Selzer, Annika; Timm, Ingo J.

Ein Vorschlag für die datenschutzkonforme Gestaltung von Datenschutz-Grundsätzen und -Schutzmaßnahmen in IT-Systemen – Angemessene technische und organisatorische Schutzmaßnahmen nach Art. 32 DSGVO

HMD Praxis der Wirtschaftsinformatik

Provided in Cooperation with:
Springer Nature

Suggested Citation: Selzer, Annika; Timm, Ingo J. (2022) : Ein Vorschlag für die datenschutzkonforme Gestaltung von Datenschutz-Grundsätzen und -Schutzmaßnahmen in IT-Systemen – Angemessene technische und organisatorische Schutzmaßnahmen nach Art. 32 DSGVO, HMD Praxis der Wirtschaftsinformatik, ISSN 2198-2775, Springer Fachmedien Wiesbaden GmbH, Wiesbaden, Vol. 60, Iss. 4, pp. 923-939, https://doi.org/10.1365/s40702-022-00897-2

This Version is available at:
https://hdl.handle.net/10419/312234

HMD (2023) 60:923–939
https://doi.org/10.1365/s40702-022-00897-2

SPEKTRUM

Ein Vorschlag für die datenschutzkonforme Gestaltung von Datenschutz-Grundsätzen und -Schutzmaßnahmen in IT-Systemen – Angemessene technische und organisatorische Schutzmaßnahmen nach Art. 32 DSGVO

Annika Selzer · Ingo J. Timm

Eingegangen: 6. April 2022 / Angenommen: 1. August 2022 / Online publiziert: 5. September 2022

Zusammenfassung Plant eine Organisation ein neues IT-System, mit dem es personenbezogene Daten ihrer Kunden oder Mitarbeiter verarbeiten möchte, so stellt es den Planer des IT-Systems häufig vor große Herausforderungen, die Entwicklung und Inbetriebnahme des neuen IT-Systems unter Beachtung der einschlägigen datenschutzrechtlichen Anforderungen umzusetzen. Häufigster Hemmschuh für eine datenschutzkonforme Entwicklung und Inbetriebnahme eines neuen IT-Systems sind einerseits fehlende Fachkenntnisse zu datenschutzrechtlichen Rahmenbedingungen – insbesondere die datenschutzrechtlichen Anforderungen, die sich aus der Datenschutz-Grundverordnung ergeben und die entsprechend des darin verankerten risikobasierten Ansatzes *angemessen* umzusetzen sind – sowie andererseits fehlende Erfahrungen zur Gestaltung der Umsetzung dieser Anforderungen, auch hinsichtlich der Einbindung von Funktionsträgern innerhalb der Organisation seitens des Planers des IT-Systems. Der vorliegende Aufsatz möchte vor diesem Hintergrund einen Beitrag dazu leisten, Planern von IT-Systemen die wichtigsten einschlägigen Datenschutzanforderungen aufzuzeigen sowie Empfehlungen zur Umsetzung dieser Anforderungen zu geben.

Schlüsselwörter Angemessenheit · Anonymität · Datenschutz · Datenschutz-Grundverordnung (DSGVO) · Personenbezogene Daten · Technische und organisatorische Schutzmaßnahmen

Der Beitrag gibt die persönliche Meinung der Autoren wieder.

Annika Selzer (✉)
Fraunhofer SIT | ATHENE, Darmstadt, Deutschland
E-Mail: annika.selzer@sit.fraunhofer.de

Ingo J. Timm
Universität Trier und DFKI, Trier, Deutschland
E-Mail: itimm@uni-trier.de

A proposal for the data protection-compliant design of data protection principles and measures in IT systems—Appropriate technical and organizational measures according to Art. 32 GDPR

Abstract If an organization is planning a new IT system with which it wants to process personal data of its customers or employees, the planner of the IT system often faces great challenges in planning the development and use of the new IT system in compliance with the relevant data protection requirements. Frequent obstacles to a data protection-compliant development and use of a new IT system are a lack of expertise in data protection requirements and its appropriate implementation. Therefore, this paper aims to help IT system planners to identify the most important relevant data protection requirements and to provide recommendations for implementing these requirements.

Keywords Anonymity · Appropriateness · Data protection · General Data Protection Regulation (GDPR) · Personal data · Technical and organizational measures

1 Problemstellung

Die Datenschutz-Grundverordnung (DSGVO) ist seit dem 25. Mai 2018 in allen Mitgliedstaaten der Europäischen Union direkt anwendbar und hat zum Ziel, europaweit für ein einheitlich hohes Datenschutzniveau zu sorgen. Die DSGVO verfolgt hierbei einen *risikobasierten Ansatz*, verknüpft also die Höhe der Verarbeitungsrisiken für die von einer personenbezogenen Datenverarbeitung betroffene, natürliche Personen (betroffene Person) unmittelbar mit dem Umfang der durch den für die personenbezogene Datenverarbeitung Verantwortlichen (Verantwortliche) zu treffenden technischen und organisatorischen Schutzmaßnahmen. Diese sollen die betroffene Person – entsprechend dem risikobasierten Ansatz – *angemessen* schützen (Schröder 2019; Ehmann und Selmayr 2017; Gola und Klug 2018).

Neben der Umsetzung technischer und organisatorischer Schutzmaßnahmen sind bei jeder Datenverarbeitung auch die allgemeinen Datenschutz-Grundsätze umzusetzen, die u. a. regeln, dass personenbezogene Daten nur auf Basis einer Rechtsgrundlage, zu rechtmäßigen und eindeutigen Zwecken sowie nur wenn und solange die personenbezogene Datenverarbeitung zur Erreichung dieser Zwecke unbedingt erforderlich ist, verarbeitet werden dürfen (Art. 5 DSGVO). Aus diesen Grundsätzen ergibt sich auch die Notwendigkeit, vor der Planung einer neuen personenbezogenen Datenverarbeitung zunächst zu prüfen, ob der rechtmäßige Verarbeitungszweck auch unter Verarbeitung rein anonymer Daten erreicht werden kann. Auf die Verarbeitung anonymer Daten finden das Datenschutzrecht – und somit auch die strengen Vorschriften der DSGVO – keine Anwendung (Erwgr. 26 DSGVO).

