Leitlinien 4/2019 zu Artikel 25

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Version 2.0

Angenommen am 20. Oktober 2020

Versionsverlauf

Version 1.0	13. November 2019	Annahme der Leitlinien zur öffentlichen Konsultation
Version 2.0	20. Oktober 2020	Annahme der Leitlinien des EDSA nach der öffentlichen Konsultation

Inhaltsverzeichnis

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 70 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden „DSGVO“),

gestützt auf das EWR-Abkommen, insbesondere auf Anhang XI und das Protokoll 37, in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 geänderten Fassung,

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung –

HAT DIE FOLGENDEN LEITLINIEN ANGENOMMEN:

Zusammenfassung

In einer zunehmend digitalisierten Welt spielt die Einhaltung der Anforderungen im Zusammenhang mit Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (im englischer Sprachfassung „Data Protection by Design and by Default“ und im Folgenden kur „DPbDD“ oder „Technikgestaltung und Voreinstellung“) eine wesentliche Rolle bei der Förderung der Privatsphäre und des Datenschutzes in der Gesellschaft. Daher ist es von grundlegender Bedeutung, dass die Verantwortlichen diese Verantwortung ernst nehmen und die Verpflichtungen gemäß DSGVO bei der Gestaltung von Verarbeitungsvorgängen umsetzen.

Die vorliegenden Leitlinien geben eine allgemeine Orientierungshilfe zur Verpflichtung zum DPbDD nach Artikel 25 der DSGVO. Diese Verpflichtung gilt für alle Verantwortlichen unabhängig von Umfang und Komplexität der Verarbeitung. Um die Anforderungen im Zusammenhang mit dem DPbDD einhalten zu können, ist es für Verantwortliche von entscheidender Bedeutung, die Datenschutzgrundsätze zu verstehen und die Rechte und Freiheiten der betroffenen Personen zu kennen.

Die zentrale Verpflichtung ist die Umsetzung *geeigneter Maßnahmen* und notwendiger Garantien zur *wirksamen Umsetzung der Datenschutzgrundsätze* und folglich zum *Schutz der Rechte und Freiheiten der betroffenen Personen durch Technikgestaltung und Voreinstellung*. Artikel 25 sieht für beide Maßnahmen Aspekte vor, die berücksichtigt werden sollten. Diese Aspekte werden in den vorliegenden Leitlinien präzisiert.

Artikel 25 Absatz 1 legt fest, dass die für die Verantwortlichen DPbDD frühzeitig berücksichtigen sollen, wenn sie einen neuen Verarbeitungsvorgang planen. Die Verantwortlichen sollen DPbDD *vor* der Verarbeitung umsetzen und gewährleisten ihn durch die regelmäßige Überprüfung der Wirksamkeit der gewählten Maßnahmen und Garantien *kontinuierlich* bei der Verarbeitung. DPbDD gilt auch für bestehende Systeme, die personenbezogene Daten verarbeiten.

Die Leitlinien enthalten zudem Anleitungen für die wirksame Umsetzung der in Artikel 5 genannten Datenschutzgrundsätze; hierzu werden zentrale Aspekte der Technikgestaltung und der Voreinstellung aufgeführt und zur Veranschaulichung praktische Fälle beschrieben. Der Verantwortliche prüft die Eignung der vorgeschlagenen Maßnahmen im Zusammenhang mit der betreffenden konkreten Verarbeitung.

Der EDSA legt Empfehlungen vor, wie Verantwortliche, Auftragsverarbeiter und Hersteller bei der Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zusammenarbeiten können. Der Ausschuss ruft die Verantwortlichen in der Industrie, die Auftragsverarbeiter und Hersteller dazu auf, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als Möglichkeit zu nutzen, sich bei der Vermarktung ihrer Produkte bei Verantwortlichen und betroffenen Personen einen Wettbewerbsvorteil zu verschaffen. Außerdem regt der Ausschuss alle Verantwortlichen an, von Zertifizierungen und Verhaltensregeln Gebrauch zu machen.

1 ANWENDUNGSBEREICH

1. Zentraler Gegenstand der Leitlinien ist die Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen auf der Grundlage der Verpflichtung nach Artikel 25 DSGVO.[1] Auch in Artikel 25 nicht direkt genannte sonstige Akteure, wie Auftragsverarbeiter und Hersteller von Produkten, Diensten und Anwendungen (im Folgenden „Hersteller“) können aus diesen Leitlinien Nutzen für die Gestaltung von DSGVO-konformen Produkten und Diensten ziehen, die die Verantwortlichen in die Lage versetzen, ihren Datenschutzpflichten nachzukommen.[2] Der Erwägungsgrund 78 der DSGVO sieht ergänzend vor, dass der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen auch bei öffentlichen Ausschreibungen zu berücksichtigen ist. Obwohl alle Verantwortlichen verpflichtet sind, bei ihren Verarbeitungstätigkeiten den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen einzubeziehen, fördert diese Bestimmung die Aneignung der Datenschutzgrundsätze; hierbei sollten öffentliche Verwaltungen mit gutem Beispiel vorangehen. Da der Verantwortliche für die Einhaltung der Verpflichtungen zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen bei der Verarbeitung, die seine Auftragsverarbeiter und Unterauftragsverarbeiter ausführen, verantwortlich ist, sollte er bei der Vergabe von Aufträgen an diese Parteien darauf hinweisen, dass diese Verpflichtungen einzuhalten sind.

2. Die in Artikel 25 genannte Anforderung richtet sich an die Verantwortlichen und sieht vor, den Datenschutz in die Verarbeitung personenbezogener Daten zu integrieren und eine entsprechende Voreinstellung vorzunehmen; dies gilt für den gesamten Lebenszyklus der Verarbeitung. Der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen muss auch bei Verarbeitungssystemen gewährleistet sein, die bereits vor Inkrafttreten der DSGVO angewandt wurden. Die Verantwortlichen müssen die Verarbeitung in Einklang mit der DSGVO laufend aktualisieren. Weitere Informationen über die Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen bei einem bestehenden System können dem Unterkapitel 2.1.4 der vorliegenden Leitlinien entnommen werden. Im Kern sieht die Bestimmung vor, dass ein *geeigneter* und *wirksamer* Datenschutz sowohl durch *Technikgestaltung* als auch durch *Voreinstellung* sicherzustellen ist; dies bedeutet, dass die Verantwortlichen nachweisen können

[1] Die hierin enthaltenen Auslegungen gelten ebenso für Artikel 20 der Richtlinie (EU) 2016/680 und Artikel 27 der Verordnung (EU) 2018/1725.

[2] In Erwägungsgrund 78 DSGVO ist diese Notwendigkeit eindeutig festgelegt: „*In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen*“.

sollten, dass sie für die Verarbeitung geeignete Maßnahmen ergriffen und Garantien umgesetzt haben, um die Wirksamkeit der Datenschutzgrundsätze und der Rechte und Freiheiten betroffener Personen zu gewährleisten.

3. In Kapitel 2 der Leitlinien liegt der Schwerpunkt auf der Auslegung der in Artikel 25 genannten Anforderungen. Ferner werden hier die mit dieser Bestimmung eingeführten rechtlichen Verpflichtungen behandelt. Kapitel 3 enthält Beispiele für die Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen im Zusammenhang mit spezifischen Datenschutzgrundsätzen.

4. In Kapitel 4 der Leitlinien wird die Möglichkeit untersucht, ein Zertifizierungssystem für den Nachweis der Einhaltung von Artikel 25 einzurichten, und in Kapitel 5 geht es darum, wie die Aufsichtsbehörden die Einhaltung des Artikels durchsetzen können. Schließlich werden den Interessengruppen in den Leitlinien weitere Empfehlungen dazu unterbreitet, wie der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen erfolgreich umgesetzt werden kann. Der EDSA ist sich der Schwierigkeiten bewusst, die die umfassende Einhaltung der Verpflichtungen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen für kleine und mittlere Unternehmen (im Folgenden „KMU") bedeutet; in Kapitel 6 legt er deshalb zusätzliche Empfehlungen vor, die sich speziell an KMU richten.

2 ANALYSE VON ARTIKEL 25 (1) UND (2): DATENSCHUTZ DURCH TECHNIKGESTALTUNG UND DURCH DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

5. In diesem Kapitel sollen die Anforderungen an den Datenschutz durch Technikgestaltung nach Artikel 25 Absatz 1 und an den Datenschutz durch datenschutzfreundliche Voreinstellungen nach Artikel 25 Absatz 2 untersucht und entsprechende Leitlinien aufgestellt werden. Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen ergänzen sich und verstärken sich gegenseitig. Betroffene Personen werden einen größeren Nutzen von dem Datenschutz durch datenschutzfreundliche Voreinstellungen haben, wenn gleichzeitig der Datenschutz durch Technikgestaltung umgesetzt wird – und umgekehrt.

6. Der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ist von allen Verantwortlichen umzusetzen, von kleinen Unternehmen ebenso wie von multinationalen Unternehmen. Daher kann die Komplexität der Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen je nach Verarbeitungsvorgang variieren. Unabhängig vom Umfang kann die Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen dem Verantwortlichen und der betroffenen Person jedoch in jedem Fall Vorteile bringen.

2.1 Artikel 25 Absatz 1: Datenschutz durch Technikgestaltung

2.1.1 Pflicht des Verantwortlichen, geeignete technische und organisatorische Maßnahmen und notwendige Garantien im Rahmen der Verarbeitung umzusetzen

7. Nach Artikel 25 Absatz 1 trifft der Verantwortliche *geeignete* technische und organisatorische *Maßnahmen*, die darauf abzielen, die Datenschutzgrundsätze umzusetzen und die *notwendigen Garantien* in die Verarbeitung aufzunehmen, um den Anforderungen zu genügen und die Rechte und

Freiheiten der betroffenen Personen zu schützen. Sowohl die geeigneten Maßnahmen als auch die notwendigen Garantien sollen demselben Zweck dienen, nämlich die Rechte der betroffenen Personen zu schützen und sicherzustellen, dass der Schutz ihrer personenbezogenen Daten in die Verarbeitung aufgenommen wird.

8. Als *technische und organisatorische Maßnahmen* und notwendige *Garantien* können im weiten Sinne alle Methoden oder Mittel verstanden werden, die ein Verantwortlicher bei der Verarbeitung anwenden kann. Das Kriterium der *Eignung* ist erfüllt, wenn die Maßnahmen und die notwendigen Garantien dazu dienen können, den beabsichtigten Zweck zu erreichen, d. h. die Datenschutzgrundsätze *wirksam* umzusetzen.[3] Das Erfordernis der Eignung steht daher in engem Zusammenhang mit dem Erfordernis der Wirksamkeit.

9. Als technische oder organisatorische Maßnahme und als Garantie gilt jedes Mittel, vom Einsatz fortschrittlicher technischer Lösungen bis hin zur grundlegenden Schulung von Mitarbeitern. Als Beispiele, die je nach Kontext und nach den Risiken der betreffenden Verarbeitung geeignet sein können, kommen unter anderem in Betracht: Pseudonymisierung personenbezogener Daten[4]; Speicherung personenbezogener Daten in einem strukturierten, allgemein maschinenlesbaren Format; Schaffung der Möglichkeit für betroffene Personen, in die Verarbeitung einzugreifen; Bereitstellung von Informationen über die Speicherung personenbezogener Daten; Vorhandensein von Systemen zur Erkennung von Schadsoftware; Schulung der Mitarbeiter in den Grundlagen der „Cyberhygiene"; Einführung von Managementsystemen für Datenschutz und Informationssicherheit, vertragliche Verpflichtung von Auftragsverarbeitern zur Anwendung spezifischer Datenminimierungsverfahren usw.

10. Von Verbänden und anderen Gremien anerkannte Standards, bewährte Verfahren und Verhaltensregeln können bei der Festlegung geeigneter Maßnahmen hilfreich sein. Allerdings muss der Verantwortliche prüfen, ob die Maßnahmen für die betreffende konkrete Verarbeitung geeignet sind.

2.1.2 Auslegung für die wirksame Umsetzung der Datenschutzgrundsätze und den Schutz der Rechte und Freiheiten der betroffenen Personen

11. Die *Datenschutzgrundsätze* sind in Artikel 5 dargelegt (im Folgenden „die Grundsätze"); die *Rechte und Freiheiten der betroffenen Personen* sind die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere das Recht natürlicher Personen auf den Schutz personenbezogener Daten, deren Schutz nach Artikel 1 Absatz 2 Ziel der DSGVO ist (im Folgenden „die Rechte").[5] Der genaue Wortlaut dieser Rechte kann der Charta der Grundrechte der Europäischen Union entnommen werden. Es ist unerlässlich, dass der Verantwortliche die Bedeutung *der Grundsätze* und *der Rechte* als Grundlage für den durch die DSGVO gewährleisteten Schutz versteht und insbesondere die Verpflichtung zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen kennt.

12. Bei der Umsetzung der geeigneten technischen und organisatorischen Maßnahmen sind die Maßnahmen und Garantien im Hinblick auf die wirksame Umsetzung aller vorgenannten Grundsätze und im Hinblick auf den hieraus resultierenden Schutz der Rechte *auszulegen*.

Wirksamkeit

[3] Der Aspekt der „Wirksamkeit" wird in dem Unterkapitel 2.1.2 unten behandelt.
[4] Definition in Artikel 4 Absatz 5 DSGVO.
[5] Siehe Erwägungsgrund 4 DSGVO.

13. Wirksamkeit ist der Kern des Konzepts des Datenschutzes durch Technikgestaltung. Die Anforderung zur wirksamen Umsetzung der Grundsätze bedeutet, dass die Verantwortlichen die für den Schutz dieser Grundsätze erforderlichen Maßnahmen und Garantien umsetzen müssen, um die Rechte der betroffenen Personen zu gewährleisten. Jede umgesetzte Maßnahme sollte zu den beabsichtigten Ergebnissen für die vom Verantwortlichen vorgesehene Verarbeitung führen. Aus dieser Feststellung ergeben sich zwei Konsequenzen.

14. Zum einen, dass Artikel 25 nicht die Umsetzung bestimmter technischer und organisatorischer Maßnahmen vorsieht, sondern dass die gewählten Maßnahmen und Garantien speziell für die Umsetzung der Datenschutzgrundsätze bei der betreffenden konkreten Verarbeitung angelegt sein sollten. Dabei sollte bei den Maßnahmen und Garantien die Wirksamkeit im Vordergrund stehen, und der Verantwortliche sollte weitere Maßnahmen umsetzen können, um einer etwaigen Risikoerhöhung Rechnung tragen zu können.[6] Die Wirksamkeit von Maßnahmen hängt daher von den Rahmenbedingungen der betreffenden Verarbeitung und von einer Prüfung bestimmter Aspekte ab, die bei der Festlegung der Mittel für die Verarbeitung zu berücksichtigen sind. Die vorgenannten Aspekte werden in dem Unterkapitel 2.1.3. unten behandelt.

