Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO

Accountability

INHALT

Accountability

Gemäß Art. 5 Abs. 2 DS-GVO muss der für die Verarbeitung Verantwortliche die Einhaltung der im Absatz 1 des Artikels festgelegten Grundsätze der Verarbeitung personenbezogener Daten nachweisen können. Hieraus folgt eine umfassende Rechenschaftspflicht (engl.: „Accountability“) mit zahlreichen Dokumentations- und Nachweispflichten.

Präzisiert werden die Anforderungen an die Nachweispflicht in Art. 24 Abs. 1 DS-GVO. Hier wird festgelegt, dass der Verantwortliche den Nachweis zu erbringen hat, dass er Maßnahmen getroffen hat, die sicherstellen, dass die Verarbeitung gemäß der DS-GVO erfolgt.

Klare Vorgaben, wie die Nachweispflicht umzusetzen ist, macht die DS-GVO nicht. Die Formulierung in Art. 24 DS-GVO legt jedoch nahe, dass eine Art Datenschutz-Managementsystem (DSMS) zu implementieren ist, da festgelegt wird, dass die Maßnahmen überprüft und aktualisiert werden müssen. Es genügt also nicht, Maßnahmen einmalig festzulegen und zu implementieren, sondern die Wirksamkeit der ergriffenen Maßnahmen ist regelmäßig zu überprüfen und gegebenenfalls sind Anpassungen vorzunehmen. Die Nachweispflicht besteht ausschließlich gegenüber den Aufsichtsbehörden. Ein Verstoß gegen diese Pflichten kann mit Bußgeldern von bis zu 20 Mio. EUR bzw. bis zu 4 % des weltweit erzielten Jahresumsatzes geahndet werden.

Diese Praxishilfe soll einen Überblick vermitteln, welche Themen bei der Erfüllung der Rechenschaftspflicht eine Rolle spielen können. Diese erheben weder einen Anspruch auf Vollständigkeit, noch sind u. U. die Themen von allen Verantwortlichen zu berücksichtigen.

Es wird von der Art und den Zwecken der Verarbeitung personenbezogener Daten, der Qualität und Quantität der Daten sowie spezifischen Faktoren des Verantwortlichen, wie Größe, Geschäftsstrategie oder Risikosituation abhängen, welche der aufgezeigten Themenbereiche im jeweiligen Einzelfall zu bearbeiten sind.

Es empfiehlt sich zu den einzelnen Themenbereichen die von der GDD veröffentlichten Praxishilfen als vertiefende Lektüre hinzuzuziehen.

1. Überblick – Accountability nach Art. 5 DS-GVO

1.1 Umfang

Die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO umfasst zunächst sämtliche Grundsätze des Art. 5 Abs. 1 DS-GVO:

- „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“ (lit. a)
- „Zweckbindung“ (lit. b)
- „Datenminimierung“ (lit. c)
- „Richtigkeit“ (lit. d)
- „Speicherbegrenzung“ (lit. e)
- „Integrität und Vertraulichkeit“ (lit. f)

Präzisiert werden die Anforderungen an die Nachweispflicht durch Art. 24 Abs. 1 DS-GVO, wonach der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umsetzt, **um sicherzustellen und den Nachweis dafür erbringen zu können**, dass die Verarbeitung rechtmäßig erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

Accountability bedeutet einen Dreiklang aus Sicherstellung – Nachweis – Überprüfung.

Entsprechend der Vorgabe in Art. 24 Abs. 3 DS-GVO kann die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO bzw. eines genehmigten Zertifizierungsverfahrens gem. Art. 42 DS-GVO als Gesichtspunkt herangezogen werden, um den geforderten Nachweis zu erbringen.

In Erwägungsgrund 78 wird ausgeführt, dass der Verantwortliche zu Nachweiszwecken interne Richtlinien festlegen und Maßnahmen ergreifen sollte, die insbesondere den Grundsätzen des Datenschutzes durch Technik (Data Protection by Design) und durch datenschutzfreundliche Voreinstellungen (Data Protection by Default) genügen.

Die Erfüllung der Rechenschaftspflichten setzt immer eine Angemessenheitskontrolle und Risikobewertung voraus, vgl. Art. 24 Abs. 1 DS-GVO bzw. Erwägungsgrund 74.