Planer von IT-Systemen, die für ihre Organisation neue Systeme zur Verarbeitung der *organisationseigenen*,[1] personenbezogenen Kunden- und/oder Mitarbeiterdaten planen und umsetzen sollen, stehen häufig vor der großen Herausforderung, die Entwicklung und Inbetriebnahme des neuen IT-Systems unter Beachtung der einschlägigen datenschutzrechtlichen Anforderungen umzusetzen: Einerseits sind fehlende Fachkenntnisse zu datenschutzrechtlichen Rahmenbedingungen, andererseits fehlende Erfahrungen zur Gestaltung des Zeitplans einer datenschutzkonformen Umsetzung des geplanten IT-Systems und fehlende Praxisempfehlungen zur Notwendigkeit der Einbindung von Funktionsträgern innerhalb der Organisation seitens des Planers des IT-Systems typische Hemmschuhe für eine datenschutzkonforme Entwicklung und Inbetriebnahme eines solchen Systems.

2 Ziel, Vorarbeiten und Vorgehensweise

Um eine datenschutzkonforme Entwicklung und Inbetriebnahme von IT-Systemen zu ermöglichen, soll der vorliegende Aufsatz einen Beitrag dazu leisten, Planern von IT-Systemen die wichtigsten einschlägigen Datenschutzanforderungen aufzuzeigen sowie Empfehlungen zur zeitlichen und personellen Umsetzung der Anforderungen zu geben.

Die Grundlage der Empfehlungen sind folgende Vorarbeiten der Autoren: In (Selzer und Timm 2021b) wurden die in jeden Datenverarbeitungssystem, in dem personenbezogene Daten verarbeitet werden sollen, zu berücksichtigenden Datenschutz-Grundsätze der DSGVO vorgestellt und anhand eines beispielhaften Datenverarbeitungssystem Vorschläge zu deren Umsetzung gegeben. In (Selzer 2021) wurden die datenschutzrechtlichen Anforderungen, die durch die DSGVO an die Implementierung geeigneter und angemessener Schutzmaßnahmen gestellt werden, beschrieben und aus rechtlicher Sicht interpretiert. In (Selzer et al. 2021) wurden die Implementierungskosten beispielhafter, dem Stand der Technik entsprechenden technischer und organisatorischer Schutzmaßnahmen aus Sicht der Wirtschaftsinformatik sowie die Kosten eines Datenschutzverstoßes zu Lasten betroffener Personen aus Sicht der Wirtschaftsinformatik und Rechtswissenschaften erhoben, um daraus Erkenntnisse zur Abwägung der genannten Faktoren als Basis der Implementierung angemessener Schutzmaßnahmen abzuleiten. In (Selzer und Timm 2021a) wurden die Wichtigkeit der Vorbewertung der Notwendigkeit der personenbezogenen Datenverarbeitung in einem geplanten IT-System und die Relevanz dieser Vorbewertung in Bezug auf das Treffen angemessener Schutzmaßnahmen diskutiert.

Diese Ergebnisse aufgreifend und von konkreten Verarbeitungsszenarien abstrahierend leitet der vorliegende Aufsatz einen Vorschlag für die datenschutzkonforme Gestaltung von Datenschutz-Grundsätzen und -Schutzmaßnahmen in IT-Systemen ab. Nach der initialen Erstellung dieses Vorschlags wurde dieser im Rahmen

[1] Dieser Beitrag betrachtet die Planung und Entwicklung neuer IT-Systeme, die in der systementwickelnden Organisation später zur Verarbeitung der eigenen Kunden- und/oder Mitarbeiterdaten eingesetzt werden sollen, für die die Organisation die Rolle des datenschutzrechtlichen Verantwortlichen (weitere Ausführungen zur Rolle des Verantwortlichen erfolgen in Kapitel 3.1) innehält.

von sieben Erst- und Folgeworkshops evaluiert. Im Rahmen der Erstworkshops, an denen zwei betriebliche Datenschutzbeauftragte/Datenschutzkoordinatoren und IT-Sicherheitsbeauftragte (bzw. Mitarbeiter dieser), Mitarbeiter von Rechtsabteilungen, Verfahrenseigner (die gleichzeitig neue Verarbeitungssysteme entwickeln und umsetzen), betroffene Personen, Verantwortliche und Mitarbeiter von Datenschutzaufsichtsbehörden[2] teilnahmen, wurde der Vorschlag initial vorgestellt und anhand eines vorbereiteten, mit drei Personen validierten Gesprächsleitfaden diskutiert. Basierend auf diesen Diskussionen wurde der Vorschlag überarbeitet und sodann in einem zweiten Workshop mit dem gleichen Teilnehmerkreis vorgestellt und die finale Rückmeldung der Teilnehmer (ebenfalls auf Basis eines mit drei Personen validierten Gesprächsleitfadens) eingeholt. Die Erstworkshops sollten insofern Änderungsbedarf an dem Gestaltungsvorschlag aufzeigen, die Folgeworkshops sollten sicherstellen, dass sich durch die nach den Erstworkshops erfolgten Änderungen des Gestaltungsvorschlages keine Fehler in den Gestaltungsvorschlag eingeschlichen haben.

3 Vorschlag für die datenschutzkonforme Gestaltung von Datenschutz-Grundsätzen und -Schutzmaßnahmen in IT-Systemen

Nachfolgend wird ein praxisorientierter Vorschlag für die datenschutzkonforme Gestaltung von Datenschutz-Grundsätzen und Schutzmaßnahmen in IT-Systemen unterbreitet.

