to understand how an automated decision-making process or profiling works. The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision. The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm. The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision."[183]

One may wonder to what extent an explanation on, for example, algorithmic decision-making to which workers are subject, can be made in clear and accessible terms in practice. The comments of the European Working Party indicate that these processes are very complicated and difficult to understand for non-experts. There is a main issue of informational asymmetry.[184] In the employment context, one could envisage organizing this transparency rather through workers' representatives, allowing them to acquire the necessary expertise.[185]

A case for a more collective right to be informed on algorithmic decision can be construed on the nature and complexity of the problem. When it comes to give some disclosure about the potential discrimination effects, or their avoidance, or that fact that some effects or data do not just concern an individual but rather a group, a collective based approach of the right to have access and information can be envisaged.[186]

Right to human interface

Under article 22, 3 GDPR (relating to fully automated decision-making) the data subject (the worker) has at least the right to obtain human intervention on the part of the controller (the employer). According to the European Working Party, human intervention is a key element in the GDPR's data protection and any review (of AI decisions) must be carried out by someone who has the appropriate authority and capability to change the decision.[187]

---

183 *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (Working Party, updated Feb 6, 2018).
184 Bayamlioglu 2018.
185 Hendrickx 2019b.
186 Mazur 2018.
187 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, 17/EN WP251rev.01, 27.

It is, however, not provided what this human interface must mean or how far such intervention in the decision-making needs to go in order to make it valid. In any case, a worker has additionally, according to article 22,3 GDPR, the right to express his or her point of view and to contest the decision. Expressing one's point of view means, according to the GDPR's recital, the right to obtain an explanation of the decision reached after such assessment and to challenge the decision.[188]

The rights under the GDPR are very consistent with the demands for a human-in-command approach in the future of work. According to the Global Commission on the Future of Work:

> "It also means adopting a 'human-in-command' approach to artificial intelligence that ensures that the final decisions affecting work are taken by human beings."[189]

4.3. From data protection to AI regulation

The increasing development of AI systems and related technology shows the relevance of general data protection standards. At the same time, it is understood that there may be limits to data protection standards and new, complementary formulas or standards are needed.[190] In light of this, many initiatives have been taken in the area of AI.

Some have been initiated through the development of privacy and data protection approach. An example is the resolution from the **Global Privacy Assembly**, grouping national data protection authorities globally, adopted as a 'Declaration on Ethics and Data Protection in Artificial Intelligence' in 2018.[191] It not only promotes principles such as fairness and transparency, but also governance, intelligibility, ethics by design, empowerment and the avoidance bias and discrimination. These principles are related and partly overlapping with data protection, but also go beyond the current known standards.

Also within international and regional organisations, new AI initiatives are in full development. In May 2019, the OECD adopted a Recommendation on Artificial Intelligence.[192] The 'principles on AI' in this recommendation are the first international standards agreed by governments.[193] UNESCO started an AI and ethics programme in order to reach consensus on a recommendation. The UNESCO Recommendation on the ethics of artificial intelligence was adopted in November 2021.[194] The Council of Europe started work on AI[195] and adopted a Recommendation in 2020 on the human rights impacts of algorithmic systems.[196] The EU took steps to establish a regulatory framework,[197] following the guidelines of an High-Level Expert Group (HLEG) on trustworthy AI[198] and the European Commission's 'White Paper on Artificial Intelligence' (2020).[199] It has led to a legislative proposal for a Regulation on artificial intelligence, known as the 'AI Act'.[200] The initiatives have in common that they focus on human-centred values, fairness, inclusivity and accountability.

188 GDPR, Recital 7.
189 ILO 2019.
190 The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, June 2020, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.
191 http://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf.
192 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
193 https://www.oecd.org/going-digital/ai/.
194 https://unesdoc.unesco.org/ark:/48223/pf0000380455.
195 https://www.coe.int/en/web/artificial-intelligence/cahai/.
196 https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.
197 https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe.
198 https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top.
199 https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.
200 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

Conclusion

This working paper looked into international and regional legal frameworks relating to personal data protection. The aim was to give a global and updated outlook of the main and basic principles in this area with a view to improve their understanding in the employment context. Taking into account legal sources and principles from a comparative perspective, the focus has been on data protection principles with a general nature embedded in a global approach.