1.2 Nachweis gegenüber der Datenschutzaufsichtsbehörde

Die Rechenschaftspflichten dienen nicht allein internen Zwecken, sondern vor allem dem Nachweis gegenüber der jeweiligen Aufsichtsbehörde. Artt. 5 Abs. 2 und 24 Abs. 1 DS-GVO stellen klar, dass die Beweislast für die Rechtmäßigkeit der Verarbeitung beim Verantwortlichen liegt.[1]

Gemäß Art. 58 Abs. 1 lit. a DS-GVO kann die Behörde den Verantwortlichen anweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Kontrollaufgaben erforderlich sind. Für einen Verstoß bemisst sich das Bußgeld nach Art. 24 Abs. 1 DS-GVO i.V.m. der jeweiligen Norm, welche die allgemeinen Verpflichtungen von Art. 5 DS-GVO konkretisiert.[2] Das kann im Einzelfall abhängig von der Norm, gegen die verstoßen wurde, zu einer Geldbuße von bis zu 20 Mio. EUR oder im Fall eines Unternehmens von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres führen.

1 Pötters in: Gola, DS-GVO, 2. Aufl. 2018, Art. 5 Rn. 34.

2 Jung, Datenschutz-(Compliance-)Management-Systeme, ZD 2018, S. 208, 209.

2. Sicherstellung der Accountability – Etablierung eines Datenschutz-Managementsystems

Aufgrund der hohen Anforderungen an die Rechenschafts- und Nachweispflichten, hat der Verantwortliche sicherzustellen, dass er seine Maßnahmen zur Umsetzung des Datenschutzes fortlaufend dokumentiert.[3] Dazu empfiehlt sich die Einführung eines Datenschutz-Managementsystems (DSMS). Dieses umfasst alle Elemente, die zum Steuern/Führen, Umsetzen, Kontrollieren/Prüfen und Weiterentwickeln im Datenschutz erforderlich sind. Durch einen systematischen Ansatz (z.B. PDCA-Modell[4]) soll eine permanente Verbesserung der Datenschutz-Situation in einer Organisation erreicht werden. Neben der Datenschutz-Organisation als Gesamtheit aller Maßnahmen (strukturell, prozessual, regelsetzend), die der Umsetzung des Datenschutzes dienen, umfasst das Datenschutz-Managementsystem auch Instrumente zur Analyse der aktuellen und Planung der gewünschten Situation, Führungsinstrumente zur Erreichung des gewünschten Verhaltens, Kontrollwerkzeuge zur Überprüfung der Wirksamkeit von Maßnahmen sowie Informations- und Kommunikationssysteme zur Vermittlung von Wissen und Know-how.

Ein DSMS ermöglicht das Erkennen von Risiken bei der Einhaltung der gesetzlichen Vorgaben und der organisationsinternen Regelungen (s. hierzu auch die GDD-Praxishilfe DS-GVO - Die Datenschutz-Richtlinie - Grundlagen, Grundstrukturen und typische Regelungsbereiche[5]) und ein angemessenes Risikomanagement im Sinne eines kontinuierlichen Verbesserungsprozesses. Es dient insbesondere als Nachweis gegenüber der Behörde, welche Maßnahmen ergriffen wurden und wie der Verantwortliche identifizierten Anpassungsbedarf abarbeitet.

2.1 Interne Vorgaben (Datenschutzrichtlinien, Arbeitsanweisungen)

Eine Datenschutzrichtlinie stellt nach Innen eine allgemeinverbindliche betriebliche Anweisung dar und sollte grundsätzlich für alle Beschäftigten der Organisation gelten. Richtlinien konkretisieren das Recht des Verantwortlichen (der Leitung), die Leistungspflicht der Beschäftigten nach Zeit, Inhalt und Ort sowie deren Beschäftigtenpflichten näher zu bestimmen und bringen konkret die spezifischen Anforderungen der Organisation mit den sich aus dem Datenschutzrecht ergebenden Anforderungen in Einklang. Informationen und praktische Hinweise zum Erstellen einer Datenschutzrichtlinie finden Sie in der GDD-Praxishilfe DS-GVO - Die Datenschutz-Richtlinie.

Hierarchische Durchsetzung in der Organisation

Von entscheidender Bedeutung für die Wirkung einer solchen Datenschutzrichtlinie ist eine klare Zuweisung von Rollen und Verantwortlichkeiten im Rahmen der Delegation von Aufgaben in der Datenschutz-Organisation[6]. Die nachgeordneten Organisationseinheiten (Abteilungen) sind jeweils in ihren Bereichen für die Durchsetzung verantwortlich und setzen die grundlegenden Prinzipien und Entscheidungen der Unternehmensleitung angepasst auf ihre jeweiligen Aufgabenbereiche um.