Um Empfehlungen für die zeitliche Umsetzung der Anforderungen geben zu können, wird die Planung der Umsetzung und Inbetriebnahme eines IT-Systems, mit dem (voraussichtlich) personenbezogene Daten verarbeitet werden sollen, beispielhaft für ein Umsetzungsprojekt mit zwei Jahren Laufzeit aufgezeigt. Des Weiteren wird die Annahme getroffen, dass das zu entwickelnde IT-System eine Eigenentwicklung des Verantwortlichen ist, der das IT-System später für die Verarbeitung seiner Kunden- und Mitarbeiterdaten zu nutzen plant und hierfür ausschließlich auf eine von ihm selbst innerhalb des Europäischen Wirtschaftsraumes betriebenen IT-Infrastruktur zurückgreift. Zudem wird davon ausgegangen, dass es sich bei dem Verantwortlichen um eine nicht-öffentliche, europäische Organisation ohne Organisationsstrukturen außerhalb des Europäischen Wirtschaftsraumes handelt, im Rahmen der geplanten Datenverarbeitung keine sogenannten besonderen Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) verarbeitet werden und neben den Anforderungen der Datenschutz-Grundverordnung keine weiteren datenschutzrechtlichen Anforderungen einschlägig sind.[3]

[2] Die genannten Rollen werden im Kapitel „3.1 Rollen möglicher Beteiligter“ näher vorgestellt.

[3] Außer der zeitlichen Begrenzung resultieren die hier beschriebenen Einschränkungen auf dem Wunsche des Ausschlusses der Betrachtung weiterführender Datenschutzanforderungen, die i. d. R. nicht innerhalb eines IT-Systems selbst umgesetzt werden (u. a. zur Auftragsverarbeitung und Drittstaatübermittlung).

3.1 Rollen möglicher Beteiligter

Zunächst sind die Rollen möglicher Beteiligter an den einzelnen Prozessschritten zu definieren:

Betroffene Person (bP) ist die natürliche Person, deren personenbezogene Daten in dem geplanten IT-System verarbeitet werden sollen.

Datenschutzaufsichtsbehörde (DSAB) ist eine unabhängige staatliche Stelle zur Überwachung der datenschutzrechtlichen Vorgaben. Innerhalb Deutschlands ist dies – je nach Zuständigkeit – der Bundesbeauftragte oder ein Landesbeauftragter für den Datenschutz und die Informationsfreiheit. In bestimmten Fällen besteht die Pflicht, die für einen Verantwortlichen zuständige Aufsichtsbehörde vor Beginn der Inbetriebnahme eines neuen IT-Systems zu konsultieren. Die zuständige Aufsichtsbehörde ist – je nach Einzelfall – u. a. dazu befugt, die Inbetriebnahme des IT-Systems zu untersagen, insbesondere bis zu dem Zeitpunkt der Umsetzung zusätzlicher Schutzmaßnahmen, sofern die Aufsichtsbehörde diese fordert.

Datenschutzbeauftragter, betrieblicher/behördlicher/externer, (DSB) ist eine natürliche oder juristische Person, die in vielen Organisationen verpflichtend zu bestellen ist, um bzgl. der Umsetzung der datenschutzrechtlichen Anforderungen zu beraten und die Umsetzung organisationsintern zu überwachen.

Informationssicherheitsbeauftragter/-verantwortlicher, betrieblicher/behördlicher/externer (ISB) ist eine natürliche oder juristische Person, die in vielen Organisation bestellt wird, um bzgl. der Umsetzung der Informationssicherheit zu beraten und die Umsetzung organisationsintern zu überwachen.

Rechtsabteilung, intern oder extern, (RA) ist in den meisten Organisationen die einzige Organisationseinheit, die von der Geschäftsführung/dem Vorstand der Organisation die Befugnis zum Erstellen und Freigeben rechtsverbindlicher Dokumente, wie z. B. Einwilligungserklärungen, erhalten hat.

Verfahrenseigner (VE) ist diejenige natürliche Person, die in ihrer Funktion als Mitarbeiter einer Organisation eine bestimmte, personenbezogene Datenverarbeitung (wie die Inbetriebnahme eines neuen IT-Systems) verantwortet. Während der Planungsphase wird in diesem Gestaltungsvorschlag davon ausgegangen, dass die Rolle des (zukünftigen) Verfahrenseigners von einem Team erfüllt wird, das aus dem Projektleiter, dem Anforderungsanalysten, dem Entwickler und dem späteren Betreiber besteht. Die personelle Hauptverantwortung sollte bei dem Projektleiter des Entwicklungsprozesses liegen, der die Aufgaben des VE wiederum innerhalb des vorgenannten Teams delegieren kann. Es ist davon auszugehen, dass viele für den VE definierten Aufgaben in enger Abstimmung zwischen allen vorgenannten Rollen zu erfolgen hat.[4]

Verantwortlicher (V) im Sinne der DSGVO ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten in dem geplanten IT-System entscheidet (Art. 4 Nr. 7 DSGVO). I.d.R. wird der

[4] Nach Inbetriebnahme des IT-Systems ist davon auszugehen, dass die Rolle des Verfahrenseigners nicht mehr als Team ausgeführt wird. Wem die Rolle des Verfahrenseigners im Wirkbetrieb zukommt, ist organisationsabhängig.

datenschutzrechtlich Verantwortliche durch die Geschäftsführung/den Vorstand der Organisation vertreten. Je nach Ausgestaltung der Rollen innerhalb einer Organisation, hat dieser die Entscheidungsbefugnis zur Budgetierung des Datenschutzes ggf. an die Verwaltungsleitung delegiert.

3.2 Gestaltung von Datenschutz-Grundsätzen und -Schutzmaßnahmen in IT-Systemen

Für die datenschutzkonforme Gestaltung neu geplanter IT-Systeme sind im Wesentlichen vier Schritte umzusetzen:[5]

- die Entscheidung darüber, ob das neu geplante IT-System personenbezogene oder anonyme Daten verarbeiten soll;
- die Vorprüfung der Machbarkeit aus rechtlicher und technischer Sicht;
- die Planung der Umsetzung der allgemeinen Grundsätze des Datenschutzrechts, z. B. der Planung des Einholens einer Einwilligung und der Planung der Umsetzung von Löschpflichten;
- die Planung der Umsetzung technischer und organisatorischer Schutzmaßnahmen, wie z. B. die Umsetzung des Vier-Augen-Prinzips und das Verschlüsseln von Daten.

