Dominika Juszczyk

Data Protection by Design/by Default im Unternehmen

EINFÜHRUNG

Data Protection by Design[1] ist vielleicht das am schwierigsten zu verstehende und zu implementierende Konzept für Unternehmen. Es wird argumentiert, dass der Datenschutz bei allem, was der Verantwortliche tut, im Vordergrund stehen muss. Im Kern bedeutet es, dass man geeignete und notwendige Maßnahmen in die Systeme, Prozesse und Verfahren integrieren muss, die eine wirksame Umsetzung der Datenschutzgrundsätze gem. Art. 5 Datenschutz-Grundverordnung („DSGVO") und folglich den Schutz der Rechte der betroffenen Personen gewährleisten. Es sollte kein nachträglicher Gedanke oder ein Zusatz zu den Prozessen oder der Infrastruktur sein. Der Verantwortliche muss den Datenschutz auf jeder Ebene integrieren und dafür sorgen, dass alle Beteiligten die Umsetzung unterstützen. Es besteht kein Grund, die Anforderungen der DSGVO als negativen oder verzögernden Faktor für das Wachstum des Unternehmens zu sehen oder die Funktionalität für den Datenschutz zu opfern. Es ist eher ein Kulturwandel, der ein Gleichgewicht zwischen Wachstum und Sicherheit erfordert. Im digitalen Zeitalter ist es essenziell für einen effektiven Datenschutz zu sorgen, und das kann auch einen Wettbewerbsvorteil bedeuten. Data Protection by Default[2] wird als komplemen-

1 Der deutsche Titel des Art. 25 DSGVO „Datenschutz durch Technikgestaltung" ist irreführend. In anderen Sprachfassungen, u. a. Englisch (die Sprache in der die DSGVO ausgehandelt wurde), wird die Vorschrift als „Datenschutz durch Gestaltung" bezeichnet. Die Einschränkung auf eine technische Sicht ist inkorrekt und findet in vielen Sprachen nicht statt. Aus diesem Grund wird an dieser Stelle der englische Begriff „*Data Protection by Design*" verwendet.

2 Data Protection by Default wird u. a. in den „Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" näher erklärt.

täre Anforderung verstanden, ein besonderer Fall oder eine Konkretisierung[3] zu *Data Protection by Design*. So müssen im Gestaltungsprozess der Verarbeitung die Anforderungen beider Konzepte berücksichtigt werden.

Welche wesentlichen Aspekte müssen aus Unternehmenssicht berücksichtigt werden, um die Anforderungen des Art. 25 DSGVO (*Data Protection by Design/ by Default)* zu erfüllen?

ADRESSAT

Data Protection by Design ist eine verbindliche gesetzliche Anforderung, die vom Verantwortlichen im Sinne des Art. 4 Nr. 7 DSGVO eingehalten werden muss. Hersteller von Produkten, Diensten und Anwendungen sind nicht direkt angesprochen[4], können durch die Erfüllung dieser Voraussetzungen jedoch hilfreich oder indirekt dazu beitragen, dass Verantwortliche sich bewusst für diese Produkte und Dienstleistungen entscheiden. Dies gilt im Besonderen, wenn Dienstleister als Auftragsverarbeiter tätig sind, da Verantwortliche nämlich nur solche Auftragnehmer einsetzen dürfen, die aufgrund der getroffenen technischen und organisatorischen Maßnahmen dessen Datenschutzpflichten erfüllen[5].