15. Zum anderen sollten die Verantwortlichen nachweisen können, dass die Grundsätze gewahrt wurden.

16. Die umgesetzten Maßnahmen und Garantien sollten die gewünschte Wirkung in Bezug auf den Datenschutz erzielen; und der Verantwortliche sollte über eine Dokumentation der umgesetzten technischen und organisatorischen Maßnahmen verfügen.[7] Hierfür kann der Verantwortliche geeignete zentrale Leistungsindikatoren zum Nachweis der Wirksamkeit festlegen. Ein zentraler Leistungsindikator ist ein vom Verantwortlichen gewählter messbarer Wert, der Auskunft über die Wirksamkeit des Verantwortlichen bei der Erreichung seiner Datenschutzziele gibt. Die zentralen Leistungsindikatoren können *quantitativ* sein, wie z. B. der Prozentsatz von falsch-positiven oder falsch-negativen Ergebnissen, die Reduzierung von Beschwerden, die Verkürzung der Zeit für Antworten an betroffene Personen, die ihre Rechte wahrnehmen, oder *qualitativ*, wie z. B. Bewertungen der Leistung, die Verwendung von Bewertungsskalen oder Beurteilungen durch Sachverständige. Als Alternative zu den zentralen Leistungsindikatoren können die Verantwortlichen unter Umständen den Nachweis der wirksamen Umsetzung der Grundsätze dadurch erbringen, dass sie Sinn und Zweck ihrer Prüfung der Wirksamkeit der gewählten Maßnahmen und Garantien erläutern.

2.1.3 Zu berücksichtigende Aspekte

17. In Artikel 25 Absatz 1 sind die Aspekte aufgelistet, die der Verantwortliche bei der Festlegung der Maßnahmen für einen bestimmten Verarbeitungsvorgang zu berücksichtigen hat. Im Folgenden wird eine Orientierungshilfe zur Berücksichtigung dieser Aspekte im Gestaltungsprozess gegeben; hierzu gehört auch die Gestaltung der Voreinstellungen. Alle diese Aspekte tragen dazu bei, festzustellen, ob

[6] „Wesentliche Grundsätze, die für die Verantwortlichen gelten, (Legitimität, Datenminimierung, Zweckbindung, Transparenz, Datenintegrität, Datenrichtigkeit) sollten unabhängig von der Verarbeitung und den Risiken für die betroffenen Personen bestehen bleiben. Die gebührende Beachtung der Art und des Umfangs dieser Verarbeitung war jedoch stets fester Bestandteil der Anwendung dieser Grundsätze, sodass sie grundsätzlich skalierbar sind." Artikel-29-Datenschutzgruppe, „Statement on the role of a risk-based approach in data protection legal frameworks", WP 218, 30. Mai 2014, S. 3, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

[7] Siehe Erwägungsgründe 74 und 78.

eine Maßnahme für die wirksame Umsetzung der Grundsätze geeignet ist. Die einzelnen Aspekte sind daher nicht selbst das Ziel, sondern Faktoren, die für die Erreichung des Ziels zu berücksichtigen sind.

2.1.3.1 Stand der Technik

18. Das Konzept „Stand der Technik" findet sich in verschiedenen Elementen des (gemeinschaftlichen Besitzstands) (ggf. einfacher: der Rechtsvorschriften der EU?), z. B. im Umweltschutz und in der Produktsicherheit. In der DSGVO wird nicht nur in Artikel 32 hinsichtlich der Sicherheitsmaßnahmen[8, 9] auf den Stand der Technik[10] Bezug genommen, sondern auch in Artikel 25; damit wird dieser Standard auf alle technischen und organisatorischen Maßnahmen im Rahmen der Verarbeitung ausgeweitet.

19. Im Zusammenhang mit Artikel 25 wird den Verantwortlichen mit dem Verweis auf den Stand der Technik bei der Festlegung der geeigneten technischen und organisatorischen Maßnahmen die Pflicht auferlegt, **den gegenwärtigen technischen Fortschritt** auf dem Markt zu berücksichtigen. Die Verantwortlichen sind gehalten, den technischen Fortschritt zu kennen und sich diesbezüglich auf dem Laufenden zu halten; sie müssen wissen, welche datenschutzbezogenen Risiken oder Chancen die Technik für den Verarbeitungsvorgang bedeuten kann und wie die Maßnahmen und Garantien, die die *wirksame Umsetzung* der Grundsätze und der Rechte der betroffenen Personen gewährleisten,unter Berücksichtigung der in der Entwicklung befindlichen technischen Rahmenbedingungen, umzusetzen und zu aktualisieren sind.

20. Der Stand der Technik ist ein dynamisches Konzept, das nicht zu einem bestimmten Zeitpunkt statisch definiert werden kann, sondern *kontinuierlich* entsprechend dem technischen Fortschritt beurteilt werden sollte. Angesichts der technischen Fortschritte könnte ein Verantwortlicher zu der Feststellung gelangen, dass eine Maßnahme, die in der Vergangenheit ein angemessenes Schutzniveau geboten hat, dieses Niveau aktuell nicht mehr gewährleistet. Wenn sich Verantwortliche hinsichtlich der technischen Veränderungen nicht auf dem neusten Stand halten, kann dies somit eine Nichteinhaltung von Artikel 25 bedeuten.

21. Das Kriterium „Stand der Technik" gilt nicht nur für technische Maßnahmen, sondern auch für organisatorische. Das Fehlen geeigneter organisatorischer Maßnahmen kann die Wirksamkeit einer gewählten Technologie mindern oder vollständig unterminieren. Beispiele für organisatorische Maßnahmen können die Annahme interner Strategien, Schulungen nach dem neuesten Stand in Technologie, Sicherheit und Datenschutz sowie Strategien für die Steuerung und Verwaltung der IT-Sicherheit sein.

22. Bestehende und anerkannte Rahmen, Standards, Zertifizierungen, Verhaltensregeln usw. in verschiedenen Gebieten können eine Rolle bei der Festlegung des aktuellen Stands der Technik innerhalb des vorgegebenen Einsatzgebiets spielen. Wenn es derartige Standards gibt und wenn sie der betroffenen Person den Rechtsvorschriften entsprechend – oder über die Rechtsvorschriften

[8] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security
[9] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/
[10] Vgl. Kalkar-Beschluss des Bundesverfassungsgerichts aus dem Jahr 1978: Unter https://germanlawarchive.iuscomp.org/?p=67 ist eine mögliche Grundlage für eine Methode für eine objektive Definition des Konzepts zu finden. Auf dieser Grundlage würde der Stand der Technik zwischen der Ebene der „existierenden wissenschaftlichen Erkenntnisse und Forschungsergebnisse" und den etablierteren „allgemein anerkannten Technikregeln" ermittelt werden. Der Stand der Technik kann somit definiert werden als das Technikniveau einer Dienstleistung, einer Technologie oder eines Produkts, das auf dem Markt existiert und die identifizierten Ziele am wirksamsten erreicht.

hinaus – ein hohes Schutzniveau bieten, sollten die Verantwortlichen diese Standards bei der Gestaltung und der Umsetzung von Datenschutzmaßnahmen heranziehen.

2.1.3.2 Implementierungskosten

23. Der Verantwortliche kann bei der Wahl und bei der Umsetzung von geeigneten technischen und organisatorischen Maßnahmen und erforderlichen Garantien für die wirksame Umsetzung der Grundsätze zum Schutz der Rechte betroffener Personen die Kosten der Implementierung berücksichtigen. Diese Kosten beziehen sich auf Ressourcen im Allgemeinen, einschließlich Zeit und Personal.

24. Der Kostenaspekt verpflichtet den Verantwortlichen nicht dazu, einen unverhältnismäßig großen Ressourcenaufwand zu betreiben, wenn es alternative, weniger ressourcenintensive, aber dennoch wirksame Maßnahmen gibt. Die Implementierungskosten sind ein Faktor, der bei der Umsetzung des Datenschutzes durch Technikgestaltung zu berücksichtigen ist, sollten jedoch nicht als Grund dafür herangezogen werden, den Datenschutz durch Technikgestaltung nicht umzusetzen.

25. Demnach gewährleisten die gewählten Maßnahmen, dass die Verarbeitung personenbezogener Daten bei dem vom Verantwortlichen vorgesehenen Verarbeitungsvorgang, unabhängig von den Kosten, nicht gegen die Grundsätze verstößt. Die Verantwortlichen sollten die Gesamtkosten steuern können, um alle Grundsätze wirksam umsetzen und folglich die Rechte schützen zu können.

2.1.3.3 Art, Umfang, Umstände und Zweck der Verarbeitung

26. Die Verantwortlichen müssen bei der Festlegung der erforderlichen Maßnahmen Art, Umfang, Umstände und Zweck der Verarbeitung berücksichtigen.

27. Diese Faktoren sind durchgängig in Einklang mit ihrer Bedeutung in anderen Bestimmungen der DSGVO z. B. den Artikeln 24, 32 und 35 auszulegen; Ziel ist es, die Datenschutzgrundsätze durch Technikgestaltung in die Verarbeitung einzubeziehen.

28. Zusammenfassend ist festzuhalten, dass unter der **Art der Verarbeitung** die der Verarbeitung innewohnenden[11] Eigenschaften verstanden werden können. Der **Umfang der Verarbeitung** bezieht sich auf das Ausmaß und den Bereich der Verarbeitung. Die **Umstände der Verarbeitung** beziehen sich auf die Bedingungen der Verarbeitung, die sich auf die Erwartungen der betroffenen Personen auswirken können, während der **Zweck der Verarbeitung** auf die Ziele der Verarbeitung abhebt.

2.1.3.4 Unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen

29. Die DSGVO verfolgt in vielen ihrer Bestimmungen, in den Artikeln 24, 25, 32 und 35, einen kohärenten risikobasierten Ansatz, mit dem Ziel, geeignete technische und organisatorische Maßnahmen zum Schutz natürlicher Personen, zum Schutz ihrer personenbezogenen Daten und zur Erfüllung der Anforderungen der DSGVO zu ermitteln. Die Schutzobjekte sind stets dieselben (natürliche Personen, über den Schutz ihrer personenbezogenen Daten); sie werden vor denselben Risiken (für die Rechte

[11] Beispiele hierfür sind besondere Kategorien persönlicher Daten, automatische Entscheidungsfindung, asymmetrische Machtverhältnisse, unvorhersehbare Verarbeitung, Schwierigkeiten der betroffenen Person, ihre Rechte wahrzunehmen.

natürlicher Personen) geschützt, wobei dieselben Bedingungen (Art, Umfang, Umstände und Zweck der Verarbeitung) berücksichtigt werden.

30. Bei der Durchführung der Risikoanalyse zur Einhaltung von Artikel 25 muss der Verantwortliche die Risiken für die Rechte betroffener Personen ermitteln, die mit einem Verstoß gegen die Grundsätze verbunden sind, und die Eintrittswahrscheinlichkeit und Schwere dieser Risiken bestimmen, um Maßnahmen zur wirksamen Minderung der festgestellten Risiken umzusetzen. Eine systematische und gründliche Bewertung der Verarbeitung ist bei der Risikobewertung von zentraler Bedeutung. Beispiel: Im Zuge der Verarbeitung personenbezogener Daten von Kindern und Jugendlichen unter 18 Jahren als schutzbedürftiger Gruppe beurteilt ein Verantwortlicher in einem Fall, in dem es keine andere Rechtsgrundlage gibt, die konkreten Risiken, die mit dem Fehlen einer freiwillig erteilten Einwilligung, einem Verstoß gegen den Grundsatz der Rechtmäßigkeit, verbunden sind, und setzt geeignete Maßnahmen für den Umgang mit den festgestellten Risiken für diese Gruppe von betroffenen Personen und für die wirksame Minderung dieser Risiken um.

31. Die „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA)“ des EDSA[12], die schwerpunktmäßig die Feststellung behandeln, ob ein Verarbeitungsvorgang voraussichtlich mit einem hohen Risiko für die betroffene Person verbunden ist oder nicht, geben auch Hilfestellung für die Bewertung von Datenschutzrisiken und für die Durchführung solcher Bewertungen. Diese Leitlinien können auch bei der Risikobewertung nach allen vorstehend genannten Artikeln, unter anderem Artikel 25, von Nutzen sein.

32. Der risikobasierte Ansatz schließt nicht aus, dass Basisszenarien, bewährte Verfahren und Standards zum Einsatz kommen. Diese Mittel könnten den Verantwortlichen beim Umgang mit ähnlichen Risiken in ähnlichen Situationen (Art, Umfang, Umstände und Zweck der Verarbeitung) als nützliches Instrumentarium dienen. Dennoch bleibt die Pflicht nach Artikel 25, (sowie nach den Artikeln 24, 32 und 35 Absatz 7 Buchstabe c) die *unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen* zu berücksichtigen, bestehen. Daher müssen die Verantwortlichen, auch wenn sie diese Hilfsmittel zur Unterstützung nutzen, stets eine Einzelfallbewertung der mit der jeweiligen Verarbeitungstätigkeit verbundenen Datenschutzrisiken durchführen und die Wirksamkeit der vorgeschlagenen geeigneten Maßnahmen und Garantien überprüfen. Anschließend kann zusätzlich eine DSFA bzw. eine Aktualisierung einer bestehenden DSFA erforderlich sein.

2.1.4 Der zeitliche Aspekt

2.1.4.1 Zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung

33. Der Datenschutz durch Technikgestaltung wird „*zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung*“ umgesetzt.

34. Die „*Mittel für die Verarbeitung*“ reichen von allgemeinen bis zu detaillierten Gestaltungselementen der Verarbeitung und schließen z. B. Architektur, Verfahren und Protokolle, Layout und Erscheinungsbild ein.

[12] Artikel-29-Datenschutzgruppe, „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 ´wahrscheinlich ein hohes Risiko mit sich bringt`“, WP 248 Rev. 01, 4. Oktober 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48464 – gebilligt durch den EDSA.

35. Der „*Zeitpunkt der Festlegung der Mittel für die Verarbeitung*“ bezieht sich auf den Zeitraum, in dem der Verantwortliche entscheidet, wie die Verarbeitung durchgeführt wird, wie die Verarbeitung abläuft und welche Mechanismen für die Durchführung der Verarbeitung genutzt werden. Im Rahmen dieses Prozesses muss der Verantwortliche prüfen, welche Maßnahmen und Garantien für die wirksame Umsetzung der Grundsätze und Rechte der betroffenen Personen bei der Verarbeitung geeignet sind, und Aspekte wie den Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zweck sowie Risiken berücksichtigen. Hierzu gehört auch die Zeit für die Beschaffung und Einrichtung von Anwendungsprogrammen, Geräten und Diensten für die Datenverarbeitung.

36. Die frühzeitige Berücksichtigung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ist für eine erfolgreiche Umsetzung der Grundsätze und für den erfolgreichen Schutz der Rechte der betroffenen Personen von zentraler Bedeutung. Zudem liegt es unter dem Gesichtspunkt von Kosten und Nutzen ebenfalls im Interesse der Verantwortlichen, den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen eher früher als später zu berücksichtigen, da Änderungen an Plänen, die bereits aufgestellt worden sind, und an Verarbeitungsvorgängen, die bereits gestaltet worden sind, schwierig und kostenintensiv sein können.