Die vier Schritte werden in der nachstehenden Abb. 1 zusammengefasst und in den folgenden Unterkapiteln im Detail dargestellt.

3.2.1 Schritt 1: Entscheidung über die personenbezogene oder anonyme Datenverarbeitung

Der Datenschutz-Grundsatz der Datenminimierung regelt, dass personenbezogene Daten nur dann verarbeitet werden dürfen, wenn und solange die personenbezogene

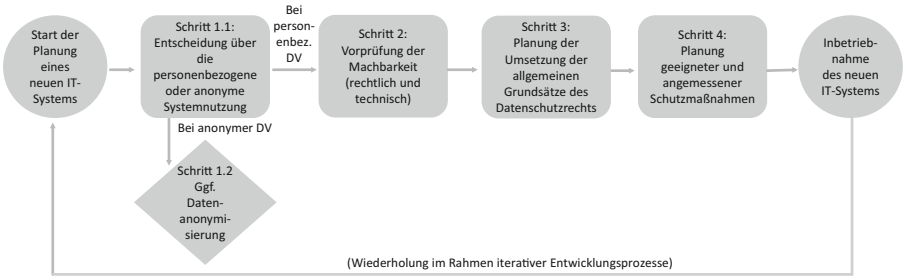

Abb. 1 Schritte zur Umsetzung des Datenschutzrechts bei der Planung neuer IT-Systeme

[5] Es handelt sich hier lediglich um einen Gestaltungs*vorschlag* aus individueller Sicht der Autoren. Der Vorschlag bildet keine individuellen Gegebenheiten einer Organisation ab – so können innerhalb einer Organisation z. B. die hier gelisteten Rollen variieren. U. a. könnte es möglich sein, dass in einer Organisation die Rolle des DSB von einem Juristen besetzt wird und daher an einigen Stellen des Gestaltungsvorschlages, an denen sowohl der DSB als auch die RA einzubeziehen sind, ggf. nur eine der beiden Rollen einbezogen werden müsste.

Tab. 1 Entscheidung über die personenbezogene oder anonyme Datenverarbeitung

Schritt	Anforderung	Regelungsgehalt	Aufgaben	Personelle Verantw.[a]	Sonstige Beteiligte	Zeitlicher Vorlauf
1.1	Vorbewertung zur Datenminimierung	Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Art. 5 DSGVO)	Bewertung, ob der Verarbeitungszweck auch mit anonymen Daten (bzw. unter anonymer Systemnutzung) erreicht werden kann (hierbei muss auch berücksichtigt werden, ob in dem IT-System Logdaten und andere technische Daten erhoben werden, die personenbezogen sind)	VE	DSB, ggf. RA	24 Monate vor Inbetriebnahme des IT-Systems
1.2	Ggf. Anonymisierung	Personenbezogene Daten müssen in einer Weise anonymisiert werden, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann (Erwgr. 26)	Ggf. Datenanonymisierung unter Beachtung der Regelungen der DSGVO, inkl. Bewertung der Gefahr, dass anonyme Daten über die Zeit (durch neue Technologien und/oder das Zusammenführen mit anderen Datensätzen) wieder Personenbezug erhalten könnten	VE	DSB, ISB, ggf. RA	Vor Inbetriebnahme des IT-Systems – da auf die Verarbeitung anonymer Daten die DSGVO keine Anwendung findet, müssten die Schritte 2–4 nicht durchgeführt werden[b]

[a]In der Spalte „personelle Verantwortlichkeit" werden Empfehlungen für die operative Verantwortlichkeit innerhalb der Organisation gegeben. Der Begriff ist nicht gleich zusetzen mit dem „Verantwortlichen" im Sinne der DSGVO (siehe Kapitel 3.1). Dies betrifft die Tab. 1, 2, 3 und 4

[b]Auch wenn dies aus datenschutzrechtlicher Sicht nicht verpflichtend ist, ist zu empfehlen, mit dem DSB zu besprechen, ob in dem System trotzdem eine kurze Datenschutzinformation hinterlegt werden sollte, um den Nutzern den Umstand aufzuzeigen, dass in dem System keine personenbezogenen Daten verarbeitet werden. Darüber hinaus sollte mit dem ISB besprochen werden, ob – außerhalb der Anforderungen des Datenschutzrechts – Anforderungen zur Umsetzung technischer und organisatorischer Schutzmaßnahmen bestehen, z. B. um vertrauliche Informationen der Organisation zu schützen, bei denen es sich nicht um personenbezogene Daten handelt

Datenverarbeitung zur Erreichung eines rechtmäßigen Verarbeitungszwecks unbedingt erforderlich ist. Vor diesem Hintergrund ergibt sich die Notwendigkeit, vor der Planung einer Datenverarbeitung zunächst zu prüfen, ob sich der geplante Verarbeitungszweck auch unter Verarbeitung anonymer Daten erreichen lässt (s. Tab. 1).

Die strengen Anforderungen des Datenschutzrechts müssen regelmäßig nur dann beachtet werden, wenn personenbezogene Daten verarbeitet werden. Auf anonyme Daten, d. h. auf Informationen, die sich nicht (mehr) auf eine identifizierte oder identifizierbare natürliche Person beziehen, finden die Anforderungen des Datenschutzrechts hingegen keine Anwendung (Erwgr. 26 DSGVO).