PROAKTIVITÄT UND RELEVANTER ZEITRAUM

Die Auswahl geeigneter technischer und organisatorischer Maßnahmen im Rahmen von Data Protection by Design muss am Anfang des Planungsprozesses stehen. Der Gesetzeswortlaut verweist auf den Zeitpunkt „bei Festlegung der Mittel für die Verarbeitung". Spätestens mit der verbindlichen Entscheidung über das Mittel der Verarbeitung muss demnach feststehen, welche Maßnahmen zur Berücksichtigung des Datenschutzes getroffen werden. Darüber hinaus muss die Eignung der gewählten Mittel zum Zeitpunkt der eigentlichen Verarbeitung überprüft und ggf. neu bewertet werden. Der Verantwortliche hat die getroffenen Maßnahmen während des gesamten Vorgangs – beim Produktlebenszyklus einschließlich Entwicklung, Testen, Wartung, Speicherung, Löschung usw. – einzubringen und zu integrieren. Dies gilt von der ersten Idee bis zum Erreichen des End-of-Life eines Produktes bzw. einer Dienstleistung. Diese Verpflichtung erstreckt sich auf die Verarbeitung durch Auftragsverarbeiter im Rahmen einer Auftragsverarbeitung i. S. d. Art. 28 DSGVO[6]. Auf diese Weise wirkt Data Protection By Design möglichen Datenschutzverletzungen im Idealfall präventiv entgegen und stärkt das Vertrauen der Betroffenen in die Verarbeitungssysteme. Wenn die Sicherheitspraxis darin bestehen würde, nachträglich Brände zu löschen und Verstöße lediglich zu beheben, dann würden Verantwortliche reaktiv statt proaktiv handeln und den Grundsatz des Data Protection By Design nicht erfüllen[7]. Darüber hinaus liegt es im Interesse des Verantwortlichen, aus Kostengründen, das Konzept eher früher als später zu beachten. Es könnte schwierig, zeitaufwendig und kostspielig sein, nachträgliche Änderungen an Plänen vorzunehmen.

ANGEMESSENHEIT

Gemäß dem Konzept der Technologieneutralität werden in der DSGVO keine genauen Maßnahmen aufgelistet, die zu ergreifen sind. Stattdessen sollen die Maßnahmen in Bezug auf den gesamten Verarbeitungsvorgang geeignet sein. Dies umfasst insbesondere Art und Umfang sowie die Umstände und Zwecke der Verarbeitung. Dementsprechend können alle Methoden oder Mittel geeignet sein, die ein Verantwortlicher bei der Verarbeitung anwenden kann und die dazu beitragen, den beabsichtigten Zweck (hier: Data Protection by Design) zu erfüllen.[8] Zusätzlich sind bei Auswahl der Maßnahmen der Stand der Technik, die Implementierungskosten sowie die unterschiedlichen Risiken für die Betroffenen zu berücksichtigen. Damit bleibt dem Verantwortlichen ein großzügiger Entscheidungsspielraum, dessen Abwägung im Rahmen der Rechenschaftspflichten zu dokumentieren ist.

BERÜCKSICHTIGUNG DES STANDES DER TECHNIK

„Stand der Technik" ist ein dynamischer Begriff, der auf die besten verfügbaren Techniken verweist. Dabei sind solche Maßnahmen zu berücksichtigen, die sich bereits in der Praxis bewährt haben oder zumindest im Betrieb mit Erfolg erprobt wurden[9]. Welche Maßnahmen aktuell dem Stand der Technik entsprechen, muss

3 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 25 Rn. 8

4 Hersteller werden nur in Erwägungsgrund 78 DSGVO erwähnt.

5 Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 25 Rn. 25, 26

6 Artikel-29-Datenschutzgruppe, WP 169, S.30 f.

7 Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DS-GVO Art. 25 Rn. 13, 14

8 EDSA, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Rn.8

9 vgl. 4.5.1 Handbuch der Rechtsförmlichkeit des Bundesjustizministeriums

der Verantwortliche fortlaufend und regelmäßig unter Berücksichtigung internationaler sowie branchenspezifischer Standards überprüfen. Der Stand der Technik als Technologieniveau und verbindlicher Mindeststandard für die zu treffenden technischen und organisatorischen Maßnahmen ist dabei abzugrenzen vom Technologiestand „Stand der Wissenschaft und Forschung“[10] und dem Technologiestand „allgemein anerkannte Regeln der Technik“[11]. Der Stand der Technik bietet demnach fortschrittlichere Techniken als die allgemein anerkannten Regeln der Technik, verlangt aber im Gegensatz zum Stand der Wissenschaft und Forschung die nachgewiesene Tauglichkeit für den praktischen Einsatz. Orientierungen dazu können sich aus den Empfehlungen der Agentur der Europäischen Union für Cybersicherheit (ENISA)[12] oder der Handreichung des Bundesverbands IT-Sicherheit e.V. (TeleTrusT)[13] ergeben.

IMPLEMENTIERUNGSKOSTEN

Der Verantwortliche soll bereits bei der Planung sowie nach Einrichtung[14] der Maßnahmen die „Implementierungskosten“ beachten. Dabei versteht man unter diesem Begriff nicht nur die finanziellen Aufwände, sondern Ressourcen im Allgemeinen, einschließlich Zeit und Personal. Die DSGVO lässt dem Verantwortlichen auch hier einen weiten Auslegungsspielraum, wobei dieser sich nicht unter Berufung auf die Kosten der Umsetzung der Einhaltung des Data Protection By Design entziehen kann[15].