Vorrangige inhaltliche Ziele

Zu den von allen zu beachtenden Prinzipien gehören vor allem:

- >> Rechtmäßigkeit jeder Verarbeitung personenbezogener Daten sowie Überprüf- und Nachweisbarkeit durch korrekte Dokumentation
- >> Zweckbindung
- >> Datenminimierung
- >> Speicherbegrenzung

3 Wichtermann, Einführung eines Datenschutz-Management-Systems im Unternehmen, ZD, S. 421, 422; Kranig u.a., Datenschutz-Compliance nach der DS-GVO, 2. Aufl. 2019, S. 31.

4 zum PDCA-Model s.u. 3. Überprüfung der Maßnahmen

5 https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/PraxishilfeDSGVODieDatenschutzRichtlinie.pdf

6 S. hierzu GDD-Praxishilfe DS-GVO - Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung, Version 2.0, Stand August 2021, https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ds-gvo-verantwortlichkeiten-und-aufgaben-nach-der-ds-gvo-inkl-synopse

>> Datenrichtigkeit
>> Integrität und Vertraulichkeit
>> Umsetzung des „Datenschutzes durch Technik“ (Data Protection by Design)
>> Datenschutzfreundliche Voreinstellungen bei Verfahren und Produkten (Data Protection by Default)
>> Beachtung von Betroffenenrechten

Datenschutz-Managementsystem

Ein Datenschutz-Managementsystem ist eine Methode, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, zu organisieren, zu steuern und zu kontrollieren und stetig zu verbessern. Hierzu gehört im Wesentlichen

>> die Definition von Aufgaben und Rollen im Datenschutz durch Festlegung einer Datenschutz-Organisation und der Delegation von Aufgaben und Verantwortlichkeiten[7],
>> die Konkretisierung von rechtlichen und internen Anforderungen in Form von Richtlinien und Handbüchern zum Datenschutz[8],
>> die Festlegung datenschutzrechtlicher Prozesse (z.B. zur Umsetzung datenschutzrechtlicher Betroffenenrechte[9] und zum Umgang mit Datenpannen[10]),
>> Sensibilisierungs- und Schulungsmaßnahmen für die Beschäftigten in der Organisation,
>> Implementierung technischer und organisatorischer Maßnahmen einschließlich der Klassifizierung von Daten in Schutzklassen zur besseren Identifikation von Schutzbedarfen,
>> Dienstleistermanagement, um sicherzustellen, dass bei der Anbindung von Dienstleistern die erforderlichen datenschutzrechtlichen Verträge geschlossen werden
>> und die rechtzeitige Einbindung des Datenschutzbeauftragten[11].

Zur Erfüllung der Rechenschaftsverpflichtung sind diese Maßnahmen zu dokumentieren, inklusive eines risikobasierten Zeitplanes zur Abarbeitung der Aufgaben und regelmäßigen Überprüfung der Maßnahmen.

Generelle Anforderungen an Datensicherheit

Es ist unbedingt auf die Sicherheit der Datenverarbeitung zu achten. Wer diese Anforderungen für die jeweiligen Prozesse umsetzt, sollte sich aus einer entsprechenden Aufgabenzuweisung in der Organisation ergeben. Zertifizierungsmaßnahmen können einen wichtigen Baustein bilden, genügen für sich genommen aber nicht aus, um zu dokumentieren, dass für den jeweiligen Prozess dem Risiko angemessene Schutzmaßnahmen getroffen wurden.

Die Einhaltung definierter technischer und organisatorischer Maßnahmen sollte regelmäßig überprüft werden, einschließlich der Prüfung der Angemessenheit solcher Schutzmaßnahmen. Dies kann z.B. im Rahmen von internen oder externen Audits der IT-/Informationssicherheit, durch die Revision oder durch Datenschutzaudits erfolgen.

Dokumentation der Prozesse mit personenbezogenen Daten

>> Erstellung des Verzeichnisses von Verarbeitungstätigkeiten (VVT)

Zum VVT siehe unter Punkt 2.2 bzw. die GDD-Praxishilfe „Verzeichnis von Verarbeitungstätigkeiten“.