3.2.2 Schritt 2: Vorabentscheidung über die grundsätzliche Machbarkeit

Sofern in dem geplanten IT-System personenbezogene Daten verarbeitet werden sollen, muss im zweiten Schritt die grundsätzliche technische und datenschutzrechtliche Machbarkeit des Entwicklungsvorhabens bestätigt werden. Ziel dieses Schrittes ist es, ein langjähriges Entwicklungsvorhaben gar nicht erst zu beginnen, bevor aus rechtlicher und technischer Sicht bestätigt wurde, dass keine grundlegenden Bedenken gegen das Vorhaben sprechen oder das Vorhaben auf Grund einschlägiger datenschutzrechtlicher Regelungen oder technischer fest vorgegebener Anforderungen nicht umsetzbar ist (s. Tab. 2).

Tab. 2 Vorprüfung der Machbarkeit

Schritt	Anforderung	Regelungsgehalt	Aufgaben	Personelle Verantw.	Sonstige Beteiligte	Zeitlicher Vorlauf
2.1	Vorprüfung der Machbarkeit aus datenschutzrechtlicher Sicht	In dem geplanten IT-System müssen alle Datenschutz-Grund-sätze der DSGVO umsetzbar sein (Art. 5 DSGVO)	Vorgespräch mit dem Ziel, die datenschutzrechtliche Machbarkeit des Entwicklungsvorhabens zu bestätigen	VE	DSB, RA	24 Monate vor Inbetriebnahme des IT-Systems
			Datenschutzschulung für VE	DSB	VE (ist verpflichtet, den Arbeitsschritt anzustoßen)	
2.2	Vorprüfung der Machbarkeit aus technischer Sicht	Das IT-System muss technisch vorgegebene Anforderungen berücksichtigen können	Vorgespräch mit dem Ziel, die technische Machbarkeit des Entwicklungsvorhabens zu bestätigen	VE	DSB, ISB	24 Monate vor Inbetriebnahme des IT-Systems

Tab. 3 Planung der Umsetzung der allgemeinen Grundsätze des Datenschutzrechts

Schritt	Anforderung	Regelungsgehalt (Art. 5 DSGVO)	Aufgaben[a]	Personelle Verantw.	Sonstige Beteiligte	Zeitlicher Vorlauf
3.1	Rechtmäßigkeit	Personenbezogene Datenverarbeitung nur bei Vorliegen einer Rechtsgrundlage	Identifizieren der einschlägigen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten (ggf. einschlägige Rechtsgrundlage für besondere Kategorien personenbezogener Daten) Bei Einwilligung: Umsetzung des Einwilligungsprozesses inkl. Widerrufsmöglichkeit Bei berechtigtem Interesse: Durchführen einer Interessensabwägung inkl. Widerspruchsmöglichkeit Bei Vertragserfüllung: Vorbereiten des entsprechenden Vertrages (z. B. Nutzungsbedingungen)	RA	VE (ist verpflichtet, die Arbeitsschritte anzustoßen), ggf. DSB	Planungsphase: 23–17 Monate vor Inbetriebnahme des IT-Systems; Umsetzungsphase: bis zur Inbetriebnahme
3.2	Verarbeitung nach Treu und Glauben	Faire und gerechte Datenverarbeitung	Verhindern des Einsatzes verborgener bzw. unfairer Verarbeitungstechniken (z. B. verborgene Techniken zur Datenerhebung in Form geheimer Videoüberwachung)	VE	DSB, ISB	
3.3	Zweckbindung	Personenbezogene Daten dürfen nur für legitime Zwecke verarbeitet werden. Ein einmal festgelegter Zweck darf sich grundsätzlich nach der Datenerhebung nicht mehr ändern	Identifizierung des Verarbeitungszwecks/der Verarbeitungszwecke Bewertung der Legitimität des Zwecks/der Zwecke Umsetzung einer (technischen) Datentrennung von zu unterschiedlichen Zwecken erhobenen Daten sowie strenger Zugriffsrechte Definition von Prozessen zur Verhinderung nachträglicher Zweckänderungen	VE	Ggf. DSB Ggf. DSB, ggf. ISB	
3.4	Datenminimierung	Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein	Bewertung, ob die zu erhebenden personenbezogenen Daten einen Bezug zum Zweck der Verarbeitung haben Bewertung, ob die Verarbeitung der personenbezogenen Daten den rechtmäßigen Zweck fördert	VE	Ggf. DSB, ggf. RA	

Tab. 3 (Fortsetzung)

Schritt	Anforderung	Regelungsgehalt (Art. 5 DSGVO)	Aufgaben[a]	Personelle Verantw.	Sonstige Beteiligte	Zeitlicher Vorlauf
3.5	Richtigkeit	Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein	Definition und Umsetzung eines Prozesses zur regelmäßigen Bewertung der Richtigkeit personenbezogener Daten (in sämtlichen Phasen der Datenverarbeitung, unabhängig von der Verarbeitungsform)	VE	Ggf. DSB, ggf. RA	Planungsphase: 23–17 Monate vor Inbetriebnahme des IT-Systems; Umsetzungsphase: bis zur Inbetriebnahme
			Sofern für den Verarbeitungszweck erforderlich:[b] Definition und Umsetzung eines Prozesses zur regelmäßigen Bewertung der Aktualität personenbezogener Daten			
			Definition und Umsetzung eines Prozesses zur Bearbeitung von Berichtigungsersuchen betroffener Personen			
3.6	Speicherbegrenzung	Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist	Beurteilung, ob Ausnahmen von der Speicherbegrenzung bestehen (insb. für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke)	VE	Ggf. DSB	
			Ggf. Identifizierung des Löschzeitpunktes: Festlegung des Zeitpunkts, ab dem personenbezogene Daten für den Verarbeitungszweck nicht mehr erforderlich sind (a); Identifizierung ggf. bestehender gesetzlicher Aufbewahrungspflichten – u. a. aus dem Handelsgesetzbuch und der Abgabenordnung – (b); Festlegung des Zeitraumes zur Umsetzung der Löschung	VE	Ggf. DSB, RA	
			Ggf. Umsetzung der Einschränkung personenbezogener Daten für den Zeitraum zwischen (a) und (b)	VE	Ggf. ISB, ggf. DSB, ggf. RA	
			Ggf. Einplanen und Umsetzen des (automatisierten, teilautomatisierten oder regelmäßigen händischen) Löschens oder Anonymisierens von Daten, unter Einhaltung der Regelungen der DSGVO			
			Definition und Umsetzung eines Prozesses zur Bearbeitung von Ersuchen betroffener Personen zur Löschung oder Einschränkung der Verarbeitung	VE	Ggf. DSB, ISB	