The first international and regional data protection standards arose during the 1980's and 1990's. The landscape evolved strongly over time with different instruments coming into place within various international and regional organisations, as well as in many countries around the world. Throughout the years, data protection standards have evolved, received new attention or underwent revision, taking into account new developments related to legal, societal and technological change. In 2016, the European Union updated its legal framework with the adoption of the 'General Data Protection Regulation' (GDPR), twenty years after the ILO created its Code of Practice on the protection of workers' personal data.[201] The endorsement of data protection standards has been a more recent phenomenon in different parts of the world, such as in the Asian, African or Latin-America and Pacific regions. These initiatives brought a new dynamic in the standard-setting environment. While often reflecting the OECD model or European standards, global and regional legal development shows own pathways within nevertheless converging norms.

What all standards have in common is reliance on general and basic principles of data protection. There is a tendency for shared common ground at the level of principles, as identified in this study. In light of this, it has to be noted that, designed to respond to a variety of circumstances, general data protection principles are applicable in the employment context. It leads to a double finding. On the one hand, the proper knowledge of general data protection principles is key to understand their application in the employment relationship. On the other hand, the generality and abstract level of some data protection principles brings a need for further specification or guidance. The ILO Code of Practice is an example of this at global level, along with other, regional attempts to specify the general principles for the employment relationship, such as within the Council of Europe.

While both the right to privacy and the right to data protection are interdependent and recognised as a human right, the efforts towards more sector-specific principles of data protection standards is also a matter of adaptation and (regional) specificity. The existing range of country practices and experiences shows that a global recognition of general principles goes hand in hand with applications in diverse contexts. That may be more apparent in the sphere of the employment relationship, where local context remains highly relevant. Notwithstanding this, the challenges of technology and the world of work cover extremely global phenomena. It makes the case for interdependence or convergence of standards rather realistic.

In this working paper, general principles have been discussed, based on common ground taken from major regional initiatives around the world. Their relevance may vary in light of arising issues in the employment relationship, although they can be considered to be major benchmarks. The outlook shows how general data protection standards may operate in the employment relationship, how they are connected, and whether more specific guidance may be useful. The legitimacy of personal data processing in the employment context is fully recognised under the existing data protection standards. But a wide range of conditions and balancing will be required, taking into account the characteristics of the employment relationship. Standards show a general reluctance to ground personal data processing on individual consent. At the same time, legitimacy of personal data processing related to rights and obligations, but also interests related to the employment relationship, are fully recognised.

[201] This code of practice was adopted by a meeting of experts on workers' privacy of the ILO, convened in Geneva from 1 to 7 October 1996 (ILO 1997).

Some of the data protection standards are well in line with the body of knowledge in the field of human rights protection. Lawfulness, legitimate purposes, proportionality and transparency are key-conditions applied to the limitation or conditioning of human rights. Other data protection principles will shed new light on employment related issues. For example, the purpose limitation principle and the data minimisation principle pose important limits to personal data processing and will require both a fairness test and a privacy impact assessment before any processing takes place. The overview shows areas where these principles increasing play a role.

This brings us to some limitations of this working paper. The general data protection principles play also a role in specific data processing contexts, such as the processing of health related data or the area of monitoring and surveillance at the workplace. This study does not neglect the importance of data protection standards in these fields, on the contrary. However, the working paper dealt with some restrictions and it suggests that understanding the *basic* principles comes first, before complementary principles for *specific* areas are elaborated. The suggestion is to opt for an in-depth follow-up study in these areas, each in their own worth.

In this working paper, taking into account its scope, a brief outlook is given with regard to the role of artificial intelligence, robotisation and similar forms of automation, on data protection standards. Globally, with various rising initiatives, the development of standards is in full development. When looking into the future of AI and sophisticated automation, it becomes clear that the role of privacy and data protection within the context of employment will not be diminishing. It also defines the main challenge for data protection law. The general character of data protection principles gives them adaptability to new technological contexts, making them suitable to last sufficiently long. But broad discussions need to continue in search for instruments and standards specifically dealing with AI and related technology. A complementary set of specific AI related standards is a valuable way forward.