EINSCHÄTZUNG DES RISIKOS FÜR DIE BETROFFENEN

Bei Auswahl geeigneter Maßnahmen muss der Verantwortliche die „Eintrittswahrscheinlichkeit“ und „Schwere“ der Risiken für die Rechte und Freiheiten der Betroffenen berücksichtigen. Daraus folgt unmittelbar die Verpflichtung zur Risikobewertung für sämtliche Verarbeitungsvorgänge, unabhängig von der Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO, die nur im Falle voraussichtlich hoher Risiken durchzuführen ist.

HAUPTAKTEURE IN DER UMSETZUNG

Wie bereits erwähnt müssen Verantwortliche viele Aspekte bei der Umsetzung von Data Protection by Design beachten. Aus praktischer Sicht ist es enorm wichtig, dass alle Beteiligten (u.a. Geschäftsführung, Rechtsabteilung, Produkt- und Tech-Teams) innerhalb der Organisation eingebunden sind, die zur Einhaltung dieses Prinzips beitragen sollen. Besonders wichtig ist ein regelmäßiger Austausch zwischen den Datenschutz- und Sicherheitsexperten mit der Geschäftsführung. Zum Schutz der Rechte der betroffenen Personen muss der Verantwortliche auf technischer Ebene Verfahren vorsehen, um die Grundsätze der Verarbeitung sowie die Betroffenenrechte proaktiv zu gewährleisten. Beim Einsatz technischer Maßnahmen sollte die IT früh einbezogen werden. Verschiedene Spezialisten, von User-Experience-Designern über CTO und CPO bis hin zu Back-End-Entwicklern und mehr, können gefragt sein. Auch solche Teams, die sich mit künstlicher Intelligenz und maschinellem Lernen beschäftigen, werden ihre Ansätze anpassen müssen, um die Datenschutzanforderungen zu erfüllen[16].

DOKUMENATIONSPFLICHT

Data Protection by Design erfordert nicht nur die Umsetzung geeigneter technischer und organisatorischer Maßnahmen, sondern auch die vollständige Dokumentation der Auswahl. Dabei sind insbesondere die Risikoanalyse sowie die Entscheidungsgründe zur Auswahl der Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung nachzuweisen. Auch die regelmäßige Überprüfung der implementierten Maßnahmen im Hinblick auf die Eignung sollte geplant und dokumentiert werden.

10 Hier fehlt es an einer Bewährung in der Praxis.

11 Hier sind nur solche Techniken zu berücksichtigen, die auch fachlich unumstritten und anerkannt sind. Bundesverband IT-Sicherheit e.V. (TeleTrusT), IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum „Stand der Technik“ Technische und organisatorische Maßnahmen, 2021

12 Vgl. ENISA, Privacy and Data Protection by Design – from Policy to engineering, 2014; ENISA, Data Protection Engineering, 2022

13 Vgl. Bundesverband IT-Sicherheit e.V. (TeleTrusT), IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum „Stand der Technik“ Technische und organisatorische Maßnahmen, 2021

14 Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 25 Rn. 45

15 Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 25 Rn. 42

16 *Data Protection Engineering* kann als Teil von Data Protection by Design und by Default wahrgenommen werden. Es zielt darauf ab, die Auswahl, den Einsatz und die Konfiguration geeigneter technischer und organisatorischer Maßnahmen zu unterstützen, um bestimmte Datenschutzgrundsätze zu erfüllen. Mehr über die spezifischen Rollen und ihre Kontaktpunkte zum Datenschutz lesen Sie unter https://iapp.org/news/a/the-disciplines-of-modern-data-privacy-engineering/

EXEMPLARISCHE MASSNAHMEN

Die Umsetzung von Data Protection by Design kann nur wirksam erfolgen, wenn sowohl technische (u. a. *Privacy Enhancing Technologies*) als auch organisatorische Maßnahmen ausgewählt werden. Die nachfolgenden Maßnahmen dienen beispielhaft als Entscheidungshilfe:

- **Pseudonymisierung**
  Pseudonymisierung sollte verwendet werden, wenn personenbezogene Daten nicht (mehr) notwendig sind, um direkt identifizierbare personenbezogene Daten zu haben. Re-Identifizierung Betroffener im Rahmen der Pseudonymisierung ist weiterhin möglich, man braucht aber dafür zusätzliche Informationen (Schlüssel). Wichtig zu erwähnen ist, dass die Identifikationsschlüssel separat gespeichert werden müssen.
- **Anonymisierung**
  Im Gegensatz zu pseudonymisierten Daten sind anonymisierte Daten grundsätzlich nicht mehr personenbezogen. Anonymisierung wird durch Veränderung der Daten erreicht. Man spricht von einer absoluten oder faktischen/relativen Anonymisierung[17]. Eine absolute Anonymisierung ist schwer zu erreichen und erfordert in der Regel eine starke Veränderung des Datensatzes, was sich in der Regel negativ auf die Nutzbarkeit auswirkt. Bei einer relativen Anonymisierung ist die Re-Identifizierbarkeit nicht komplett ausgeschlossen. Um den besten Kompromiss zu finden, muss der Verantwortliche die Art der Daten, den Kontext und die möglichen Angriffsmodelle berücksichtigen[18].
- **Nutzung synthetischer Daten**
  Synthetische Daten sind maschinell erzeugte Daten, die den realen Daten (sowohl persönlichen als auch nicht-persönlichen) ähneln, sich aber nicht auf eine identifizierte oder identifizierbare Person beziehen. Sie sind besonders nützlich zum Testen von Diensten und Softwareanwendungen.
- **Verschlüsselung**
  Das Ziel der Verschlüsselung ist es, die Daten unlesbar zu machen und sicherzustellen, dass nur autorisierte Personen auf diese Daten zugreifen können. Dadurch werden Integrität und Vertraulichkeit der Daten technisch sichergestellt. Je nach Bedarf kann die Verschlüsselung auf drei verschiedenen Ebenen angewandt werden: Speicherebene, Datenbankebene und Anwendungsebene. Die Verschlüsselung stellt sicher[19], dass Informationen privat und vertraulich bleiben, unabhängig davon, ob sie gespeichert oder übertragen werden. Details u. a. über bestimmte Methoden in Bezug auf verschiedene Objekte (Festplatten, Dateien und E-Mails) können Sie in der Handreichung des Bundesverbands IT-Sicherheit e.V.[20] erfahren.
- **Data Tagging**
  Eine Klassifizierung der Daten (sog. Data Tagging) ist ein bewährtes Konzept mit einer Vielzahl von Anwendungsfällen, die von der Rohdatenklassifizierung bis zur Verhinderung von Datenlecks reichen. Durch eine besondere Kennzeichnung der verschiedenen Datenkategorien kann u. a. der Grundsatz der Zweckbindung durch physische oder logische Trennung der zu verschiedenen Zwecken genutzten Daten erreicht werden.[21] Data Tagging hilft auch, sensible Daten zu identifizieren, damit ihre Verarbeitung angemessen erfolgen kann.
- **Benennung eines/einer Datenschutzbeauftragten (DSB)**
  Eine der wichtigsten organisatorischen Maßnahmen in der Praxis ist, unabhängig von einer gesetzlichen Verpflichtung, die Benennung eines DSB. Durch rechtzeitige Einbeziehung in die Geschäftsprozesse kann ein DSB aufgrund seiner fachlichen Qualifikation die Einhaltung der DSGVO beratend unterstützen, aber auch gleichzeitig überwachen.
- **Regelmäßige Schulungen und Sensibilisierung der Beschäftigten**
  Die Schulung und Sensibilisierung der Beschäftigten ist eine elementare Maßnahme zur Umsetzung des erforderlichen Datenschutzniveaus. Beschäftigte sollten nicht nur die gesetzlichen Vorschriften zum Datenschutz kennen, sondern insbesondere wissen, wie mit personenbezogenen Daten im Unternehmen umzugehen ist und welche Maßnahmen zur Gewährleistung von Data Protection by Design implementiert wurden. Ergänzend empfehlen sich auch dedizierte Schulungen für bestimmte Fachbereiche oder Teams.
- **Rollen-und Berechtigungskonzept**
  Nach dem „Need-to-know-Prinzip“ erhalten nur solche Personen Zugriff auf die Daten, die am jeweiligen Geschäftsprozess und den damit verbundenen Verarbeitungsvorgängen beteiligt sind. Das Berechtigungskonzept kann sowohl organisatorisch abbilden, wer

17 Schwartmann/Jaspers/Lepperhoff/Meier, Praxisleitfaden zum Anonymisieren personenbezogener Daten, 2022

18 ENISA, Data Protection Engineering, 2022

19 Mit zunehmender technischer Entwicklung und der daraus resultierenden Erhöhung der Rechenleistung besteht die Gefahr, dass, sobald Quantencomputer verfügbar sind, die bisherigen Methoden gebrochen oder ihre Wirksamkeit mindestens halbiert werden.