2.1.4.2 Zeitpunkt der eigentlichen Verarbeitung (Beibehaltung und Überprüfung der Datenschutzanforderungen)

37. Nach dem Beginn der Verarbeitung bleibt der Verantwortliche stets verpflichtet, den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, d. h. die kontinuierliche wirksame Umsetzung der Grundsätze zum Schutz der Rechte, aufrechtzuerhalten, sich über den aktuellen Stand der Technik auf dem Laufenden zu halten, das Ausmaß des Risikos neu zu bewerten usw. Art, Umfang und Umstände der Verarbeitungsvorgänge sowie das Risiko können sich im Laufe der Verarbeitung verändern, weshalb der Verantwortliche seine Verarbeitungsvorgänge durch regelmäßige Überprüfungen und Beurteilungen der Wirksamkeit der von ihm gewählten Maßnahmen und Garantien neu beurteilen muss.

38. Die Verpflichtung zur Wartung, Überprüfung und, bei Bedarf, Aktualisierung des Verarbeitungsvorgangs erstreckt sich auch auf bereits bestehende Systeme. Dies bedeutet, dass bestehende Systeme, die vor Inkrafttreten der DSGVO gestaltet wurden, überprüft und gewartet werden müssen, um sicherzustellen, dass Maßnahmen und Garantien zur wirksamen Umsetzung der Grundsätze und der Rechte von betroffenen Personen in Einklang mit diesen Leitlinien angewandt werden.

39. Diese Verpflichtung erstreckt sich auch auf etwaige Verarbeitungen durch Auftragsverarbeiter. Die Verantwortlichen sollten die von Auftragsverarbeitern ausgeführten Verarbeitungsvorgänge regelmäßig überprüfen und beurteilen, um sicherzustellen, dass die Grundsätze bei diesen Vorgängen kontinuierlich eingehalten werden können, und damit der für die Datenverarbeitung Verantwortliche seine diesbezüglichen Pflichten erfüllen kann.

2.2 Artikel 25 Absatz 2: Datenschutz durch datenschutzfreundliche Voreinstellungen

2.2.1 Durch Voreinstellung werden grundsätzlich nur personenbezogene Daten verarbeitet, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist

40. Eine "Voreinstellung", wie sie in der Informatik üblicherweise definiert wird, bezieht sich auf den bereits bestehenden oder vorausgewählten Wert einer konfigurierbaren Einstellung, die einer

Anwendungssoftware, einem Computerprogramm oder einem Gerät zugewiesen wird. Diese Einstellungen werden vor allem bei elektronischen Geräten auch „Voreinstellungen“ oder „Werkseinstellungen“ genannt.

41. Der Begriff „durch Voreinstellung“ bezeichnet im Zusammenhang mit der Verarbeitung personenbezogener Daten Entscheidungen über Konfigurationswerte oder Verarbeitungsoptionen, die in einem Verarbeitungssystem z. B. einem Anwendungsprogramm, Dienst oder Gerät eingestellt oder vorgeschrieben sind, oder in einem manuellen Verarbeitungsverfahren, das die Menge der erhobenen personenbezogenen Daten, den Umfang der Verarbeitung, die Speicherfrist und die Zugänglichkeit dieser Daten beeinflusst.

42. Der Verantwortliche sollte die Voreinstellungen und Optionen für die Verarbeitung so auswählen, dass nur die Verarbeitung standardmäßig ausgeführt wird, die unbedingt erforderlich ist, um den vorgegebenen rechtmäßigen Zweck zu erreichen; der Verantwortliche ist für die Vornahme dieser Voreinstellungen verantwortlich. Die Verantwortlichen sollten sich hierbei auf ihre Einschätzung der Notwendigkeit der Verarbeitung im Hinblick auf die Rechtsgrundlagen nach Artikel 6 Absatz 1 stützen. Dies bedeutet, dass der Verantwortliche standardmäßig nicht mehr Daten als notwendig erhebt, die erhobenen Daten nicht weiter als für seine Zwecke notwendig verarbeitet und sie auch nicht länger als notwendig speichert. Die grundlegende Anforderung lautet, den Datenschutz durch Voreinstellungen in die Verarbeitung einzubinden.

43. Der Verantwortliche muss zuvor festlegen, für welche festgelegten, eindeutigen und legitimen Zwecke die personenbezogenen Daten erhoben und verarbeitet werden.[13] Die Maßnahmen müssen standardmäßig geeignet sein sicherzustellen, dass nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen spezifischen Verarbeitungszweck erforderlich ist. Die Leitlinien des EDSB für die Beurteilung der Erforderlichkeit und der Verhältnismäßigkeit von Maßnahmen, die das Recht auf den Schutz personenbezogener Daten einschränken, können auch bei der Entscheidung darüber hilfreich sein, welche Daten verarbeitet werden müssen, um einen bestimmten Zweck zu erreichen.[14, 15, 16]

44. Wenn der Verantwortliche Anwendungsprogramme von Dritten oder handelsübliche Anwendungsprogramme verwendet, sollte er eine Risikobewertung des Produkts durchführen und sicherstellen, dass Funktionen, die keine Rechtsgrundlage haben bzw. die mit dem beabsichtigten Zweck der Verarbeitung nicht vereinbar sind, ausgeschaltet sind.

45. Dieselben Erwägungen gelten für organisatorische Maßnahmen, die die Verarbeitungsvorgänge unterstützen. Sie sollten so gestaltet sein, dass sie von Anfang an nur die kleinste Menge personenbezogener Daten, die für die spezifischen Zwecke unbedingt erforderlich ist, verarbeiten.

[13] Artikel 5 Absatz 1 Buchstaben b bis e DSGVO.
[14] EDSB, „Guidelines on assessing the necessity and proportionality of measures that limit the right to data protection“, 25. Februar 2019, edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf.
[15] Siehe auch EDSB, „Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken: Ein Toolkit”, https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_de.
[16] Nähere Informationen über die Erforderlichkeit, siehe Artikel-29-Datenschutzgruppe, „Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG“, WP 217, 9. April 2014, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_de.pdf.

Dies sollte insbesondere bei der Gewährung des Datenzugriffs für Mitarbeiter mit unterschiedlichen Aufgaben und unterschiedlichen Zugriffsanforderungen berücksichtigt werden.

46. Der Ausdruck geeignete „technische und organisatorische Maßnahmen“ hat daher im Zusammenhang mit dem Datenschutz durch datenschutzfreundliche Voreinstellungen die gleiche Bedeutung wie in den Ausführungen im Unterkapitel 2.1.1 oben, findet jedoch konkret auf den Grundsatz der Datenminimierung Anwendung.

47. Die vorgenannte Verpflichtung, nur personenbezogene Daten zu verarbeiten, die für die einzelnen konkreten Zwecke erforderlich sind, gilt für die folgenden Aspekte:

2.2.2 Dimensionen der Verpflichtung zur Datenminimierung

48. In Artikel 25 Absatz 2 sind die Dimensionen der Verpflichtung zur Datenminimierung bei voreingestellter Verarbeitung aufgeführt; hierzu wird festgestellt, dass sich die Verpflichtung auf die Menge der erhobenen personenbezogenen Daten, auf den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit bezieht.

2.2.2.1 Menge der erhobenen personenbezogenen Daten

49. Die Verantwortlichen sollten sowohl die Menge der personenbezogenen Daten als auch die Arten und Kategorien und den Detailgrad der personenbezogenen Daten berücksichtigen, die für die Zwecke der Verarbeitung erforderlich sind. Bei ihren Entscheidungen über die Auslegung sollten sie die erhöhten Risiken für die Grundsätze der Vollständigkeit und Vertraulichkeit, der Datenminimierung und Speicherbegrenzung bei der Erhebung großer Mengen detaillierter personenbezogener Daten berücksichtigen und diese Risiken der Verringerung der Risiken bei der Erhebung von kleineren Mengen von Daten und/oder von weniger stark untergliederten Informationen über betroffene Personen gegenüberstellen. In jedem Fall beinhaltet die Voreinstellung nicht die Erhebung von personenbezogenen Daten, die für den konkreten Verarbeitungszweck nicht notwendig sind. Mit anderen Worten, wenn bestimmte Kategorien von personenbezogenen Daten oder wenn detaillierte Daten nicht notwendig sind, weil weniger detaillierte Daten ausreichen, dürfen keine überschüssigen personenbezogenen Daten erhoben werden.

50. Die gleichen Anforderungen an die Voreinstellung gelten für Dienste, unabhängig davon, welche Plattform oder welches Gerät verwendet wird; es dürfen nur die für den bestimmten Zweck erforderlichen personenbezogenen Daten erhoben werden.

2.2.2.2 Umfang ihrer Verarbeitung

51. Die Verarbeitungsvorgänge,[17] die bei personenbezogenen Daten durchgeführt werden, sind auf das Notwendige zu beschränken. Zur Erfüllung eines Verarbeitungszwecks können viele Verarbeitungsvorgänge beitragen. Die Tatsache, dass bestimmte personenbezogene Daten zur Erfüllung eines Zwecks erforderlich sind, bedeutet jedoch nicht, dass die Daten allen Arten und Häufigkeiten von Verarbeitungsvorgängen unterzogen werden können. Die Verantwortlichen sollten außerdem darauf achten, die Grenzen dessen, was als zu vereinbarende Zwecke nach Artikel 6

[17] Laut Artikel 4 Absatz 2 DSGVO umfasst dies das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Absatz 4 gilt, nicht auszudehnen, und berücksichtigen, welche Verarbeitung den angemessenen Erwartungen der betroffenen Personen entspricht.

2.2.2.3 Speicherfrist

52. Erhobene personenbezogene Daten werden nicht gespeichert, wenn es zum Zweck der Verarbeitung nicht erforderlich ist und wenn es keinen anderen mit dem Verarbeitungszweck zu vereinbarenden Zweck und keine Rechtsgrundlage gibt (Artikel 6 Absatz 4). Jede Speicherung sollte der für die Datenverarbeitung Verantwortliche in Einklang mit dem Grundsatz der Rechenschaftspflicht objektiv als erforderlich rechtfertigen können.

53. Der Verantwortliche grenzt die Speicherfrist auf den für den Zweck erforderlichen Zeitraum ein. Wenn die personenbezogenen Daten für den Verarbeitungszweck nicht mehr notwendig sind, werden sie standardmäßig gelöscht oder anonymisiert. Die Dauer der Speicherfrist richtet sich daher nach dem jeweiligen Verarbeitungszweck. Diese Verpflichtung steht in direktem Zusammenhang zu dem Grundsatz der Speicherbegrenzung nach Artikel 5 Absatz 1 Buchstabe e und wird standardmäßig erfüllt; dies bedeutet, dass der Verantwortliche systematische Verfahren für die Löschung oder Anonymisierung von Daten in den Verarbeitungsvorgang einbinden sollte.

54. Die Anonymisierung[18] personenbezogener Daten kann alternativ zur Löschung eingesetzt werden, sofern alle relevanten kontextuellen Elemente berücksichtigt werden und die Eintrittswahrscheinlichkeit und Schwere des Risikos, einschließlich des Risikos der Wiedererkennung, regelmäßig bewertet werden.[19]

2.2.2.4 Zugänglichkeit

55. Der Verantwortliche sollte den Personenkreis, der Zugang zu den personenbezogenen Daten hat, und die jeweilige Art des Zugangs auf der Grundlage einer Beurteilung der Notwendigkeit festlegen; er sollte auch sicherstellen, dass die personenbezogenen Daten bei Bedarf denjenigen, die sie z. B. in kritischen Situationen benötigen, tatsächlich zugänglich sind. Die Zugangskontrollen sollten für die gesamte Datenübermittlung während der Verarbeitung gewährleistet sein.

56. In Artikel 25 Absatz 2 ist ferner festgelegt, dass personenbezogene Daten nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl natürlicher Personen zugänglich gemacht werden dürfen. Der Verantwortliche beschränkt die Zugänglichkeit durch Voreinstellung und gibt der betroffenen Person die Möglichkeit einzugreifen, bevor ihre personenbezogenen Daten veröffentlicht oder einer unbestimmten Zahl natürlicher Personen zugänglich gemacht werden.

57. Die Bereitstellung personenbezogener Daten für eine unbestimmte Zahl von Personen kann dazu führen, dass die Daten über die ursprüngliche Absicht hinaus verbreitet werden. Dies ist insbesondere im Zusammenhang mit dem Internet und Suchmaschinen relevant. Die Verantwortlichen sollten daher betroffenen Personen standardmäßig die Möglichkeit geben einzugreifen, bevor personenbezogene

[18] Artikel-29-Datenschutzgruppe, „Stellungnahme 5/2014 zu Anonymisierungstechniken“, WP 216, 10. April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf.

[19] Vgl. Artikel 4 Absatz 1 DSGVO, Erwägungsgrund 26 DSGVO, Artikel-29-Datenschutzgruppe, „Stellungnahme 5/2014 zu Anonymisierungstechniken“. Vgl. außerdem das Unterkapitel über Speicherbegrenzung in Kapitel 3 dieses Dokuments, in dem von der Notwendigkeit die Rede ist, dass die Verantwortlichen die Wirksamkeit der umgesetzten Anonymisierungstechnik(en) sicherstellen.

Daten im offenen Internet verbreitet werden. Dies ist besonders wichtig, wenn Kinder und schutzbedürftige Gruppen betroffen sind.

58. In Abhängigkeit von der Rechtsgrundlage für die Verarbeitung könnten die Möglichkeiten des Eingreifens je nach Verarbeitungskontext variieren. Beispiele hierfür sind die Einholung einer Einwilligung in die Bereitstellung personenbezogener Daten für die Öffentlichkeit oder die Nutzung von Einstellungen zum Schutz der Privatsphäre, damit die betroffenen Personen den Zugang der Öffentlichkeit selbst kontrollieren können.

59. Selbst wenn personenbezogene Daten mit der Einwilligung und dem Wissen einer betroffenen Person öffentlich zugänglich gemacht werden, bedeutet das nicht, dass jeder andere Verantwortliche, der Zugang zu den personenbezogenen Daten hat, diese Daten selbst uneingeschränkt für seine eigenen Zwecke verarbeiten darf. Hierfür bedarf der Betreffende einer gesonderten Rechtsgrundlage.[20]

3 UMSETZUNG DER DATENSCHUTZGRUNDSÄTZE BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN IM WEGE DES DATENSCHUTZES DURCH TECHNIKGESTALTUNG UND DURCH DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

60. Der Verantwortliche sollte in allen Phasen der Gestaltung der Verarbeitungstätigkeiten, einschließlich Auftragsvergabe, Ausschreibungen, Outsourcing, Entwicklung, Unterstützung, Wartung, Erprobung, Speicherung, Löschung usw., die verschiedenen Aspekte des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigen und prüfen. Zur Veranschaulichung werden in diesem Kapitel Beispiele hierfür im Zusammenhang mit der Umsetzung der Grundsätze angeführt.[21, 22, 23]

61. Die Verantwortlichen müssen die Grundsätze umsetzen, um Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu gewährleisten. Zu diesen Grundsätzen gehören Transparenz, Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie die Rechenschaftspflicht. Diese Grundsätze sind in Artikel 5 und im Erwägungsgrund 39 der DSGVO dargelegt. Um die Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen umfassend verstehen zu können, wird betont, wie wichtig es ist, die Bedeutung der einzelnen Grundsätze zu erfassen.