A final note must go to the future of work in connection with the right to privacy. Not only will the world of work be further subject of change, with it will also follow a changing work-life relationships. Technology is an important intervening factor in this context. This is seen when modern communication tools are used, including e-mail, internet, but also social media, for both professional and private purposes. New ways of working, including telework and the creation of virtual workspaces, have further challenged the work-life boundary. As indicated above, AI and robotics will also raise new challenges for the way work is defined or how it interacts with our human essence. This is why this study has kept personal data protection against the wider horizon of the right to privacy. This embedded context provides additional value in shaping or rethinking legal concepts and frameworks in light of a human-centred agenda.

References

Abdulrauf, L. 2020. "Data Protection in the Internet: South Africa." In *Data Protection in the Internet*, edited by Dário Moura Vicente and Sofia de Vasconcelos Casimiro. Ius Comparatum - Global Studies in Comparative Law 38. 349-370. Springer.

Alunge, Rogers. 2020. "Africa's Multilateral Legal Framework on Personal Data Security: What Prospects for the Digital Environment?" in *e-Infrastructure and e-Services for Developing Countries*, edited by Rafik Zitouni, Max Agueh, Pélagie Houngue and Hénoc Soude. Proceedings of the 11th EAI International Conference, AFRICOMM 2019, Porto-Novo, Benin, December 3–4, 2019. Springer.

Bayamlioglu, E. 2018. "Contesting Automated Decisions: A View of Transparency Implications", *European Data Protection Law Review* 2018, 433-446.

Berg, J., M. Furrer, E. Harmon, U. Rani, and M. Six Silberman. 2018. *Digital labour platforms and the future of work: Towards decent work in the online world*. Geneva: ILO.

Bodie, M.T., M.A. Cherry, M.L. McCormick, and J. Tang. 2017. "The Law and Policy of People Analytics." *Colorado Law Review* 88(4): 961-1042.

Boshe, Patricia. 2016. "Protection of Personal Data in Senegal." In Makulilo 2016, 259-275.

Bygrave, Lee A. 2014. *Data privacy law: An international perspective*, Oxford University Press.

—. 2017. "Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements." *Oslo Law Review* 4(2): 105–120.

Choudary, Sangeet Paul. 2018. "The architecture of digital labour platforms: Policy recommendations on platform design for worker well-being", ILO Future of Work Research Paper No. 3.

De Stefano, V. 2020. "Algorithmic Bosses and What to Do About Them: Automation, Artificial Intelligence and Labour Protection." In *Economic and Policy Implications of Artificial Intelligence*, edited by D. Marino and M. A. Monaca. Studies in Systems, Decision and Control. 65-86. Springer.

Drahokoupil, Jan and Brian Fabo. 2019. "Outsourcing, Offshoring and the Deconstruction of Employment: New and Old Challenges." In *The Deconstruction of Employment as a Political Question: 'Employment' as a Floating Signifier*, edited by Amparo Serrano-Pascual and Maria Jepsen. 33-61. Spring International Publishing.

Eurofound and ILO. 2017. *Working anytime, anywhere: The effects on the world of work*. Luxembourg: Publications Office of the European Union and Geneva: ILO.

Fantoni-Quinton, Sophie and Anne-Marie Laflamme. 2017. "Medical selection upon hiring and the applicant's right to lie about his health status: A comparative study of French and Quebec Law." *European Journal of Disability Research* 11: 85-98.

Finkin, M.W. 2003. Privacy in Employment Law. Washington DC: BNA Books.

Freedland, Mark. 1999. *Data Protection and Employment in the European Union: An Analytical Study of the Law and Practice of Data Protection and the Employment Relationship in the EU and Its Member States.* European Commission.

Graham, M. and J. Woodcock. 2018. "Towards a Fairer Platform Economy: Introducing the Fairwork Foundation." *Alternate Routes* 29: 242-253.

Greenleaf, Graham. 2012. "The Influence of European Data Privacy Standards outside Europe: Implications for Globalization of Convention 108." *International Data Privacy Law* 2(2): 68-92.