20 Vgl. Bundesverband IT-Sicherheit e.V. (TeleTrusT), IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum „Stand der Technik“ Technische und organisatorische Maßnahmen, 2021

21 Paal/Pauly/Martini, DS-GVO, Art. 25 Rn. 30.

welche Zugriffe auf welche Daten benötigt und haben darf, als auch technisch die erforderlichen Zugriffe regeln.

- **Löschroutinen**
  Um insbesondere die Grundsätze der Datenminimierung und Speicherbegrenzung zu gewährleisten, ist es erforderlich Löschroutinen zu implementieren. Diese können organisatorisch in Form von Löschkonzepten und Richtlinien erfolgen, müssen jedoch auch technisch umgesetzt werden und nachweisbar sein.

ZERTIFIZIERUNGSVERFAHREN

Um die Einhaltung von Data Protection by Design/by Default nachzuweisen, kann ein genehmigtes Zertifizierungsverfahren gem. Art. 42 DSGVO hilfreich sein. Eine derartige, akkreditierte Zertifizierung stellt für sich zwar keine Bescheinigung für 100%ige DSGVO-Compliance dar; es ist jedoch ein wirksamer Faktor, um die Implementierung erforderlicher und geeigneter technischer und organisatorischer Maßnahmen nachzuweisen. Insbesondere kann es die Kommunikation mit Aufsichtsbehörden, Geschäftspartnern und betroffenen Personen unterstützen, entbindet aber nicht von der gesonderten Betrachtung der Erfüllung der Pflichten des Art. 25 Abs. 1, 2 DSGVO.[22]

SANKTIONEN

Artikel 25 Abs. 1, 2 DSGVO enthält verbindliche und bußgeldbewehrte Regelungen. Die Nichtbeachtung von Data Protection by Design kann auch zu weiteren Verstößen führen, z. B. zu einem Verstoß gegen die in Art. 5 DSGVO geregelten Grundsätze der Verarbeitung.[23] Ferner kann ein Verstoß gegen Art. 25 Abs. 1 DSGVO einen Schadenersatzanspruch des Betroffenen gemäß Art. 82 DSGVO auslösen. Der Verantwortliche haftet für alle materiellen und immateriellen Schäden, die dem Betroffenen durch fehlende oder unzureichende Umsetzung von Data Protection by Default verursacht wurden.[24]

ZUSAMMENFASSUNG

Die Implementierung von Data Protection by Design spiegelt ein Verständnis des Wertes personenbezogener Daten sowohl für Verantwortliche als auch für die Betroffenen wider. Datenschutz und die persönliche Kontrolle der Betroffenen über ihre Daten sind wichtige Rechte und Freiheiten, die von der DSGVO in konsequenter Weise geschützt werden. Die Umsetzung von Data Protection by Design ist herausfordernd, da es nicht auf intuitive Weise umgesetzt werden kann. Geeignete technische und organisatorische Maßnahmen sind zwingend frühzeitig zu berücksichtigen, in die Verarbeitung zu integrieren und kontinuierlich zu überprüfen.

Dominika Juszczyk, LL.M. hat ein Master Studium mit Schwerpunkt IT-Recht abgeschlossen. Seit Ende 2022 ist sie als Legal Counsel bei der IBS data protection services and consulting GmbH tätig. Als CIPP/E zertifizierte Datenschutzexpertin unterstützt sie die Einhaltung geltender gesetzlicher und regulatorischer Anforderungen im Bereich Datenschutz bei nationalen und internationalen Kunden. Ihre Beratungsschwerpunkte liegen im IT-Vertragsrecht, Datenschutzmanagement sowie technologierechtlich relevanten Fragestellungen.

22 BeckOK DatenschutzR/Paulus, 42. Ed. 1.11.2021, DS-GVO Art. 25 Rn. 14, 15

23 Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DS-GVO Art. 25 Rn. 3, 7

24 Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 25 Rn. 6