62. Bei der Vorstellung von Beispielen für die Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen wurden zu den einzelnen Grundsätzen jeweils **zentrale Aspekte des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen** zusammengestellt. Die Beispiele werfen ein Schlaglicht auf den jeweiligen konkreten Datenschutzgrundsatz; hierbei kann es aber auch zu Überschneidungen mit anderen Grundsätzen kommen, die in einem engen Zusammenhang zu den jeweils betrachteten Grundsätzen stehen. Der

[20] Vgl. Rechtssache Nr. 931/13, Satakunnan Markkinapörssi Oy und Satamedia Oy/Finnland.
[21] Weitere Beispiele finden sich hier: Norwegische Datenschutzbehörde, „Software development with Data Protection by Design and by Default“, 28. November 2017, www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729.
[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers
[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

EDSA betont, dass die zentralen Aspekte und die im Folgenden beschriebenen Beispiele weder erschöpfend noch verbindlich sind, sondern lediglich als Richtschnur für die einzelnen Grundsätze gedacht sind. Die Verantwortlichen müssen prüfen, wie die Wahrung der Grundsätze bei dem jeweiligen konkreten Verarbeitungsvorgang zu gewährleisten ist.

63. Im Mittelpunkt dieses Kapitels steht die Umsetzung der Grundsätze; die Verantwortlichen sollten jedoch zudem ebenfalls in Einklang mit Kapitel III der DSGVO *geeignete und wirksame* Mittel zum Schutz der Rechte betroffener Personen anwenden, sofern dies nicht bereits durch die Grundsätze selbst vorgeschrieben ist.

64. Der Grundsatz der Rechenschaftspflicht gilt übergreifend: Hiernach ist der Verantwortliche bei der Wahl der erforderlichen technischen und organisatorischen Maßnahmen zu verantwortlichem Handeln verpflichtet.

3.1 Transparenz[24]

65. Der Verantwortliche muss der betroffenen Person gegenüber klar und offen darlegen, wie er personenbezogene Daten erhebt, verwendet und weitergibt. Transparenz bedeutet, die betroffenen Personen in die Lage zu versetzen, ihre Rechte nach den Artikeln 15 bis 22 zu verstehen und gegebenenfalls auszuüben. Der Grundsatz ist in den Artikeln 12, 13, 14 und 34 verankert. Die zur Unterstützung des Grundsatzes der Transparenz umgesetzten Maßnahmen und Garantien sollten darüber hinaus die Umsetzung dieser Artikel unterstützen.

66. Beispiele für zentrale Aspekte der Technikgestaltung und der Voreinstellung in Bezug auf den Grundsatz der Transparenz:

- Klarheit – Die Informationen sind in klarer, deutlicher, präziser und verständlicher Sprache zu verfassen.
- Semantik – Die Kommunikation sollte für die betreffende Zielgruppe in ihrer Bedeutung klar sein.
- Zugänglichkeit – Die Informationen sind für die betroffene Person leicht zugänglich.
- Kontext – Die Informationen sollten zum maßgeblichen Zeitpunkt und in der geeigneten Form bereitgestellt werden.
- Relevanz – Die Informationen sollten relevant und für die konkrete betroffene Person zutreffend sein.
- Universelle Gestaltung – Die Informationen sind für alle betroffenen Personen zugänglich; dies beinhaltet die Verwendung maschinenlesbarer Sprache, um Lesbarkeit und Klarheit zu fördern und zu automatisieren.
- Verständlichkeit – Die betroffenen Personen sollten ein angemessenes Verständnis davon haben, was sie in Bezug auf die Verarbeitung ihrer personenbezogenen Daten erwarten können; dies gilt insbesondere dann, wenn es sich bei den betroffenen Personen um Kinder oder um andere schutzbedürftige Gruppen handelt.
- Nutzung mehrerer Kommunikationswege – Die Informationen sollten über verschiedene Kanäle und Medien, nicht nur Textmedien, bereitgestellt werden, um die Wahrscheinlichkeit zu erhöhen, dass die Informationen die betroffene Person tatsächlich erreichen.

[24] Eine Erläuterung zum Verständnis des Konzepts der Transparenz findet sich hier: Artikel-29-Datenschutzgruppe, „Leitlinien für Transparenz gemäß der Verordnung 2016/679“, WP 260 rev.01, 11. April 2018, https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Guidelines/WP260_LeitlinienFuerDieTransparenz.html – gebilligt durch den EDSA.

- Mehrstufige Kommunikation – Die Informationen sollten in mehreren Stufen vermittelt werden, so dass das Spannungsverhältnis zwischen Vollständigkeit und Verständnis aufgehoben wird, wobei den berechtigten Erwartungen der betroffenen Personen Rechnung zu tragen ist.

Beispiel[25]

Ein Verantwortlicher entwickelt eine Datenschutzerklärung auf seiner Website, um die Transparenzanforderungen zu erfüllen. Die Datenschutzerklärung sollten keine zu umfangreichen Informationen beinhalten, die die durchschnittliche betroffene Person nur mit Mühe erfassen und verstehen kann. Die Bestimmungen sind klar und knapp abzufassen und sollten es dem Nutzer der Website leichter machen zu verstehen, wie seine personenbezogenen Daten verarbeitet werden. Der Verantwortliche stellt daher die Informationen in mehreren Stufen bereit und hebt die wichtigsten Punkte hervor. Ausführlichere Informationen sind leicht zugänglich zur Verfügung zu stellen. Erläuterungen zu verschiedenen in den Datenschutzbestimmungen genannten Punkten und Konzepten können über Drop-down-Menüs und Links zu anderen Seiten abgerufen werden. Der Verantwortliche stellt zudem sicher, dass die Informationen über mehrere Kommunikationswege verbreitet werden, wobei die wichtigsten Punkte der schriftlichen Informationen in Videos erläutert werden. Synergieeffekte zwischen den verschiedenen Seiten sind von entscheidender Bedeutung, um sicherzustellen, dass das Konzept der Mehrstufigkeit keine zusätzliche Verwirrung, sondern vielmehr Klarheit schafft.

Der Zugang zur Datenschutzerklärung sollte für die betroffenen Personen unproblematisch sein. Dies bedeutet, dass die Datenschutzbestimmungen auf allen Seiten der betreffenden Website zugänglich gemacht und angezeigt werden, so dass die betroffene Person die Informationen stets durch einen einfachen Klick abrufen kann. Die bereitgestellten Informationen werden auch in Einklang mit den bewährten Verfahrensweisen und Standards der universellen Gestaltung gestaltet, damit sie für alle zugänglich sind.

Ferner sollten die erforderlichen Informationen zum passenden Zeitpunkt und im richtigen Zusammenhang bereitgestellt werden. Da der Verantwortliche zahlreiche Verarbeitungsvorgänge unter Nutzung der auf der Website erhobenen Daten ausführt, sind die Transparenzanforderungen nicht erfüllt, wenn er es auf seiner Website lediglich bei allgemeinen Datenschutzbestimmungen belässt. Der Verantwortliche gestaltet daher einen Informationsablauf, der die Bereitstellung der relevanten Informationen jeweils im passenden Kontext für die betroffene Person vorsieht, z. B. in Form von Kurzzusammenfassungen oder in Pop-up-Fenstern. Beispielsweise informiert der Verantwortliche die betroffene Person, wie die personenbezogenen Daten verarbeitet werden und warum die personenbezogenen Daten für die Verarbeitung notwendig sind, wenn die betroffene Person zur Eingabe personenbezogener Daten aufgefordert wird.

3.2 Rechtmäßigkeit

67. Der Verantwortliche muss eine gültige Rechtsgrundlage für die Verarbeitung personenbezogener Daten festlegen. Die Maßnahmen und Garantien sollten die Anforderung unterstützen,

[25] Die französische Datenschutzbehörde hat mehrere Beispiele zur Veranschaulichung von bewährten Verfahrensweisen für die Information von Nutzern wie auch für andere Transparenzgrundsätze veröffentlicht: https://design.cnil.fr/en/.

sicherzustellen, dass der gesamte Verarbeitungslebenszyklus im Einklang mit den entsprechenden Rechtsgrundlagen für die Verarbeitung steht.

68. Beispiele für zentrale Aspekte der Technikgestaltung und der Voreinstellung in Bezug auf die Rechtmäßigkeit:
    - Relevanz – Für die Verarbeitung ist die korrekte Rechtsgrundlage heranzuziehen.
    - Differenzierung[26] – Bei der Rechtsgrundlage ist nach den einzelnen Verarbeitungstätigkeiten zu differenzieren.
    - Zweckbestimmung – Die entsprechende Rechtsgrundlage muss in einem klaren Zusammenhang zu dem konkreten Zweck der Verarbeitung stehen.[27]
    - Notwendigkeit – Der Verarbeitungszweck ist rechtmäßig, wenn die Verarbeitung notwendig ist und nicht an Bedingungen geknüpft ist.
    - Autonomie – Die betroffene Person sollte die Kontrolle über die personenbezogenen Daten im Rahmen der Rechtsgrundlage so autonom wie möglich ausüben können.
    - Einholung der Einwilligung – Die Einwilligung muss freiwillig für den bestimmten Fall, in Kenntnis der Sachlage und unmissverständlich erteilt werden.[28] Besondere Aufmerksamkeit sollte der Frage gewidmet werden, ob Kinder und Jugendliche in der Lage sind, ihren Willen in Kenntnis der Sachlage zu bekunden.
    - Widerruf der Einwilligung – Wenn eine Einwilligung Rechtsgrundlage für die Verarbeitung ist, sollte es bei der Verarbeitung möglich sein, die Einwilligung zu widerrufen. Ein Widerruf der Einwilligung ist so einfach zu ermöglichen wie ihre Erteilung. Andernfalls erfüllt das Einwilligungsverfahren des Verantwortlichen die Bestimmungen der DSGVO nicht.[29]
    - Interessenabwägung – Wenn berechtigte Interessen die Rechtsgrundlage sind, muss der Verantwortliche eine ausgewogene Interessenabwägung vornehmen und dabei insbesondere das Ungleichgewicht der Kräfte berücksichtigen, vor allem dann, wenn Kinder im Alter von bis zu 18 Jahren und andere schutzbedürftige Gruppen betroffen sind. Es werden Maßnahmen und Garantien zur Reduzierung der negativen Auswirkungen auf die betroffenen Personen umgesetzt.
    - Vorherige Festlegung – Die Rechtsgrundlage wird vor der Verarbeitung festgelegt.
    - Wegfall der Rechtsgrundlage – Ein Wegfall der Rechtsgrundlage hat die Einstellung der Verarbeitung zur Folge.
    - Anpassung – Bei einer gültigen Änderung der Rechtsgrundlage für die Verarbeitung muss die konkrete Verarbeitung der neuen Rechtsgrundlage angepasst werden.[30]
    - Aufteilung der Zuständigkeiten – Falls eine gemeinsame Verantwortlichkeit für die Verarbeitung vorgesehen ist, müssen die Parteien ihre jeweiligen Zuständigkeiten der betroffenen Person gegenüber klar und transparent machen und die Maßnahmen für die Verarbeitung entsprechend dieser Zuständigkeitsverteilung gestalten.

Beispiel

[26] EDSA, „Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen“, Version 2.0, 8. Oktober 2019, edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_de.pdf.

[27] Siehe nachstehendes Kapitel über die Zweckbindung.

[28] Siehe „Guidelines 05/2020 on consent under Regulation 2016/679“, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.

[29] Siehe „Guidelines 05/2020 on consent under Regulation 2016/679“, S. 24, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.

[30] Falls die ursprüngliche Rechtsgrundlage eine Einwilligung ist, siehe „Guidelines 05/2020 on consent under Regulation 2016/679“, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.

Eine Bank beabsichtigt, eine Dienstleistung zur Verbesserung der Effizienz bei der Verwaltung von Kreditanträgen anzubieten. Im Rahmen dieser Dienstleistung soll es der Bank auf der Grundlage des vom Kunden eingeholten Einverständnisses möglich sein, Daten über den Kunden unmittelbar bei den staatlichen Steuerbehörden abzufragen. Die Verarbeitung personenbezogener Daten aus anderen Quellen wird in diesem Beispiel nicht berücksichtigt.

Die Erhebung personenbezogener Daten über die finanzielle Situation der betroffenen Person ist erforderlich, um auf Ersuchen der betroffenen Person vor dem Abschluss eines Kreditvertrags entsprechende Schritte einzuleiten.[31] Die Erhebung personenbezogener Daten unmittelbar bei der Steuerbehörde wird jedoch nicht für notwendig erachtet, da der Kunde einen Vertrag schließen kann, indem er selbst die bei der Steuerbehörde vorhandenen Angaben macht. Die Bank mag zwar ein berechtigtes Interesse daran haben, die Dokumentation direkt von der Steuerbehörde zu erlangen, um beispielsweise eine effiziente Kreditbearbeitung sicherzustellen, doch stellt die Eröffnung eines solchen direkten Zugangs zu den personenbezogenen Daten von Antragstellern für Banken ein Risiko für die Nutzung oder den potenziellen Missbrauch der Zugangsrechte dar.

Der Verantwortliche stellt bei der Umsetzung des Grundsatzes der Rechtmäßigkeit fest, dass er in diesem Zusammenhang die Rechtsgrundlage, dass die Verarbeitung „für die Vertragserfüllung notwendig ist“, auf den Teil der Verarbeitung von direkt bei den Steuerbehörden einzuholenden personenbezogenen Daten nicht anwenden kann. Die Tatsache, dass diese konkrete Verarbeitung das Risiko in sich birgt, dass die betroffene Person in geringerem Maße in die Verarbeitung ihrer personenbezogenen Daten eingebunden ist, ist auch für die Beurteilung der Rechtsmäßigkeit der eigentlichen Verarbeitung relevant. Die Bank kommt zu dem Schluss, dass für diesen Teil der Verarbeitung eine andere Rechtsgrundlage heranzuziehen ist. Die nationalen Rechtsvorschriften des betreffenden Mitgliedstaats, in dem der Verantwortliche seinen Sitz hat, ermöglichen es der Bank, Informationen direkt bei den staatlichen Steuerbehörden zu erheben, wenn die betroffene Person hierzu zuvor ihre Einwilligung erteilt hat.