Tab. 3 (Fortsetzung)

Schritt	Anforderung	Regelungsgehalt (Art. 5 DSGVO)	Aufgaben[a]	Personelle Verantw.	Sonstige Beteiligte	Zeitlicher Vorlauf
3.7	Integrität und Vertraulichkeit	Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten durch geeignete technische und organisatorische Maßnahmen sicherstellt	Planung und Umsetzung von Maßnahmen zur Umsetzung von Integrität, Vertraulichkeit, Verfügbarkeit und Belastbarkeit der Systeme/Dienste	ISB	VE (ist verpflichtet, die Arbeitsschritte anzustoßen), DSB, ggf. RA	Planungsphase: 23–17 Monate vor Inbetriebnahme des IT-Systems; Umsetzungsphase: bis zur Inbetriebnahme
			Planung und Umsetzung von Maßnahmen zur schnellen Wiederherstellbarkeit personenbezogener Daten			
			Planung und Umsetzung von Maßnahmen zur regelmäßigen Überprüfung der Wirksamkeit technischer und organisatorischer Schutzmaßnahmen			
			Definition und Umsetzung eines Prozesses zur Erkennung und Meldung von Datenpannen	VE	DSB, ISB	
3.8	Rechenschafts-pflicht	Die Einhaltung der vorgenannten Grundsätze muss nachweisbar sein	Ggf. Eintrag des IT-Systems in das Verzeichnis der Verarbeitungstätigkeiten	VE (ist zusätzlich dazu verpflichtet, den V über die Umsetzung der Rechenschaftspflicht informiert zu halten)	Ggf. DSB, ggf. ISB	
			Dokumentation der Auswahl der einschlägigen Rechtsgrundlage (inkl. Negativbegründung, warum andere Rechtsgrundlagen nicht in Frage kommen)		DSB	
			Ggf. Planung und Umsetzung der Dokumentation des Erteilens der Einwilligung durch die betroffenen Personen			
			Ggf. Planung und Umsetzung der Dokumentation des Löschens personenbezogener Daten (ohne dass die Dokumentation personenbezogene Daten enthält)		Ggf. DSB, ggf. ISB	
			Ggf. Planung und Umsetzung der Dokumentation von Datenpannen und dem Umgang mit diesen (je Datenpanne)			
			Planung und Umsetzung der Dokumentation der Auswahl geeigneter und angemessener Schutzmaßnahmen		Ggf. ISB	
			Planung und Umsetzung der Dokumentation über die Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung		Ggf. DSB	Planungsphase: wie oben; Umsetzungsphase: bis 6 Monate vor Inbetriebnahme (wg. ggf. bestehender Konsultationspflicht); ggf. Anpassungen bis zur Inbetriebnahme
			Ggf. Planung und Umsetzung der Dokumentation der Datenschutz-Folgenabschätzung		DSB, ISB	

Tab. 3 (Fortsetzung)

Schritt	Anforderung	Regelungsgehalt (Art. 5 DSGVO)	Aufgaben[a]	Personelle Verantw.	Sonstige Beteiligte	Zeitlicher Vorlauf
3.9	Transparenz	Betroffene Personen sollen – als Grundlage der Umsetzung ihrer Betroffenenrechte – Kenntnis über die wichtigsten Umstände der Datenverarbeitung haben	Ggf. Umsetzung der datenschutzrechtlichen Informationspflichten bei Direkterhebung	RA	VE (ist verpflichtet, die Arbeitsschritte anzustoßen), ggf. DSB	Planungsphase: 23–17 Monate vor Inbetriebnahme des IT-Systems; Umsetzungsphase: bis zur Inbetriebnahme
			Ggf. Umsetzung der datenschutzrechtlichen Informationspflichten bei Dritterhebung			
			Definition von Prozessen zur Umsetzung der weiteren Betroffenenrechte (sofern nicht Gegenstand der vorangegangenen Schritte)	VE	Ggf. DSB	

[a]Quellen der Aufgaben sind: Gola (2018); Kühling und Buchner (2020); Sydow (2018); Simitis et al. (2019); Paal und Pauly (2021); Wolff und Brink (2019); Durmus et al. (2019); Ehmann und Selmayr (2017); Koreng und Lachenmann (2018); Roßnagel (2018)

[b]Werden personenbezogene Daten etwa im Rahmen eines Berechtigungskonzeptes verarbeitet, so ist es regelmäßig erforderlich, die darin erhaltenen Daten auf dem neuesten Stand zu halten, da sonst der Zweck der Datenverarbeitung – nämlich den unberechtigten Zutritt, Zugang oder Zugriff auf personenbezogene Daten zu verhindern – nicht erfüllt werden könnte (Kühling und Buchner 2020, Paal und Pauly 2021)

Tab. 4 Planung geeigneter und angemessener technischer und organisatorischer Schutzmaßnahmen