7 S.o. GDD-Praxishilfe DS-GVO – Verantwortlichkeiten…

8 S.o. GDD-Praxishilfe DS-GVO - Die Datenschutz-Richtlinie…

9 S. z.B. GDD-Praxishilfe DS-GVO - Transparenzpflichten bei der Datenverarbeitung, Version 2.1, Stand April 2018, https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ds-gvo-transparenzpflichten-bei-der-datenverarbeitung

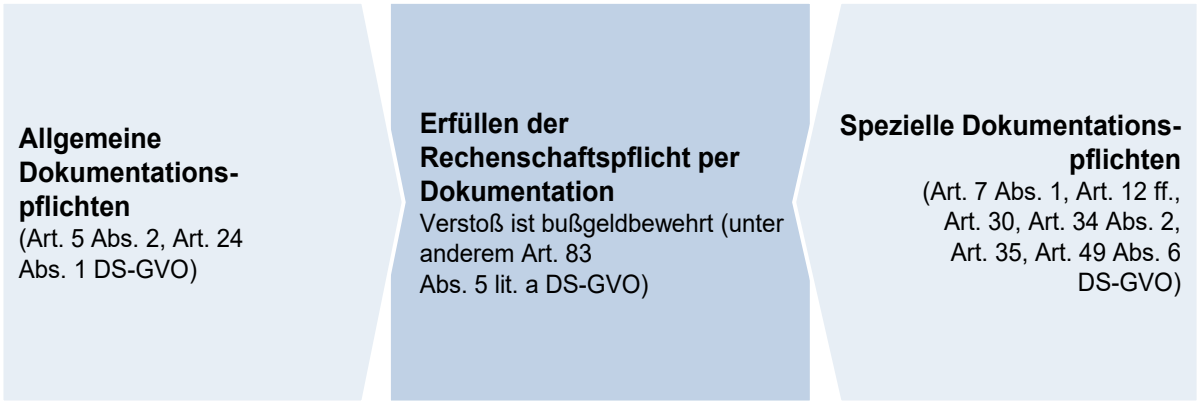
10 S. z.B. GDD-Ratgeber Datenpannen - Melde- und Benachrichtigungspflichten nach DS-GVO und BDSG, 3. Auflage, 2021.

11 S. z.B. GDD-Praxishilfe DS-GVO - Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung, Version 2.0, Stand Juli 2019, https://www.gdd.de/downloads/praxishilfen/gdd-praxishilfe_i_dsb-nach-ds-gvo_version-2.0; GDD-Ratgeber: Der betriebliche Datenschutzbeauftragte, 2. Aufl. 2019, Version 2.1.

>> Datenschutz-Folgenabschätzung[12]
>> Prozess zum Umgang mit Datenpannen[13]
>> Prozess zur Umsetzung von Betroffenenrechten[14]

Ein Praxisbeispiel für einen möglichen Aufbau einer Datenschutz-Richtlinie „Betroffenenrechte“ finden Sie in der GDD-Praxishilfe DS-GVO - Die Datenschutz-Richtlinie.

Dokumentations- und Nachweispflichten



Aus: Gola/Jaspers/Müthlein/Schwartmann, DS-GVO/BDSG im Überblick, 3. Aufl. 2018

Speziell für Auftragsverarbeiter insbesondere:

- Dokumentation der Weisungen
- Dokumentation der Weisungen für Drittlandstransfers
- Verzeichnis der Verarbeitungen nach Art. 30 Abs. 2

12 S. z.B. GDD-Praxishilfe DS-GVO - Voraussetzungen der Datenschutz-Folgenabschätzung, Version 1.0, Stand Oktober 2017, https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_10.pdf
13 S.o. GDD-Ratgeber Datenpannen
14 S.o. GDD-Praxishilfe DS-GVO - Transparenzpflichten

2.2 Dokumentation der Verarbeitungstätigkeiten

Zentraler Bestandteil einer strukturierten und transparenten Datenschutz-Dokumentation ist ein vollständiges und aktuell gehaltenes Verzeichnis der Verarbeitungstätigkeiten („VVT“).

Das VVT umfasst alle Verarbeitungstätigkeiten, mit denen die Geschäftsprozesse in der Organisation, wie z.B. Marketing und Vertrieb, die Beschaffung, das Personalmanagement usw. beschrieben werden. Als Pflichtangabe sind jeweils u.a. die Zwecke der Verarbeitung anzugeben. Hiermit lässt sich die Einhaltung der Zweckbindung aller Verarbeitungsvorgänge dokumentieren und nachhalten.

Ein entsprechendes Muster-VVT finden Sie in der GDD-Praxishilfe „Verzeichnis von Verarbeitungstätigkeiten“.

Bei Einführung oder Änderungen von einzelnen Verarbeitungstätigkeiten ist darauf zu achten, dass diese vom zuständigen Fachbereich zur Pflege des VVT gemeldet werden.

Die gemäß Art. 30 DS-GVO gebotene Beschreibung der Verarbeitungstätigkeiten umfasst wesentliche Elemente der Selbstprüfung und Accountability; weitere erforderliche Dokumente lassen sich zudem sinnvoll an das VVT „andocken“.