Die Bank stellt daher auf der Online-Plattform Informationen über die Verarbeitung bereit, denen betroffene Personen problemlos entnehmen können, welche Verarbeitung unbedingt erforderlich ist und welche optional ist. Die Verarbeitungsoptionen erlauben standardmäßig keine direkte Datengewinnung aus anderen Quellen als von der der betroffenen Person selbst. Darüber hinaus wird die Option der direkten Einholung von Informationen so präsentiert, dass die betroffene Person nicht davon abgehalten wird, zu widersprechen. Die Erteilung der Zustimmung, Daten direkt von anderen Verantwortlichen einzuholen, ist ein vorübergehendes Zugangsrecht zu einem bestimmten Datensatz.

Die Zustimmungen werden elektronisch verarbeitet und dokumentiert. Den betroffenen Personen wird außerdem die Möglichkeit gegeben, ihre Zustimmungen leicht zu kontrollieren und diese zu widerrufen.

Der Verantwortliche hat diese Anforderungen zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zuvor geprüft und bezieht alle diese Kriterien in seine Anforderungsspezifikationen für die Ausschreibung zur Beschaffung der Plattform ein. Dem Verantwortlichen ist bewusst, dass, wenn er die Anforderungen an den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen nicht in der Ausschreibung nennt, die nachträgliche Umsetzung des Datenschutzes entweder zu spät ist oder sehr kostenaufwändig wird.

[31] Vgl. Artikel 6 Absatz 1 Buchstabe b DSGVO.

3.3 Verarbeitung nach Treu und Glauben

69. Die Verarbeitung nach Treu und Glauben ist ein übergeordneter Grundsatz, nach dem personenbezogene Daten nicht auf eine Weise verarbeitet werden dürfen, die für die betroffene Person in nicht gerechtfertigter Weise schädlich, widerrechtlich diskriminierend, unerwartet oder irreführend ist. Die Maßnahmen und Garantien zur Umsetzung des Grundsatzes der Verarbeitung nach Treu und Glauben unterstützen auch die Rechte und Freiheiten betroffener Personen, insbesondere das Recht auf Information (Transparenz), das Recht auf Eingreifen (Zugang, Löschung, Datenübertragbarkeit, Berichtigung) und das Recht auf Einschränkung der Verarbeitung (das Recht, nicht Gegenstand automatisierter Entscheidungsfindung im Einzelfall zu sein, und das Recht auf Nichtdiskriminierung der betroffenen Personen in diesen Prozessen).

70. Beispiele für zentrale Aspekte der Technikgestaltung und der Voreinstellung in Bezug auf die Verarbeitung nach Treu und Glauben sind:
    - Autonomie – Den betroffenen Personen sollte bei der Bestimmung über die Nutzung ihrer personenbezogenen Daten sowie über Umfang und Bedingungen dieser Nutzung oder Verarbeitung der höchstmögliche Grad an Autonomie gewährt werden.
    - Interaktion – Die betroffenen Personen müssen in der Lage sein, ihre Rechte in Bezug auf die von dem Verantwortlichen verarbeiteten personenbezogenen Daten mitzuteilen und auszuüben.
    - Erwartung – Die Verarbeitung sollte den berechtigten Erwartungen der betroffenen Personen entsprechen.
    - Nichtdiskriminierung – Der Verantwortliche darf die betroffenen Personen nicht in unfairer Weise diskriminieren.
    - Nichtnutzung – Der Verantwortliche sollte die Bedürfnisse und die Schutzbedürftigkeit betroffener Personen nicht ausnutzen.
    - Wahlmöglichkeit der Verbraucher – Der Verantwortliche sollte seine Nutzer nicht in unlauterer Weise an sich „binden“. Wenn es sich bei dem Dienst für die Verarbeitung personenbezogener Daten um einen proprietären Dienst handelt, kann eine dienstbezogene Bindung geschaffen werden; ein solcher Lock-in-Effekt kann unlauter sein, wenn er die Möglichkeit der betroffenen Personen beeinträchtigt, ihr Recht auf Datenübertragbarkeit nach Artikel 20 auszuüben.
    - Gleichgewicht der Kräfte – Das Gleichgewicht der Kräfte sollte ein zentrales Ziel für das Verhältnis zwischen dem Verantwortlichen und der betroffenen Person sein. Ein Kräfteungleichgewicht sollte vermieden werden. Falls sich ein solches Ungleichgewicht nicht vermeiden lässt, sollte es anerkannt werden, und es sollten geeignete Gegenmaßnahmen ergriffen werden.
    - Kein Risikotransfer – Die Verantwortlichen sollten die Risiken des Unternehmens nicht auf die betroffenen Personen abwälzen.
    - Keine betrügerische Absicht – Informationen über die Datenverarbeitung und Optionen zur Datenverarbeitung sollten objektiv und neutral bereitgestellt werden, wobei weder die Formulierungen noch die Gestaltung irreführend oder manipulativ sein sollten.
    - Wahrung der Rechte – Der Verantwortliche muss die Grundrechte betroffener Personen wahren und geeignete Maßnahmen und Garantien umsetzen; er darf nicht in diese Rechte eingreifen, es sei denn, ein solcher Eingriff ist ausdrücklich durch das Gesetz gerechtfertigt.
    - Ethik – Der Verantwortliche sollte die größeren Auswirkungen auf die Rechte und die Würde des Einzelnen im Blick haben.

- Wahrhaftigkeit – Der Verantwortliche muss Informationen darüber bereitstellen, wie er personenbezogene Daten verarbeitet; er sollte sich bei seinen Handlungen seinem Wort entsprechend verhalten und die betroffenen Personen nicht in die Irre führen.
- Menschliches Eingreifen – Der Verantwortliche muss in Einklang mit dem Recht nach Artikel 22[32], nicht Gegenstand automatischer Entscheidungsfindung im Einzelfall zu sein, ein *qualifiziertes* menschliches Eingreifen vorsehen, um auf diese Weise Fehler aufzudecken, die durch Maschinen entstehen können.
- Faire Algorithmen – Anhand regelmäßiger Prüfungen wird untersucht, ob die Algorithmen zweckentsprechend funktionieren; die Algorithmen werden angepasst, um festgestellte Fehler zu minimieren und die Verarbeitung nach Treu und Glauben zu gewährleisten. Betroffene Personen sollten darüber informiert werden, dass die Verarbeitung personenbezogener Daten auf der Grundlage von Algorithmen erfolgt, dass mithilfe der Algorithmen Analysen oder Prognosen über sie erstellt werden, z. B. in Bezug auf Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Bewegungen.[33]

Beispiel 1

Ein Verantwortlicher betreibt eine Suchmaschine, die hauptsächlich nutzergenerierte personenbezogene Daten verarbeitet. Der Verantwortliche profitiert davon, über große Mengen personenbezogener Daten zu verfügen und für gezielte Werbung nutzen zu können. Der Verantwortliche ist daher bestrebt, die betroffenen Personen dahingehend zu beeinflussen, dass sie ihr Einverständnis mit einer weitergehenden Erhebung und Nutzung ihrer personenbezogenen Daten erteilen. Die betroffene Person ist über die Optionen der Verarbeitung zu informieren, wenn sie um ihr Einverständnis ersucht wird.

Bei der Umsetzung des Grundsatzes der Verarbeitung nach Treu und Glauben unter Berücksichtigung von Art, Umfang, Umständen und Zweck der Verarbeitung stellt der Verantwortliche fest, dass er die Optionen nicht so präsentieren kann, dass die betroffene Person dahingehend beeinflusst wird, demVerantwortlichen zu erlauben, mehr personenbezogene Daten zu sammeln, als wenn die Optionen in gleicher und neutraler Weise vorgestellt würden. Er darf die Verarbeitungsoptionen also nicht so präsentieren, dass es den betroffenen Personen erschwert wird, die Weitergabe ihrer Daten zu untersagen oder ihre Datenschutzeinstellungen anzupassen und die Verarbeitung einzuschränken. Diese Beispiele sind so genannte Dark Patterns, die dem Geist von Artikel 25 widersprechen. Die Standardoptionen der Verarbeitung sollten nicht invasiv sein, und die Wahlmöglichkeit der weiteren Verarbeitung sollte so präsentiert werden, dass die betroffenen Personen nicht zur Erteilung ihres Einverständnisses gedrängt werden. Deshalb präsentiert der Verantwortliche die Optionen zur Erteilung bzw. zur Verweigerung des Einverständnisses als zwei gleichberechtigte erkennbare Wahlmöglichkeiten, wobei die betroffene Person über die Auswirkungen der jeweiligen Entscheidung korrekt informiert wird.

[32] Siehe „Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679“, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826.
[33] Vgl. Erwägungsgrund 71 DSGV.

Beispiel 2

Ein weiterer Verantwortlicher verarbeitet personenbezogene Daten für die Bereitstellung einer Streaming-Dienstleistung, bei der die Nutzer zwischen einem regulären Abonnement mit Standardqualität und einem Premiumabonnement mit höherer Qualität wählen können. Das Premiumabonnement sieht eine bevorzugte Behandlung der Abonnenten beim Kundendienst vor.

Dem Grundsatz der Verarbeitung nach Treu und Glauben entsprechend dürfen die Kunden mit Standardabonnement durch die bevorzugte Behandlung von Premiumabonnenten beim Kundendienst in Bezug auf den Zugang zur Ausübung ihrer Rechte nach Artikel 12 DSGVO nicht diskriminiert werden. Dies bedeutet, dass die Premiumabonnenten zwar bevorzugt behandelt werden, diese Bevorzugung aber nicht dazu führen kann, dass keine geeigneten Vorkehrungen getroffen werden, um Anfragen von Standardabonnenten ohne unangemessene Verzögerung und in jedem Fall binnen eines Monats nach Eingang der Anfragen zu beantworten.

Kunden mit Vorzugsabonnement mögen zwar einen höheren Preis für einen besseren Service zahlen; dennoch haben alle betroffenen Personen gleichberechtigten und diskriminierungsfreien Zugang im Hinblick auf die Durchsetzung ihrer Rechte und Freiheiten nach Artikel 12.

3.4 Zweckbindung[34]

71. Der Verantwortliche muss die Daten für festgelegte, eindeutige und legitime Zwecke erheben und darf sie nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeiten.[35] Die Verarbeitung sollte daher so gestaltet werden, dass nur die für die Erreichung der Zwecke notwendigen Daten verarbeitet werden. Soll eine weitere Verarbeitung stattfinden, muss der Verantwortliche zunächst sicherstellen, dass diese Verarbeitung zu Zwecken erfolgt, die mit den ursprünglichen Zwecken vereinbar sind, und diese Verarbeitung dementsprechend gestalten. Ob ein neuer Zweck mit dem ursprünglichen Zweck vereinbar ist oder nicht, ist anhand der Kriterien in Artikel 6 Absatz 4 zu prüfen.

72. Beispiele für zentrale Aspekte der Technikgestaltung und der Voreinstellung in Bezug auf die Zweckbindung sind:
    - Vorherige Bestimmung – Die rechtmäßigen Zwecke werden vor der Gestaltung der Verarbeitung festgelegt.
    - Spezifizität (vlt. einfach Genauigkeit ?) – Die Zwecke sind zu präzisieren, und sie sind hinsichtlich des Grunds der Verarbeitung personenbezogener Daten eindeutig.
    - Zweckorientierung – Die Gestaltung der Verarbeitung und die Festlegung der Grenzen für die Verarbeitung sollten sich am Zweck der Verarbeitung orientieren.
    - Notwendigkeit – Anhand des Zwecks wird festgelegt, welche personenbezogenen Daten für die Verarbeitung notwendig sind.
    - Vereinbarkeit – Jeder neue Zweck muss mit dem ursprünglichen Zweck, für den die Daten erhoben wurden, vereinbar sein und bei Veränderungen der Gestaltung berücksichtigt werden.

[34] Die Artikel-29-Datenschutzgruppe hat eine Stellungnahme zum Verständnis des Grundsatzes der Zweckbindung nach der Richtlinie 95/46/EG veröffentlicht. Die Stellungnahme wurde zwar nicht vom EDSA angenommen, ist aber dennoch von Bedeutung, da der Wortlaut des Grundsatzes in der DSGVO derselbe ist. Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203, 2. April 2013, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[35] Artikel 5 Absatz 1 Buchstabe b DSGVO.

- Beschränkung der weiteren Verarbeitung – Der Verantwortliche sollte weder Datensätze verbinden noch eine weitere Verarbeitung für neue mit dem ursprünglichen Zweck nicht zu vereinbarende Zwecke vornehmen.
- Beschränkungen der Wiederverwendung – Der Verantwortliche sollte technische Maßnahmen unter anderem Hashing und Verschlüsselung anwenden, um die Möglichkeit einzuschränken, dass personenbezogene Daten einem neuen Zweck zugeführt werden. Der Verantwortliche sollte auch organisatorische Maßnahmen anwenden, die die Wiederverwendung personenbezogener Daten einschränken, und z. B. Strategien und vertragliche Verpflichtungen festlegen.
- Überprüfung – Der Verantwortliche sollte regelmäßig überprüfen, ob die Verarbeitung für die Zwecke, für die die Daten erhoben wurden, erforderlich ist, und die Gestaltung unter dem Aspekt der Zweckbindung testen.

Beispiel

Der Verantwortliche verarbeitet die personenbezogenen Daten seiner Kunden. Der Zweck der Verarbeitung besteht darin, einen Vertrag zu erfüllen, d. h. Waren an die richtige Adresse zu liefern und dafür eine Bezahlung zu erhalten. Die gespeicherten personenbezogenen Daten sind Kaufhistorie, Name, Adresse, E-Mail-Adresse und Telefonnummer.

Der Verantwortliche erwägt, ein Produkt für das „Customer Relationship Management“ (CRM) bzw. Kundenbeziehungsmanagement zu erwerben, bei dem alle Kundendaten wie Daten über Umsätze, Marketing und Kundendienst an einer Stelle zusammengeführt werden. Das Produkt bietet die Möglichkeit, alle Anrufe, Aktivitäten, Dokumente, E-Mails und Marketingkampagnen zu speichern, um ein Gesamtbild des Kunden zu erhalten. Darüber hinaus lässt sich mit dem Produkt für das Kundenbeziehungsmanagement unter Verwendung öffentlicher Informationen die Kaufkraft des Kunden analysieren. Der Zweck der Analyse ist die zielgerichtetere Durchführung von Werbemaßnahmen. Diese Maßnahmen gehören nicht zum ursprünglichen rechtmäßigen Zweck der Verarbeitung.

Zur Wahrung des Grundsatzes der Zweckbindung schreibt der Verantwortliche dem Produktanbieter vor, die verschiedenen Verarbeitungstätigkeiten, bei denen personenbezogene Daten für die für den Verantwortlichen relevanten Zwecke verwendet werden, zu erfassen und zu beschreiben.

Nach Erhalt der Ergebnisse der Erfassung und Beschreibung prüft der Verantwortliche, ob der neue Vermarktungszweck und der Zweck der gezielten Werbung mit den ursprünglichen, zum Zeitpunkt der Erhebung festgelegten Zwecken vereinbar sind und ob es eine hinreichende Rechtsgrundlage für die entsprechende Verarbeitung gibt. Ergibt diese Prüfung kein positives Ergebnis, wendet der Verantwortliche die entsprechenden Funktionen nicht mehr an. Alternativ könnte der Verantwortliche auf die Prüfung verzichten und die beschriebenen Funktionen des Produkts einfach nicht nutzen.