Schritt	Anforderung	Regelungsgehalt	Aufgaben	Personelle Verantw.	Sonstige Beteiligte	Zeitlicher Vorlauf
4.1	Privacy by Design	Technische und organisatorische Schutzmaßnahmen müssen bereits in der Planungsphase neuer IT-Systeme berücksichtigt werden	Konzeption technischer und organisatorischer Schutzmaßnahmen zu Beginn der Planungsphase (s. Schritt 3.7, z. B. Passwortschutz, Datenverschlüsselung)	VE	DSB, ISB, bei Bedarf der Neubeschaffung: V	24–0 Monate vor Inbetriebnahme des IT-Systems (kontinuierlich)
4.2	Privacy by Default	Im IT-System müssen die datenschutzfreundlichsten Einstellungen voreingestellt sein	Einplanung der Möglichkeit zur Umsetzung und Umsetzung datenschutzfreundlicher Voreinstellungen vor Inbetriebnahme	VE	DSB	Planungsphase: 23–17 Monate vor Inbetriebnahme des IT-Systems; Umsetzungsphase: bis zur Inbetriebnahme
4.3	Ggf. Datenschutz-Folgenabschätzung	Bei geplanten Datenverarbeitungen mit einem besonders hohen Risiko für die Rechte und Freiheiten der betroffenen Personen ist eine Datenschutz-Folgenabschätzung verpflichtend durchzuführen	Systematische Beschreibung der geplanten Verarbeitung Bewertung der Notwendigkeit und Verhältnismäßigkeit der Datenverarbeitung Bewertung der Risiken der Datenverarbeitung	VE	DSB, ggf. DSAB (bei Konsultationspflicht)	Planungsphase: 23–17 Monate vor Inbetriebnahme des IT-Systems
			Planung technischer und organisatorischer Schutzmaßnahmen zur Begegnung der identifizierten Risiken; regelmäßige Bewertung von Neu- und Restrisiken	ISB	VE (ist verpflichtet, die Arbeitsschritte anzustoßen), ggf. DSB, bei Bedarf der Neubeschaffung: V, ggf. Auswahl bP und sonstiger Interessensgruppen wie z. B. dem Betriebsrat, ggf. DSAB (bei Konsultationspflicht)	Umsetzungsphase: bis 6 Monate vor Inbetriebnahme (wegen ggf. bestehender Konsultationspflicht); ggf. Anpassungen bis zur Inbetriebnahme

Tab. 4 (Fortsetzung)

Schritt	Anforderung	Regelungsgehalt	Aufgaben	Personelle Verantw.	Sonstige Beteiligte	Zeitlicher Vorlauf
4.4	Geeignetheit	Es müssen technische und organisatorische Schutzmaßnahmen umgesetzt werden, die zur Umsetzung der Integrität, Vertraulichkeit und Verfügbarkeit *geeignet* sind	Bewertung der funktionalen Geeignetheit der Maßnahmen – so sind z. B. ein Sicherheitsschloss oder Wachpersonal grundsätzlich geeignet, das Ziel zu erreichen, den unberechtigten Zutritt zu Räumen zu unterbinden, in denen personenbezogene Daten verarbeitet werden, während ein Feuerlöscher zur Erreichung dieses Ziels nicht geeignet ist	ISB	VE (ist verpflichtet, die Arbeitsschritte anzustoßen), DSB, bei Bedarf der Neubeschaffung: V	Planungsphase: 23–17 Monate vor Inbetriebnahme des IT-Systems Umsetzungsphase: bis zur Inbetriebnahme
4.5	Angemessenheit	Es müssen technische und organisatorische Schutzmaßnahmen umgesetzt werden, die zur Umsetzung der Integrität, Vertraulichkeit und Verfügbarkeit *angemessen* sind	*Bewertung der Angemessenheit der Maßnahmen anhand folgender Kriterien (Selzer 2021; Selzer und Timm 2021b):* Stand der Technik (insbesondere unter zur Hilfenahme des Standard-Datenschutzmodells, der entsprechenden Leitfäden der DSK und des EDSA sowie des BSI und der ENISA)[a] Implementierungskosten (inkl. Folgekosten und unter Berücksichtigung der finanziellen Gewinnabsichten des Verantwortlichen an der Datenverarbeitung) *Art* (u. a. Datenarten, Verarbeitungsarten, Kategorien betroffener Personen, genutzte Verarbeitungstechnik), *Umfang* (u. a. Menge der betroffenen Personen und der verarbeiteten Daten), *Umstände* (u. a. Verarbeitungsort, Verarbeitungszeit, eingesetzte Systeme, wirtschaftliche Interessen des Verantwortlichen) und *Zwecke* (kritische und/oder weit gefasste Verarbeitungszwecke) der Verarbeitung Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten der betroffenen Personen (insb. physische, materielle oder immaterielle Schäden für die betroffenen Personen) Schutzbedarf der personenbezogenen Daten (z. B. normal, hoch, sehr hoch)	ISB	VE (ist verpflichtet, die Arbeitsschritte anzustoßen), DSB, bei Bedarf der Neubeschaffung: V	Planungsphase: 23–17 Monate vor Inbetriebnahme des IT-Systems Umsetzungsphase: bis zur Inbetriebnahme

[a]U. a. BfDI (2020); BSI (2017); ENISA und TeleTrust (2019)

3.2.3 Schritt 3: Planung der Umsetzung der allgemeinen Grundsätze des Datenschutzrechts

Ergibt Schritt 1 der datenschutzkonformen Gestaltung von Datenschutz-Grundsätzen und -Schutzmaßnahmen in IT-Systemen die Notwendigkeit, in dem geplanten Datenverarbeitungssystem personenbezogene Daten zu verarbeiten, und ergibt Schritt 2 die grundsätzliche technische und datenschutzrechtliche Machbarkeit des Entwicklungsvorhabens, so sind zunächst die allgemeinen Grundsätze der DSGVO umzusetzen (s. Tab. 3).

3.2.4 Schritt 4: Planung geeigneter und angemessener technischer und organisatorischer Schutzmaßnahmen

Als Konkretisierung des inhaltlich vage formulierten Grundsatzes der Integrität und Vertraulichkeit obliegt es dem Verantwortlichen, technische und organisatorische Maßnahmen zu implementieren, die funktional geeignet und in Bezug auf die Risiken für die Rechte und Freiheiten der betroffenen Personen, die Implementierungskosten und den Stand der Technik angemessen sind (s. Tab. 4).