—. and B. Cottier. 2020. *Comparing African Data Privacy Laws: International, African and Regional Commitments.* University of New South Wales Law Research Series. Available at SSRN: https://ssrn.com/abstract=3582478

Hendrickx, Franck. 1999. *Privacy en Arbeidsrecht (Privacy and Labour Law),* die Keure.

—. (ed.). 2002. *Employment privacy law in the European Union: surveillance and monitoring.* Intersentia.

—. (ed.). 2003. *Employment privacy law in the European Union: human resources and sensitive data.* Intersentia.

—. 2014. "Employment Privacy", in *Comparative Labour Law and Industrial Relations in Modernized Market Economies*, edited by R. Blanpain. 465-488. Kluwer Law International.

—. 2019a. "From digits to robots: the privacy-autonomy nexus in new labour law machinery." *Comparative Labor Law and Policy Journal* 40(1): 365-388.

—. 2019b. "Privacy 4.0. at work: regulating employment, technology, and automation." *Comparative Labor Law and Policy Journal* 41(1): 147-172.

ILO. 1997. *Protection of workers' personal data: An ILO code of practice.*

—. 2019. *Global Commission on the Future of Work: Work for a brighter future.*

Jasmontaite, L., I. Kamara, G. Zanfir-Fortuna and S. Leucci . 2018. "Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR". *European Data Protection Law Review* 4(2): 168-189.

Kilhoffer, Z., W. De Groen, K. Lenaerts, I. Smits, H. Hauben, W. Waeyaert, E. Giacumacatos, J.-P. Lhernould, and S. Robin-Olivier. 2020. *Study to gather evidence on the working conditions of platform workers*. Luxembourg: Publications Office of the European Union.

Kim, Taemie, Erin McFee, Daniel O. Olguin, Ben Waber, Alex Pentland. 2012. "Sociometric badges: Using sensor technology to capture new forms of collaboration." *Journal of Organizational Behavior* 33(3): 412-427.

Krotoszynski, Ronald J. 2016. *Privacy revisited: a global perspective on the right to be left alone*. Oxford University Press.

Lehuedé, Héctor J. 2019. *Corporate governance and data protection in Latin America and the Caribbean*. Production Development Series No. 223. Santiago: ECLAC.

Long, William, Francesca Blythe, Alan C. Raul. 2020. "EU Overview", in *Privacy, Data Protection and Cybersecurity Law Review*, Seventh Edition, edited by A. C. Raul. Law Research Business Ltd.

Makulilo, Alex B. 2016. *African data privacy laws*. Springer International Publishing.

Mangan, David. 2019. "Beyond Procedural Protection: Information Technology, Privacy, and the Workplace." *European Law Review* 4: 559-571.

Mazur, Joanna. 2018. "Right to access information as a collective-based approach to the GDPR's right to explanation in European law." *Erasmus law review* 11(3): 178-189.

Mittelstadt, Brent. 2018. "From Individual to Group Privacy in Biomedical Big Data." In *Big data, health law, and bioethics*, edited by I. Cohen, H. Lynch, E. Vayena & U. Gasser. 175-192. Cambridge University Press.

Moore, P. 2020. *Data subjects, digital surveillance, AI and the future of work.* STUDY - Panel for the Future of Science and Technology. European Parliamentary Research Service, Scientific Foresight Unit.

Murphy, R. 2000. *Introduction to AI robotics.* Cambridge: MIT Press.

Navarro-Arribas, Guillermo and Vicenç Torra. 2015. *Advanced Research in Data Privacy*. Springer International Publishing.

Nouwt, S., B.R. de Vries, and C. Prins. 2005. *Reasonable Expectations of Privacy?* The Hague: TMC Asser Press.

Peeters, Tina, Jaap Paauwe and Karina Van De Voorde. 2020. "People analytics effectiveness: developing a framework." *Journal of Organizational Effectiveness: People and Performance* 7(2): 203-219.

Purtova, Nadezhda. 2017. "Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights." *Netherlands Quarterly of Human Rights* 28(2): 179-198.