3.5 Datenminimierung

73. Nur personenbezogene Daten, die angemessen, relevant und auf das für den Zweck **Notwendige** beschränkt sind, dürfen verarbeitet werden.[36] Im Ergebnis muss der Verantwortliche vorher

[36] Artikel 5 Absatz 1 Buchstabe c DSGVO.

bestimmen, welche Merkmale und Parameter der Verarbeitungssysteme und ihrer unterstützenden Funktionen zulässig sind. Die Datenminimierung untermauert und operationalisiert den Grundsatz der Notwendigkeit. Bei der weiteren Verarbeitung sollte der Verantwortliche regelmäßig prüfen, ob die verarbeiteten personenbezogenen Daten noch immer angemessen, relevant und notwendig sind oder ob die Daten gelöscht oder anonymisiert werden müssen.

74. Die Verantwortlichen sollten zunächst festlegen, ob die Verarbeitung personenbezogener Daten für ihre entsprechenden Zwecke überhaupt erforderlich ist. Der Verantwortliche sollte überprüfen, ob die entsprechenden Zwecke durch die Verarbeitung einer kleineren Zahl von personenbezogenen Daten erfüllt werden können, ob weniger stark untergliederte oder aggregierte personenbezogene Daten ausreichen oder ob die Verarbeitung personenbezogener Daten ganz verzichtbar ist.[37] Diese Überprüfung sollte vor einer etwaigen Verarbeitung durchgeführt werden, könnte aber auch jederzeit während des Lebenszyklus der Verarbeitung erfolgen. Dies steht auch im Einklang mit Artikel 11.

75. Die Minimierung kann sich außerdem auf den Grad der Identifizierung beziehen. Ist es für die Verarbeitung nicht notwendig, dass sich der endgültige Datensatz auf ein identifiziertes oder identifizierbares Individuum bezieht, (wie in Statistiken) dies jedoch bei der ursprünglichen Verarbeitung der Fall ist, (z. B. vor der Datenaggregierung) muss der Verantwortliche die personenbezogenen Daten löschen oder anonymisieren, sobald die Identifizierung nicht mehr erforderlich ist. Falls die weitere Identifizierung aber für andere Verarbeitungstätigkeiten erforderlich ist, sollten die personenbezogenen Daten pseudonymisiert werden, um die Risiken für die Rechte der betroffenen Personen zu minimieren.

76. Beispiele für zentrale Aspekte der Technikgestaltung und der Voreinstellung in Bezug auf die Datenminimierung sind:
    - Datenvermeidung – Auf die Verarbeitung personenbezogener Daten sollte grundsätzlich verzichtet werden, wenn dies bei dem entsprechenden Zweck möglich ist.
    - Beschränkung – Die Menge der erhobenen personenbezogenen Daten muss auf das für den Zweck Notwendige beschränkt sein.
    - Zugangsbeschränkung – Bei der Gestaltung der Datenverarbeitung ist darauf zu achten, dass eine möglichst geringe Zahl von Personen für die Ausführung ihrer Aufgaben Zugang zu personenbezogenen Daten haben muss und der Zugang entsprechend beschränkt wird.
    - Relevanz – Die personenbezogenen Daten sollten für die betreffende Verarbeitung relevant sein, und der Verantwortliche sollte diese Relevanz nachweisen können.
    - Notwendigkeit – Alle Kategorien personenbezogener Daten müssen für die angegebenen Zwecke notwendig sein und sollten nur verarbeitet werden, wenn es nicht möglich ist, den Zweck mit anderen Mitteln zu erreichen.
    - Aggregation – Nach Möglichkeit sollten aggregierte Daten verwendet werden.
    - Pseudonymisierung – Personenbezogene Daten sollten pseudonymisiert werden, sobald keine Notwendigkeit mehr für direkt identifizierbare personenbezogene Daten besteht, und Identifizierungsschlüssel sollten separat gespeichert werden.
    - Anonymisierung und Löschung – Sind personenbezogene Daten nicht oder nicht mehr für den Zweck notwendig, sind sie zu anonymisieren oder zu löschen.
    - Datenübermittlung – Die Datenübermittlung sollte so effizient gestaltet sein, dass nicht mehr Kopien als notwendig erstellt werden.

[37] In Erwägungsgrund 39 DSGVO heißt es: „...Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann."

- Stand der Technik – Der Verantwortliche sollte moderne und geeignete Technologien anwenden, um Daten zu vermeiden und zu minimieren.

Beispiel 1

Ein Buchladen möchte seine Umsätze steigern und seine Bücher auch online verkaufen. Der Ladenbesitzer möchte ein standardisiertes Formular für den Bestellvorgang einrichten. Um sicherzustellen, dass die Kunden alle gewünschten Angaben machen, definiert der Ladenbesitzer alle Felder des Formulars als Pflichtfelder (werden nicht alle Felder ausgefüllt, kann die Bestellung nicht abgeschlossen werden). Der Online-Shop-Besitzer verwendet zunächst ein Standardkontaktformular, in dem die Kunden unter anderem nach Geburtsdatum, Telefonnummer und Wohnanschrift gefragt werden. Nicht alle Felder des Formulars sind jedoch für den Zweck des Kaufs und der Lieferung von Büchern notwendig. Wenn die betroffene Person das Produkt im Voraus bezahlt, sind in diesem konkreten Fall ihr Geburtsdatum und ihre Telefonnummer für den Kauf des Produkts nicht erforderlich. Daher können diese Angaben im Onlineformular nicht als Pflichtangaben für den Kauf des Produkts festgelegt werden, sofern der Verantwortliche nicht klar nachweisen kann, dass sie ansonsten notwendig sind und warum die Felder benötigt werden. Darüber hinaus gibt es Fälle, in denen eine Adresse nicht notwendig ist. Bei der Bestellung eines elektronischen Buches z. B. kann der Kunde das Produkt direkt auf sein Gerät herunterladen.

Deshalb entscheidet sich der Online-Shop-Besitzer für zwei Online-Formulare: ein Formular für die Bestellung von Büchern mit einem Feld für die Kundenanschrift und ein Formular für die Bestellung von eBooks ohne ein solches Feld.

Beispiel 2

Ein öffentliches Verkehrsunternehmen möchte statistische Daten über Reiserouten erheben. Dies ist zweckmäßig, um angemessene Entscheidungen über Änderungen der Fahrpläne öffentlicher Verkehrsmittel und geeignete Zugstrecken zu treffen. Die Fahrgäste müssen jedes Mal beim Ein- und Aussteigen ihren Fahrschein durch ein Lesegerät führen. Nach einer Bewertung der Risiken, die mit der Erhebung von Reiserouten von Fahrgästen für die Rechte und Freiheiten der Fahrgäste verbunden sind, stellt der Verantwortliche fest, dass Fahrgäste, die in dünn besiedelten Gebieten wohnen oder arbeiten, bei einer Einzelstreckenerkennung anhand der Fahrscheinkennung identifiziert werden können. Da die Fahrscheinkennung für den Zweck der Optimierung der Fahrpläne öffentlicher Verkehrsmittel und der Zugstrecken nicht notwendig ist, speichert der Verantwortliche sie nicht. Nach Beendigung der Reise speichert der Verantwortliche nur die einzelnen Reiserouten, damit es nicht möglich ist, Reisen anhand eines einzelnen Fahrscheins zu identifizieren, und speichert lediglich Informationen über separate Reiserouten.

In Fällen, in denen immer noch das Risiko bestehen kann, eine Person allein anhand der Route ihrer Reise mit öffentlichen Verkehrsmitteln zu identifizieren, wendet der Verantwortliche statistische Maßnahmen zur Risikominimierung an, z. B. das Abschneiden des Anfangs und des Endes der Route.

Beispiel 3

Ein Kurier möchte die Effizienz seiner Kurierfahrten im Hinblick auf Zustellzeiten, Planung des Arbeitsvolumens und Kraftstoffverbrauch bewerten. Um dieses Ziel zu erreichen, muss der Kurier einige personenbezogene Daten in Bezug auf die Angestellten (Fahrer) und die Kunden (Empfänger, zu liefernde Gegenstände usw.) verarbeiten. Dieser Verarbeitungsvorgang birgt das Risiko der Überwachung der Mitarbeiter, was besondere rechtliche Vorkehrungen erfordert, und der Beobachtung der Gewohnheiten der Kunden, da bekannt ist, welche Gegenstände im Laufe der Zeit geliefert werden. Diese Risiken können durch eine angemessene Pseudonymisierung der Mitarbeiter und Kunden signifikant gesenkt werden. Wenn vor allem die Pseudonymisierungsschlüssel häufig gewechselt werden und Makrobereiche anstelle von genauen Anschriften berücksichtigt werden, findet eine wirksame Datenminimierung statt, und der Verantwortliche kann sich ausschließlich auf den Lieferprozess und den Zweck der Ressourcenoptimierung konzentrieren, ohne eine Grenze hin zur Überwachung des Verhaltens von Einzelpersonen (Kunden oder Mitarbeitern) zu überschreiten.

Beispiel 4

Ein Krankenhaus erhebt Daten über seine Patienten in einem Krankenhausinformationssystem (einer elektronischen Patientenakte). Die Mitarbeiter des Krankenhauses müssen Zugang zu Patientenakten haben, um über geeignete Pflege- und Behandlungsmaßnahmen entscheiden und um alle Diagnosen, Pflege- und Behandlungsmaßnahmen dokumentieren zu können. Standardmäßig wird nur dem medizinischen Personal Aktenzugang gewährt, das in der Fachabteilung, in der es tätig ist, für die Behandlung des betreffenden Patienten zuständig ist. Die Gruppe der Personen, die Zugang zur Akte eines Patienten haben, wird größer, wenn andere Abteilungen oder Diagnostikabteilungen zur Behandlung hinzugezogen werden. Nach der Entlassung des Patienten und nach Abschluss der Abrechnung wird der Aktenzugang auf eine kleine Gruppe von Angestellten pro Fachabteilung begrenzt, die Anfragen nach medizinischen Informationen oder einer Konsultation, die von anderen medizinischen Dienstleistern gestellt oder erbeten werden, nach Genehmigung durch den jeweiligen Patienten beantworten.

3.6 Richtigkeit

77. Die personenbezogenen Daten sind sachlich richtig und immer auf dem neuesten Stand; dabei werden alle angemessenen Maßnahmen getroffen, um sicherzustellen, dass personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.[38]

78. Die Anforderungen sollten im Verhältnis zu den Risiken und Folgen der konkreten Datennutzung stehen. Unrichtige personenbezogene Daten können Risiken für die Rechte und Freiheiten der betroffenen Personen bergen, wenn sie beispielsweise in einem Gesundheitsprotokoll zu einer fehlerhaften Diagnose oder einer Fehlbehandlung führen. Auch kann ein falsches Bild von einer Person dazu führen, dass Entscheidungen entweder manuell oder anhand einer automatisierten Entscheidungsfindung oder mithilfe von künstlicher Intelligenz auf der falschen Grundlage getroffen werden.

[38] Artikel 5 Absatz 1 Buchstabe d DSGVO.

79. Beispiele für zentrale Aspekte der Technikgestaltung und der Voreinstellung in Bezug auf die Richtigkeit sind:
    - Datenquelle – Quellen personenbezogener Daten sollten, was die Richtigkeit der Daten anbelangt, verlässlich sein.
    - Grad der Richtigkeit – Die einzelnen Elemente personenbezogener Daten sollten so genau sein, wie es für den spezifischen Zweck erforderlich ist.
    - Messbare Richtigkeit - Die Zahl falscher Positivergebnisse / falscher Negativergebnisse, z. B. Fehler bei automatischer Entscheidungsfindung und beim Einsatz künstlicher Intelligenz, ist zu reduzieren.
    - Überprüfung – In Abhängigkeit davon, um welche Art von Daten es sich handelt und wie häufig sich die Daten ändern können, (z. B. bei Altersanforderungen) sollte der Verantwortliche die betroffene Person vor der Verarbeitung und in verschiedenen Phasen der Verarbeitung ersuchen, die Richtigkeit personenbezogener Daten zu überprüfen.
    - Löschung/Berichtigung – Der Verantwortliche löscht bzw. berichtigt falsche Daten unverzüglich. Der Verantwortliche ermöglicht dies insbesondere dann, wenn es sich bei den betroffenen Personen um Kinder handelt bzw. handelte, die später die Löschung dieser personenbezogenen Daten wünschen.[39]
    - Vermeidung einer Fehlerfortpflanzung – Die Verantwortlichen sollten die Auswirkungen eines kumulierten Fehlers in der Verarbeitungskette abmildern.
    - Zugang – Die betroffenen Personen sollten nach den Artikeln 12 bis 15 DSGVO über die personenbezogenen Daten informiert werden und tatsächlichen Zugang zu diesen Daten erhalten, um die Richtigkeit zu kontrollieren und bei Bedarf Berichtigungen vorzunehmen.
    - Kontinuierliche Richtigkeit – Die personenbezogenen Daten sollten in allen Phasen der Verarbeitung korrekt sein; in kritischen Phasen sollte die Richtigkeit überprüft werden.
    - Aktualität – Die personenbezogenen Daten müssen aktualisiert werden, falls es für den Zweck erforderlich ist.
    - Datengestaltung - Technische und organisatorische Gestaltungsmerkmale sollten zur Reduzierung der Fehlerhaftigkeit eingesetzt werden; z. B. sollten knapp formulierte vorgegebene Antwortmöglichkeiten anstelle von Freitextfeldern verwendet werden.

Beispiel 1

Ein Versicherungsunternehmen möchte künstliche Intelligenz (KI) einsetzen, um ein Profil der Kunden zu erstellen, die eine Versicherung abschließen, und dieses Profil als Grundlage für seine Entscheidungen bei der Berechnung des Versicherungsrisikos heranziehen. Bei der Festlegung der Entwicklung seiner KI-Lösungen bestimmt das Unternehmen die Verarbeitungsmittel und berücksichtigt bei der Wahl einer KI-Anwendung eines Anbieters und bei der Entscheidung darüber, wie die künstliche Intelligenz trainiert werden soll, die Umsetzung des Datenschutzes durch Technikgestaltung.

Bei der Entscheidung darüber, wie die künstliche Intelligenz trainiert werden soll, sollte der Verantwortliche korrekte Daten haben, um genaue Ergebnisse zu erzielen. Daher sollte der Verantwortliche sicherstellen, dass die für das Training der künstlichen Intelligenz verwendeten Daten richtig sind.

Angenommen, dass sich das Unternehmen für das Training der künstlichen Intelligenz unter Verwendung von personenbezogenen Daten aus einem großen Datensatz seiner Bestandskunden auf

[39] Vgl. Erwägungsgrund 65.

eine gültige Rechtsgrundlage stützen kann, wählt der Verantwortliche einen für die Bevölkerung repräsentativen Pool von Kunden, um auch Verzerrungen zu vermeiden.