Letztendlich ist die Entwicklung eines neuen IT-Systems als iterativer Prozess zu verstehen, im Rahmen dessen i. d. R. unmittelbar nach Inbetriebnahme des IT-Systems die Entwicklung neuer Funktionalitäten des IT-Systems weiterentwickelt werden. Insofern ist nach der initialen Inbetriebnahme dafür Sorge zu tragen, dass auch die Entwicklung neuer Funktionalitäten datenschutzkonform erfolgt und die in diesem Gestaltungsvorschlag unterbreiteten Schritte insofern erneut durchlaufen werden müssen (Art. 32 Abs. 1 lit. d DSGVO). In diesem Zusammenhang sollte zudem evaluiert werden, ob sich im Rahmen des bisherigen Entwicklungsprozesses datenschutzrechtliche Anforderungen (z. B. durch neue Gesetze) verändert haben oder neue Anforderungen hinzugekommen sind. Letztgenannte Aufgabe läge in der personellen Verantwortlichkeit der Rechts-abteilung, der Verfahrenseigner wäre jedoch verpflichtet, den entsprechenden Arbeitsschritt anzustoßen.

4 Fazit

I.d.R. stellt es den Planer eines neuen IT-Systems vor große Herausforderungen, die Entwicklung und Inbetriebnahme dieses Systems in datenschutzkonformer Weise umzusetzen. Häufig fehlen seitens der Planer Fachkenntnisse zu datenschutzrechtlichen Rahmenbedingungen, andererseits fehlt es häufig an Erfahrungen zur Gestaltung des Zeitplans einer datenschutzkonformen Umsetzung des geplanten IT-Systems und zur Notwendigkeit der Einbindung von Funktionsträgern innerhalb der Organisation. Vor diesem Hintergrund zeigte der vorliegende Aufsatz die Datenschutz-Anforderungen auf, die bei der Umsetzung neuer IT-Systeme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, umzusetzen sind und gab Empfehlungen zur zeitlichen und personellen Umsetzung dieser Anforderungen.

Zukünftige, praxisnahe und interdisziplinäre Forschung sollte sich mit der Frage befassen, durch welche weiterführenden Hilfestellungen, Leitlinie und Vordrucke

der hier unterbreitete Vorschlag ergänzt werden könnte, um die Planer neuer IT-Systeme in die Lage zu versetzen, nicht nur sämtliche datenschutzrechtlichen Anforderungen, deren konkrete Teilaufgaben, Verantwortlichkeiten und Zeitplanung zu kennen, sondern diese auch anhand von an Entwicklungsprozessen orientierten Leitlinien umzusetzen sowie deren Umsetzung mit Hilfe entsprechender Vordrucke zu dokumentieren.

Danksagung Das diesem Beitrag zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) unter dem Förderkennzeichen 16KIS1361K gefördert. Die Verantwortung für den Inhalt liegt bei dem Autor. Dieser Beitrag wurde zudem vom BMBF im Rahmen der Förderung des Projektes AKRIMA (FKZ 13N16251) unterstützt.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

BfDI (2020) Das Standard-Datenschutzmodell. https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/SDM.html. Zugegriffen: 13. Febr. 2022

BSI (2017) BSI-Standard 100-2 – IT-Grundschutz-Vorgehen. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-1-Managementsysteme-fuer-Informationssicherheit/bsi-standard-200-1-managementsysteme-fuer-informationssicherheit_node.html. Zugegriffen: 5. Jan. 2022

Durmus E, Selzer A, Pordesch U (2019) Das Löschen nach der DSGVO – Eine Diskussion der datenschutzkonformen Umsetzung bei E-Mails. Datenschutz Datensich 43:786–791

Ehmann E, Selmayr M (2017) Datenschutz-Grundverordnung. C.H. Beck, München

Gola P (2018) Datenschutz-Grundverordnung – Kommentar. C.H. Beck, München

Gola P, Klug C (2018) Die Entwicklung des Datenschutzrechts im ersten Halbjahr 2018. Neue Jurist Wochenschr 71:2608–2611

Koreng A, Lachenmann M (2018) Formularhandbuch Datenschutzrecht. München, C.H. Beck

Kühling J, Buchner B (2020) Datenschutz-Grundverordnung Kommentar. C. H. Beck, München

Paal B, Pauly D (2021) Datenschutz-Grundverordnung – Kompakt-Kommentar. C.H. Beck, München

Roßnagel A (2018) Datenschutzgrundsätze – unverbindliches Programm oder verbindliches Recht? – Bedeutung der Grundsätze für die datenschutzrechtliche Praxis. Z Datenschutz 8:339–344

Schröder M (2019) Der risikobasierte Ansatz in der DS-GVO – Risiko oder Chance für den Datenschutz? Z Datenschutz 9:503–506

Selzer A (2021) The appropriateness of technical and organisational measures under article 32 GDPR. Eur Data Prot Law Rev 7:120–128

Selzer A, Timm IJ (2021a) Chances and limitations of personal and Anonymized data processing—implementing appropriate technical and organizational measures and creating added value in smart cities. GI Informatik, Berlin, S 773–787

Selzer A, Timm IJ (2021b) Gestaltung eines Systems zum anonymen Datenaustausch – Gestaltung angemessener Schutzmaßnahmen. Datenschutz Datensich 45:826–830

Selzer A, Woods D, Böhme R (2021) An economic analysis of appropriateness under article 32 GDPR. Eur Data Prot Law Rev 7:456–470

Simitis S, Hornung G, Spiecker I (2019) Datenschutzrecht – DSGVO mit BDSG (Kommentar). Nomos, Baden Baden

Sydow G (2018) Europäische Datenschutzgrundverordnung – Handkommentar. Nomos, Baden Baden

TeleTrusT, ENISA (2019) IT-Sicherheitsgesetz und Datenschutz-Grundverordnung – Handreichung zum „Stand der Technik“ technischer und organisatorischer Maßnahmen. https://www.teletrust.de/fileadmin/docs/fachgruppen/2019-02_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf. Zugegriffen: 5. Jan. 2022

Wolff H, Brink S (2019) Datenschutzrecht – Online-Kommentar. C.H. Beck, München