Raepsaet, F. 2011. "Les attentes raisonnables en matière de vie privée." *Journal des tribunaux du travail* 1094: 145-158.

Schwab, K. 2017. *The Fourth Industrial revolution.* Crown Publishing.

Shapiro, Carl and Hal R. Varian. 1998. *Information Rules: A Strategic Guide to The Network Economy*, Harvard Business Review Press.

Shrivastava, S., K. Nagdev, and A. Rajesh. 2018. "Redefining HR using people analytics: the case of Google", *Human Resource Management International Digest* 26 (2): 3-6.

Silva, J. 2020. "Reasonable expectations of privacy in the digital age." *Seton Hall Legislative Journal* 44 (3): 607-627.

Solove, D. 2001 "Privacy and Power: Computer Databases and Metaphors for Information Privacy." *Stanford Law Review* 53 (6): 1393-1462.

Stewart, Hamish. 2019. "A Juridical Right to Lie." *Kantian Review* 24(3): 465-481.

Strandburg, Katherine J. 2019. "Rulemaking and inscrutable automated decision tools." *Columbia Law Review* 119(7): 1851-1886.

Traça, João Luís and Lídia Neves. 2016. "Data Protection in Mozambique: Inception Phase." In Makulilo 2016. 363-367. Springer.

Upchurch, Martin and Phoebe Moore. 2018. "Deep automation and the world of work." In *Humans and machines at work: Monitoring, Surveillance and Automation in Contemporary Capitalism*, edited by Phoebe V. Moore, Martin Upchurch, Xanthe Whittaker. 45-71. Palgrave MacMillan.

Wachter, Sandra, Brent Mittelstadt, and Chris Russell. 2018. "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR." *Harvard Journal of Law and Technology:* 31(2): 841-888.

Wallach, S. 2011. "The Medusa Stare: Surveillance and Monitoring of Employees and the Right to Privacy". *International Journal of Comparative Labour Law and Industrial Relations* 27(2): 189-219.

Walters, Robert, Leon Trakman and Bruno Zeller. 2019. *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches*, Singapore: Springer.

Warren, S.D, and L.D. Brandeis. 1890. "The right to privacy." *Harvard Law Review* 4(5): 193-220.

Whitman, James Q. 2004. "The Two Western Cultures of Privacy: Dignity versus Liberty." *Yale law journal* 113: 1151-1221.

Acknowledgements

Special thanks goes to the following experts for their input with country specific information: Australia: Anna Chapman, Melbourne Law School / Brazil: Ana Virginia Moreira Gomes, Universidade de Fortaleza / Bulgaria: Vasil Mrachkov and Yaroslava Genova, University of Plovdiv / Croatia: Ivana Vukorepa, University of Zagreb / Czech Republik: Martin Stefko, Charles University Prague Estonia / Germany: Elena Gramano, Bocconi University (free format) / Greece: Costas Papadimitriou, University of Athens / Hungary: Tamás Gyulavári, Pázmány Péter Catholic University / Ireland: David Mangan and Michael Doherty, Maynooth University / Israel: Lilach Lurie, Tel-Aviv University / Italy: Elena Gramano, Bocconi University / Luxembourg: Luca Ratti, University of Luxembourg / New Zealand: Paul Roth, University of Otago / Poland: Marta Otto, University of Lodz / Portugal: Rita Canas da Silva, Católica University Lisbon / Romania: Raluca Dimitriu, University of Economic Studies Bucharest / Slovakia: Andrej Poruban, Alexander Dubcek University of Trencin / Slovenia: Barbara Kresal, University of Ljubljana / Spain: Adrian Todoli Signes, University of Valencia / Sweden: Annamaria Westregard, Lund University.

Advancing social justice, promoting decent work

The International Labour Organization is the United Nations agency for the world of work. We bring together governments, employers and workers to improve the working lives of all people, driving a human-centred approach to the future of work through employment creation, rights at work, social protection and social dialogue.

Contact details

Conditions of Work and Equality Department (WORKQUALITY)
Inclusive Labour Markets, Labour Relations and Working Conditions Branch (INWORK)

International Labour Organization
Route des Morillons 4
1211 Geneva 22
Switzerland

ISBN 9789220368909