Anschließend werden die Kundendaten aus dem entsprechenden Datenverarbeitungssystem erhoben, unter anderem Daten über die Versicherungsart z. B. Krankenversicherung, Hausversicherung, Reiseversicherung, sowie Daten aus öffentlichen Verzeichnissen, zu denen das Unternehmen rechtmäßigen Zugang hat. Alle Daten werden vor der Übertragung in das System für das Training des KI-Modells pseudonymisiert.

Um sicherzustellen, dass die für das Training der künstlichen Intelligenz verwendeten Daten so genau wie möglich sind, erhebt der Verantwortliche nur Daten aus Datenquellen mit korrekten und aktuellen Informationen.

Das Versicherungsunternehmen testet sowohl bei der Entwicklung als auch schließlich vor der Freigabe des Produktes, ob die künstliche Intelligenz zuverlässig ist und diskriminierungsfreie Ergebnisse liefert. Wenn die künstliche Intelligenz umfassend trainiert wurde und einsatzbereit ist, verwendet das Versicherungsunternehmen die entsprechenden Ergebnisse, um die Beurteilungen des Versicherungsrisikos zu unterstützen; bei seinen Entscheidungen über die Gewährung einer Versicherung verlässt es sich jedoch nicht ausschließlich auf die künstliche Intelligenz, sofern die Entscheidung nicht nach Maßgabe der Ausnahmen in Artikel 22 Absatz 2 DSGVO getroffen wird.

Das Versicherungsunternehmen führt auch regelmäßig Überprüfungen der Ergebnisse der künstlichen Intelligenz durch, um die Zuverlässigkeit zu wahren und den Algorithmus bei Bedarf anzupassen.

Beispiel 2

Der Verantwortliche ist eine Gesundheitseinrichtung, die auf der Suche nach Methoden ist, wie Integrität und Richtigkeit personenbezogener Daten in ihren Patientenverzeichnissen sichergestellt werden können.

Wenn zwei Personen zur selben Zeit in die Einrichtung kommen und dieselbe Behandlung erhalten, besteht Verwechslungsgefahr, wenn sie nur anhand ihres Namens unterschieden werden können. Um die Richtigkeit sicherzustellen, muss der Verantwortliche jeder Person eine einmalige Kennung zuordnen und benötigt daher mehr Daten als nur den Namen des Patienten.

Die Einrichtung verwendet verschiedene Systeme, die personenbezogene Daten der Patienten enthalten, und muss sicherstellen, dass die Informationen über die Patienten in allen Systemen jederzeit korrekt, präzise und einheitlich sind. Die Einrichtung hat festgestellt, dass verschiedene Risiken auftreten können, wenn Angaben in einem System geändert werden, in den anderen Systemen aber nicht.

Der Verantwortliche entscheidet, das Risiko durch den Einsatz einer Hashing-Technik zu mindern, mit der die Integrität der Daten im Behandlungsprotokoll sichergestellt werden kann. Für die Einträge im Behandlungsprotokoll und für den zugehörigen Patienten werden unveränderliche kryptografische Zeitstempel erstellt, sodass etwaige Änderungen erkannt, zueinander in Beziehung gesetzt und bei Bedarf nachverfolgt werden können.

3.7 Speicherbegrenzung

80. Der Verantwortliche muss sicherstellen, dass die personenbezogenen Daten nur so lange, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht.[40]
Es ist von grundlegender Bedeutung, dass der Verantwortliche genau weiß, welche personenbezogenen Daten das Unternehmen verarbeitet und warum. Der Zweck der Verarbeitung ist das Hauptkriterium bei der Entscheidung, wie lange personenbezogene Daten gespeichert werden.

81. Die Maßnahmen und Garantien zur Umsetzung des Grundsatzes der Speicherbegrenzung ergänzen die Rechte und Freiheiten der betroffenen Personen, insbesondere das Recht auf Löschung und das Widerspruchsrecht.

82. Beispiele für zentrale Aspekte der Technikgestaltung und der Voreinstellung in Bezug auf die Speicherbegrenzung sind:
- Löschung und Anonymisierung – Der Verantwortliche sollte über klare interne Verfahren und Funktionen für die Löschung und/oder Anonymisierung von Daten verfügen.
- Wirksamkeit der Anonymisierung/Löschung – Der Verantwortliche stellt sicher, dass anonymisierte Daten nicht wieder identifizierbar gemacht und gelöschte Daten nicht wiederhergestellt werden können, und sollte entsprechende Tests durchführen.
- Automatisierung – Die Löschung bestimmter personenbezogener Daten sollte automatisiert sein.
- Speicherkriterien – Der Verantwortliche muss bestimmen, welche Daten und welche Speicherdauer für den Zweck notwendig sind.
- Begründung – Der Verantwortliche muss rechtfertigen können, warum die Dauer der Speicherung für den Zweck und in Bezug auf die betreffenden personenbezogenen Daten erforderlich ist, und er muss die Begründung und die Rechtsgrundlage für die Speicherfrist angeben können.
- Durchsetzung der Speicherverfahren – Der Verantwortliche sollte die internen Speicherverfahren durchsetzen und nachprüfen, ob seine Verfahren in der Organisation eingehalten werden.
- Backups/Logdateien – Die Verantwortlichen legen fest, welche personenbezogenen Daten und welche Speicherdauer für Backups und Logdateien notwendig sind.
- Datenübermittlung – Die Verantwortlichen sollten die Übermittlung personenbezogener Daten und die Speicherung von Kopien dieser Daten verhüten und bestrebt sein, eine „vorübergehende“ Speicherung dieser Daten und Kopien zu begrenzen.

Beispiel

Der Verantwortliche erhebt personenbezogene Daten; der Zweck der Verarbeitung besteht darin, die Mitgliedschaft der betroffenen Person zu verwalten. Bei Beendigung der Mitgliedschaft werden die personenbezogenen Daten gelöscht; für eine weitere Speicherung der Daten gibt es keine Rechtsgrundlage.

Der Verantwortliche erarbeitet zunächst ein internes Verfahren für die Speicherung und die Löschung von Daten. Das Verfahren sieht vor, dass die Mitarbeiter personenbezogene Daten nach Ablauf der Speicherfrist manuell löschen. Der Mitarbeiter befolgt das Verfahren für die regelmäßige Löschung

[40] Artikel 5 Absatz 1 Buchstabe c DSGVO.

und Berichtigung der Daten auf Geräten, in Backups, Logdateien und E-Mails sowie auf anderen relevanten Speichermedien.

Danach führt der Verantwortliche stattdessen ein automatisches System für die automatische, zuverlässige und regelmäßigere Löschung ein, um die Daten wirksamer und weniger fehleranfällig zu löschen. Die Konfiguration des Systems sieht vor, dass das vorgegebene Verfahren für die Löschung der Daten befolgt wird; in zuvor festgelegten regelmäßigen Abständen werden dann personenbezogene Daten aus allen Speichermedien des Unternehmens gelöscht. Der Verantwortliche überprüft und testet das Speicherverfahren regelmäßig und stellt sicher, dass es in Einklang mit der aktuellen Speicherstrategie steht.

3.8 Integrität und Vertraulichkeit

83. Der Grundsatz der Integrität und Vertraulichkeit beinhaltet den Schutz durch geeignete technische oder organisatorische Maßnahmen vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung. Die Sicherheit personenbezogener Daten erfordert geeignete Maßnahmen zur Verhütung und Bewältigung von Verletzungen des Schutzes personenbezogener Daten, zur Gewährleistung der ordnungsgemäßen Ausführung der Datenverarbeitungsaufgaben und der Einhaltung der anderen Grundsätze sowie zur Erleichterung der wirksamen Ausübung der Rechte des Einzelnen.

84. Nach Erwägungsgrund 78 könnten Maßnahmen für den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen darin bestehen, dass der Verantwortliche in die Lage versetzt wird, *Sicherheitsfunktionen zu schaffen und zu verbessern*. Neben anderen Maßnahmen zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen wird in Erwägungsgrund 78 empfohlen, dass die Verantwortlichen dafür verantwortlich sein sollen, kontinuierlich zu prüfen, ob sie stets die geeigneten Mittel für die Verarbeitung einsetzen, und zu prüfen, ob die gewählten Maßnahmen in Bezug auf die bestehenden Schwachstellen tatsächlich Abhilfe schaffen. Darüber hinaus sollten die Verantwortlichen die Maßnahmen für Informationssicherheit im Umfeld der personenbezogenen Daten und zum Schutz dieser Daten sowie das Verfahren für den Umgang mit Verletzungen des Datenschutzes regelmäßig überprüfen.

85. Beispiele für zentrale Aspekte der Technikgestaltung und der Voreinstellung in Bezug auf die Integrität und Vertraulichkeit sind:
    - Managementsystem für Informationssicherheit – Für die Verwaltung der Strategien und Verfahren für Informationssicherheit steht ein operatives Mittel bereit.
    - Risikoanalyse – Die Risiken für die Sicherheit personenbezogener Daten werden unter Berücksichtigung der Auswirkungen auf die Rechte der Einzelnen bewertet; festgestellten Risiken wird entgegengewirkt. Für die Risikobewertung werden ein umfassendes, systematisches und realistisches „Gefahrenmodell“ sowie eine Angriffsanalyse der Oberfläche der gestalteten Anwendungsprogramme entwickelt und gepflegt, um Angriffsvektoren zu reduzieren und Gelegenheiten für die Ausnutzung von Schwachstellen und Anfälligkeiten zu verringern.
    - Sicherheit durch Technikgestaltung – Sicherheitsanforderungen werden möglichst früh bei der Gestaltung und Entwicklung des Systems berücksichtigt; Tests dieser Sicherheitsanforderungen werden kontinuierlich integriert und durchgeführt.
    - Pflege – Anwendungsprogramme, Geräte, Systeme, Dienste usw. werden regelmäßig überprüft und getestet, um anfällige Stellen der Systeme, die die Verarbeitung unterstützen, zu erkennen.

- Zugangskontrollmanagement – Nur die befugten Mitarbeiter, die zur Ausführung ihrer Verarbeitungsaufgaben Zugang zu den personenbezogenen Daten haben müssen, sollten einen solchen Zugang haben; der Verantwortliche sollte bei den Zugangsrechten für die befugten Mitarbeiter differenzieren.
    - Zugangsbeschränkung (Bevollmächtigte) – Bei der Gestaltung der Datenverarbeitung ist darauf zu achten, dass eine möglichst kleine Zahl von Personen für die Ausführung ihrer Aufgaben Zugang zu personenbezogenen Daten haben muss und dass der Zugang entsprechend beschränkt wird.
    - Zugangsbeschränkung (Inhalt) – Bei jedem einzelnen Verarbeitungsvorgang sollte der Zugang auf die Attribute je Datensatz begrenzt werden, die für die Ausführung dieses Vorgangs erforderlich sind. Zudem sollte der Zugang zu Daten über diejenigen betroffenen Personen beschränkt werden, die den Aufgabenbereich des betreffenden Mitarbeiters berühren.
    - Zugangssegregation – Bei der Gestaltung der Datenverarbeitung ist darauf zu achten, dass keine Einzelperson umfassenden Zugang zu allen über eine betroffene Person erhobenen Daten, erst recht nicht zu allen personenbezogenen Daten einer bestimmten Kategorie von betroffenen Personen haben muss.
- Sichere Übertragungen – Übertragungen sind vor unbefugtem und unbeabsichtigtem Zugriff und vor unbefugten und unbeabsichtigten Änderungen zu schützen.
- Sichere Speicherung – Datenspeicher sind vor unbefugtem Zugriff und unbefugten Änderungen zu schützen. Verfahren für die Bewertung des Risikos einer zentralisierten oder dezentralisierten Speicherung sollten eingerichtet sein, ebenso Verfahren für die Beurteilung, für welche Kategorien von personenbezogenen Daten dies gilt. Einige Daten erfordern unter Umständen zusätzliche Sicherheitsmaßnahmen oder müssen von anderen Daten getrennt werden.
- Pseudonymisierung – Personenbezogene Daten und Backups/Logdateien sollten zur Sicherheit pseudonymisiert werden, um die Risiken möglicher Verletzungen des Datenschutzes zu minimieren, beispielsweise durch Hashing oder Verschlüsselung.
- Backups/Logdateien – Backups und Logdateien werden nur so lange aufbewahrt, wie es für die Informationssicherheit erforderlich ist; bei der routinemäßigen Sicherheitskontrolle sollten Prüfpfade und Ereignisüberwachung eingebunden werden. Backups und Logdateien sind vor unbefugtem und unbeabsichtigtem Zugang und vor unbefugten und unbeabsichtigten Änderungen zu schützen und regelmäßig zu überprüfen; bei Zwischenfällen sollte umgehend Abhilfe geschaffen werden.
- Notfallwiederherstellung/Betriebskontinuität – Anforderungen an die Notfallwiederherstellung des Informationssystems und die Betriebskontinuität sollte Rechnung getragen werden, um die Verfügbarkeit von personenbezogenen Daten nach größeren Zwischenfällen wieder zu gewährleisten.
- Risikobezogener Schutz – Zum Schutz aller Kategorien personenbezogener Daten sollten Maßnahmen zur Verhütung des Risikos einer Sicherheitsverletzung eingeführt werden. Daten, die mit besonderen Risiken verbunden sind, sollten nach Möglichkeit von den übrigen personenbezogenen Daten getrennt aufbewahrt werden.
- Abhilfemaßnahmen bei Sicherheitsvorfällen – Abläufe, Verfahren und Ressourcen sollten eingesetzt werden, um Verletzungen des Datenschutzes zu erkennen, einzudämmen, zu bewältigen, zu melden und um Lehren aus diesen Datenschutzverletzungen zu ziehen.
- Zwischenfallmanagement – Der Verantwortliche sollte über Verfahren zur Bewältigung von Datenschutzverletzungen und Zwischenfällen verfügen, um das Verarbeitungssystem weiter

zu stärken. Hierzu gehören Meldeverfahren z. B. die Verwaltung von Meldungen (an die Aufsichtsbehörde) und von Informationen (an betroffene Personen).

Beispiel

Ein Verantwortlicher möchte große Mengen personenbezogener Daten aus einer medizinischen Datenbank mit elektronischen (Patienten-) Krankenakten extrahieren, die sich auf einem speziellen Datenbankserver im Unternehmen befindet, um die extrahierten Daten zum Zweck der Qualitätssicherung zu verarbeiten. Eine Risikobewertung durch das Unternehmen ergab, dass bei der Extraktion auf einen Server, der für alle Mitarbeiter des Unternehmens zugänglich ist, vermutlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Da lediglich eine Abteilung des Unternehmens die extrahierten Patientendaten verarbeiten muss, beschließt der Verantwortliche, nur den Mitarbeitern dieser Abteilung Zugang zu dem speziellen Server zu gewähren. Darüber hinaus werden die Daten zur weiteren Risikominimierung vor der Übertragung pseudonymisiert.

Das Unternehmen beschließt, das Netzwerk abzutrennen und Zugangskontrollen zum Server einzurichten, um den Zugang zu regulieren und mögliche Schäden durch Schadsoftware zu mindern. Darüber hinaus richtet es eine Sicherheitsüberwachung und ein Einbruchmelde- und - präventionssystem ein und nimmt eine Trennung von der routinemäßigen Verwendung vor. Es wird ein automatisiertes Prüfsystem eingerichtet, um Zugriff und Änderungen zu überwachen. Das System löst Meldungen und automatisierte Warnungen aus, wenn bestimmte Ereignisse in Verbindung mit der Nutzung konfiguriert sind. Der Verantwortliche stellt sicher, dass der Zugang auf die Nutzer beschränkt ist, die Kenntnis der Daten haben müssen und die über die entsprechenden Zugangsrechte verfügen. Eine unbefugte Nutzung kann schnell und einfach erkannt werden.

Einige der extrahierten Daten müssen mit neu extrahierten Daten verglichen werden, weshalb sie drei Monate lang gespeichert werden müssen. Der Verantwortliche beschließt, sie auf demselben Server in gesonderten Datenbanken zu speichern und für die Speicherung sowohl die transparente Datenverschlüsselung als auch die Verschlüsselung auf Spaltenebene anzuwenden. Schlüssel zur Entschlüsselung von Daten in Spalten werden in gesonderten Sicherheitsmodulen gespeichert, die nur von befugten Mitarbeitern verwendet werden können, jedoch nicht extrahiert werden können.

Die Bewältigung auftretender Zwischenfälle bewirkt eine Stärkung des Systems und eine Verbesserung seiner Zuverlässigkeit. Dem für die Verarbeitung Verantwortlichen ist bewusst, dass präventive und wirksame Maßnahmen und Garantien bei allen Verarbeitungen personenbezogener Daten, die er jetzt und in Zukunft durchführt, vorgesehen sein sollten und dass dies zur Verhütung künftiger Verletzungen des Datenschutzes beitragen kann.

Der Verantwortliche legt diese Sicherheitsmaßnahmen fest, um sowohl die Richtigkeit, Integrität und Vertraulichkeit sicherzustellen als auch die Verbreitung von Schadsoftware durch Cyberangriffe zu verhüten und um die Lösung robuster zu machen. Die Umsetzung wirksamer Sicherheitsmaßnahmen fördert die Vertrauensbildung bei den betroffenen Personen.

3.9 Rechenschaftspflicht[41]

86. Nach dem Grundsatz der Rechenschaftspflicht ist der Verantwortliche für die Einhaltung aller vorgenannten Grundsätze verantwortlich und muss die Wahrung dieser Grundsätze nachweisen können.

[41] Siehe Erwägungsgrund 74, wonach die Verantwortlichen die Wirksamkeit ihrer Maßnahmen nachweisen müssen.

87. Der Verantwortliche muss die Wahrung dieser Grundsätze nachweisen können. Zu diesem Zweck hat er die Möglichkeit aufzuzeigen, welche Auswirkungen die Maßnahmen haben, die er zum Schutz der Rechte der betroffenen Personen umgesetzt hat, und warum die Maßnahmen für geeignet und wirksam erachtet werden. So kann beispielsweise demonstriert werden, warum eine Maßnahme geeignet ist, den Grundsatz der Speicherbegrenzung wirksam umzusetzen.

88. Voraussetzung für die Verarbeitung personenbezogener Daten in verantwortlicher Weise ist, dass der Verantwortliche sowohl über die Kenntnisse für die Umsetzung des Datenschutzes als auch über die hierfür erforderlichen Fähigkeiten verfügt. Dies bedeutet, dass der Verantwortliche die Datenschutzverpflichtungen, die ihm aus der DSGVO erwachsen, kennt und dass er diese Verpflichtungen einhalten kann.

4 ARTIKEL 25 ABSATZ 3: ZERTIFIZIERUNG

89. Nach Artikel 25 Absatz 3 kann eine Zertifizierung gemäß Artikel 42 als Nachweis der Einhaltung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen dienen. Umgekehrt können Unterlagen, die die Einhaltung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen belegen, auch für das Zertifizierungsverfahren hilfreich sein. Wenn also ein Verarbeitungsvorgang eines Verantwortlichen oder eines Auftragsverarbeiters nach Artikel 42 zertifiziert ist, berücksichtigen die Aufsichtsbehörden diese Zertifizierung bei ihrer Beurteilung der Einhaltung der DSGVO, insbesondere im Hinblick auf den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.

90. Wenn ein Verarbeitungsvorgang eines Verantwortlichen oder eines Auftragsverarbeiters nach Artikel 42 zertifiziert ist, sind die Elemente, die dazu beitragen, die Einhaltung von Artikel 25 Absätze 1 und 2 nachzuweisen, die Gestaltungsprozesse, d. h. der Prozess der Festlegung der Verarbeitungsmittel, der Steuerung und der technischen und organisatorischen Maßnahmen zur Umsetzung der Datenschutzgrundsätze. Die Zertifizierungsgremien oder die Eigner des Zertifizierungsprogramms legen die Kriterien für die Zertifizierung des Datenschutzes fest, die anschließend von der zuständigen Aufsichtsbehörde oder dem EDSA genehmigt werden. Nähere Informationen über Zertifizierungssysteme können den Zertifizierungsleitlinien[42] des EDSA und weiteren auf der Website des EDSA veröffentlichten relevanten Leitlinien entnommen werden.

91. Auch wenn ein Verarbeitungsvorgang nach Artikel 42 zertifiziert wurde, bleibt der Verantwortliche weiterhin für die kontinuierliche Überwachung dieses Vorgangs und für die Verbesserung der Einhaltung der in Artikel 25 genannten Kriterien für den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen verantwortlich.

5 DURCHSETZUNG VON ARTIKEL 25 UND AUSWIRKUNGEN

92. Die Aufsichtsbehörden können die Einhaltung von Artikel 25 gemäß den Verfahren nach Artikel 58 überprüfen. Die Abhilfebefugnisse werden in Artikel 58 Absatz 2 behandelt und beinhalten

[42] EDSA, „Leitlinien 1/2018 für die Zertifizierung und Ermittlung von

Zertifizierungskriterien nach den Artikeln 42 und 43 der

Verordnung (EU) 2016/679“, Version 3.0, 4. Juni 2019,
edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_de.pdf

Warnungen, Verwarnungen, Anweisungen zur Wahrung der Rechte der betroffenen Personen, Beschränkungen oder Verbote der Verarbeitung, Geldbußen usw.

93. Der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ist weiterhin ein Faktor für die Festlegung der Höhe von Geldbußen bei Verstößen gegen die DSGVO, vgl. Artikel 83 Absatz 4.[43, 44]

6 EMPFEHLUNGEN

94. Auftragsverarbeiter und Hersteller werden in Artikel 25 zwar nicht direkt erwähnt, gelten jedoch hinsichtlich der Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als wichtige Akteure, denen bewusst sein sollte, dass die Verantwortlichen für die Verarbeitung personenbezogener Daten nur Systeme und Techniken mit integriertem Datenschutz verwenden dürfen.

95. Bei der Verarbeitung im Namen eines Verantwortlichen oder bei der Bereitstellung von Lösungen für Verantwortliche sollten Auftragsverarbeiter und Hersteller auf ihr Fachwissen zurückgreifen, um Vertrauen aufzubauen und ihre Kunden einschließlich KMU bei der Gestaltung/Beschaffung von Verarbeitungslösungen mit integriertem Datenschutz zu beraten. Dies wiederum bedeutet, dass die Produkte und Dienste den Erfordernissen der Verantwortlichen entsprechend gestaltet werden sollten.

96. Bei der Einhaltung von Artikel 25 sollte berücksichtigt werden, dass die *wirksame Umsetzung* der Grundsätze und des *Schutzes* der Rechte betroffener Personen in die geeigneten Maßnahmen für die Verarbeitung das wichtigste Ziel der Gestaltung ist. Die folgenden Empfehlungen richten sich sowohl an Verantwortliche als auch an Hersteller und Auftragsverarbeiter und dienen dazu, die Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu fördern und zu verbessern:
    - Die Verantwortlichen sollten den Datenschutz bereits in der *Anfangsphase* der Planung eines Verarbeitungsvorgangs berücksichtigen, also noch vor der Festlegung der Verarbeitungsmittel.
    - Für den Fall, dass der Verantwortliche einen Datenschutzbeauftragten eingesetzt hat, empfiehlt der EDSA, diesen Datenschutzbeauftragten aktiv in die Einbindung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in die Beschaffungs- und Entwicklungsverfahren und während des gesamten Verarbeitungslebenszyklus einzubeziehen.
    - Ein Verarbeitungsvorgang kann *zertifiziert* sein. Die Möglichkeit der Zertifizierung eines Verarbeitungsvorgangs bietet einem Verantwortlichen bei der Wahl zwischen verschiedenen Anwendungsprogrammen, Geräten, Diensten und/oder Systemen von Herstellern oder Auftragsverarbeitern für die Datenverarbeitung einen zusätzlichen Nutzen. Deshalb sollten die Hersteller bestrebt sein, den Nachweis dafür zu erbringen, dass der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen im Lebenszyklus der

[43] In Artikel 83 Absatz 2 Buchstabe d DSGVO ist festgelegt, dass bei der Verhängung von Geldbußen für Verstöße gegen die DSGVO der *Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen* gebührend zu berücksichtigen ist.
[44] Weitere Informationen zu Geldbußen finden sich in Artikel-29-Datenschutzgruppe, „Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679“, WP 253, 3. Oktober 2017, http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49781 – gebilligt durch den EDSA.

von ihnen entwickelten Verarbeitungslösung gewährleistet ist. Auch ein Gütesiegel kann betroffenen Personen bei ihrer Wahl zwischen verschiedenen Waren und Diensten Orientierungshilfe geben. Die Möglichkeit, eine Zertifizierung für eine Verarbeitung zu erlangen, kann für Hersteller, Auftragsverarbeiter und Verantwortliche ein Wettbewerbsvorteil sein und fördert zudem das Vertrauen der betroffenen Personen in die Verarbeitung ihrer personenbezogenen Daten. Wenn keine Zertifizierung angeboten wird, sollten die Verantwortlichen sich um sonstige *Garantien* bemühen, aus denen hervorgeht, dass die Hersteller oder Auftragsverarbeiter die Anforderungen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen erfüllen.

- Verantwortliche, Auftragsverarbeiter und Hersteller sollten ihre Pflichten in Bezug auf den besonderen Schutz von Kindern unter 18 Jahren und anderen schutzbedürftigen Gruppen bei der Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigen.
- Hersteller und Auftragsverarbeiter sollten bestrebt sein, die Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu erleichtern, um den Verantwortlichen dabei zu unterstützen, die Verpflichtungen nach Artikel 25 einzuhalten. Auf der anderen Seite sollten die Verantwortlichen keine Hersteller oder Auftragsverarbeiter wählen, deren Systeme sie nicht in die Lage versetzen oder sie dabei unterstützen, die Bestimmungen in Artikel 25 einzuhalten, da sie bei unzulänglicher Umsetzung dieser Bestimmungen zur Verantwortung gezogen werden.
- Hersteller und Auftragsverarbeiter sollten aktiv dazu beitragen, dass die Erfüllung der Kriterien in Bezug auf den Stand der Technik sichergestellt ist, und sie sollten Verantwortliche über etwaige Änderungen des Stands der Technik, die sich auf die Wirksamkeit der von ihnen eingeleiteten Maßnahmen auswirken können, informieren. Die Verantwortlichen sollten diese Anforderung als Vertragsklausel aufnehmen, um sicherzustellen, dass sie auf dem neusten Stand gehalten werden.
- Der EDSA empfiehlt den Verantwortlichen, Hersteller und Auftragsverarbeiter dazu aufzufordern, zu zeigen, inwiefern ihre Geräte, Anwendungsprogramme, Dienste oder Systeme den Verantwortlichen in die Lage versetzen, den Anforderungen der Rechenschaftspflicht in Bezug auf den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu entsprechen; dies geschieht beispielsweise durch die Verwendung zentraler Leistungsindikatoren, die die Wirksamkeit der Maßnahmen und Garantien für die Umsetzung der Grundsätze und Rechte belegen.
- Der EDSA unterstreicht, dass für die wirksame Umsetzung der Grundsätze und Rechte ein einheitlicher Ansatz notwendig ist, und ermutigt Verbände oder Gremien, die Verhaltensregeln nach Maßgabe von Artikel 40 erstellen, auch sektorspezifische Leitlinien für den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen aufzunehmen.
- Die Verantwortlichen sollten sich fair gegenüber den betroffenen Personen verhalten und transparent machen, wie sie die wirksame Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen beurteilen und nachweisen, in gleicher Weise, wie sie die Einhaltung der DSGVO nach dem Rechenschaftsgrundsatz nachweisen.
- Auf dem neuesten Stand der Technik beruhende, ausgereifte datenschutzfreundliche Technologien können als eine Maßnahme in Einklang mit den Anforderungen des

Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen angewandt werden, wenn sich dies im Rahmen eines risikobasierten Ansatzes als geeignet erweist. Datenschutzfreundliche Technologien decken für sich genommen die Verpflichtungen nach Artikel 25 nicht unbedingt ab. Die Verantwortlichen beurteilen, ob die Maßnahme im Hinblick auf die Umsetzung der Datenschutzgrundsätze und der Rechte der betroffenen Personen angemessen und wirksam ist.

- Für bestehende ältere Systeme gelten die gleichen Pflichten für die Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen wie für neue Systeme. Wenn die Einhaltung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen bei älteren Systemen nicht bereits gewährleistet ist und wenn keine Änderungen vorgenommen werden können, um den Verpflichtungen nachzukommen, erfüllt ein solches älteres System die Verpflichtungen zur Gewährleistung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen nicht und kann folglich für die Verarbeitung personenbezogener Daten nicht eingesetzt werden.
- Artikel 25 sieht keine Senkung der Anforderungen für KMU vor. Die Beachtung nachstehender Empfehlungen kann KMU die Einhaltung der Bestimmungen nach Artikel 25 erleichtern:
    - Führen Sie frühzeitig Risikobewertungen durch.
    - Beginnen Sie mit kleinen Verarbeitungsschritten und gehen Sie anschließend dazu über, den Umfang zu erweitern und die Komplexität zu erhöhen.
    - Versuchen Sie, vom Hersteller und Auftragsverarbeiter Garantien für die Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu erhalten, z. B. in Form einer Zertifizierung und der Bestätigung, dass Verhaltensregeln eingehalten werden.
    - Nehmen Sie die Dienste erfahrener Partner in Anspruch.
    - Informieren Sie sich bei Datenschutzbehörden.
    - Lesen Sie die Leitlinien der Datenschutzbehörden und des EDSA.
    - Halten Sie ggf. bestehende Verhaltensregeln ein.
    - Nehmen Sie professionelle Hilfe und Beratung in Anspruch.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)