2.3 Datenschutz-Folgenabschätzung

Verarbeitungen, mit denen voraussichtlich ein hohes Risiko für die Persönlichkeitsrechte von betroffenen Personen verbunden ist, bedürfen einer Datenschutz-Folgenabschätzung (DSFA). Auch um zum Ergebnis zu kommen, dass/wo solche Risiken nicht vorliegen, bedarf es eines systematischen Ansatzes zur datenschutzrechtlichen Risikoanalyse, sog. Schwellwertanalyse[15]. Dies geschieht sinnvollerweise im Zuge der Erfassung der einzelnen Verarbeitungstätigkeiten. Somit bietet es sich an, auch die Dokumentation der Risikoanalysen und der DSFA an das VVT anzufügen.

2.4 Rechtmäßigkeit der Verarbeitung

Es empfiehlt sich, die jeweilige(n) Rechtsgrundlage(n) einer Verarbeitung personenbezogener Daten in das interne Formular zur Verarbeitungsmeldung[16] mit aufzunehmen und auch diese an das VVT „anzudocken“. So kann an dieser Stelle auch die zentrale Vorgabe der Rechtmäßigkeit der Verarbeitung dokumentiert werden. Weitere Informationen finden Sie in der GDD-Praxishilfe DS-GVO - Verzeichnis von Verarbeitungstätigkeiten.

Werden Datenverarbeitungen auf eine Einwilligung[17] gestützt, existiert eine Nachweispflicht: Verantwortliche müssen gemäß Art. 7 Abs. 1 DS-GVO den Nachweis des Vorliegens einer rechtsgültigen Einwilligung erbringen können. Die Nachweispflicht erstreckt sich auf

- Freiwilligkeit,
- Bestimmtheit,
- Zweckbindung,
- Informiertheit sowie
- Ausdrücklichkeit in den Fällen des Art. 9 Abs. 2 lit. a, Art. 22 Abs. 2 lit. c sowie Art. 49 Abs. 1 lit. f DS-GVO.

15 Vgl. Erwägungsgrund 75 VO (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 (Datenschutz-Grundverordnung).

16 Ein Muster für eine Verarbeitungsmeldung findet sich in der GDD-Praxishilfe DS-GVO - Verzeichnis von Verarbeitungstätigkeiten, Version 2.0, Stand März 2020, https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ds-gvo-verzeichnis-von-verarbeitungstaetigkeiten

17 S.a. GDD-Praxishilfe DS-GVO - Einwilligung, Version 1.1, Stand Mai 2018, https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ds-gvo-einwilligung

Daher sollte sowohl der Inhalt der Einwilligung als auch die Tatsache der Einwilligung nachgewiesen werden können.

Die DS-GVO schreibt jedoch nicht vor, wie der Nachweis zu erbringen ist; bei elektronischen Einwilligungen wird regelhaft eine Protokollierung für den Nachweis eingesetzt[18].

2.5 Gewährleistung von Rechten der betroffenen Person

Das Herstellen einer umfassenden Transparenz der Verarbeitung[19] der personenbezogenen Daten ist wesentliche Verpflichtung der Accountability nach Art. 5 DS-GVO. Zum Nachweis der Umsetzung der Accountability ist organisationsbezogen und risikoorientiert zu jedem einzelnen Element der Betroffenenrechte zu prüfen und zu dokumentieren, welche Prozesse und Maßnahmen bestehen.

Festlegung der Prozesse und Verantwortlichkeiten

In allen Fällen ist bei einer Umsetzung der Informationspflichten und Betroffenenrechte für eine klare Anweisungslage hinsichtlich der Prozesse, der Verantwortlichkeiten der Fachbereiche und Beschäftigten zu sorgen. Es empfiehlt sich, die Vorgehensweise durch die Leitung der Organisation schriftlich festzulegen (z.B. in Form einer Richtlinie zur Umsetzung datenschutzrechtlicher Betroffenenrechte) und die typischen Fragen, „wer ist zuständig für die Prüfung", „innerhalb welcher Frist ist die Antwort zu erteilen", „wie wird das Ganze innerhalb welcher Löschfristen dokumentiert", festzuhalten. Für Aufgabenzuweisungen eignen sich auch Verantwortlichkeitsmatrizen (z.B. RASCI, DEMI).

Wichtig hierbei ist im Sinne von Art. 24 Abs. 1 DS-GVO, dass die Maßnahmen risikoorientiert erfolgen, regelmäßig überprüft und aktualisiert werden.

Ein Beispiel für den Aufbau einer Richtlinie Betroffenenrechte finden Sie in der GDD-Praxishilfe DS-GVO - Die Datenschutz-Richtlinie.

Transparenzpflichten (Artt. 13 und 14 DS-GVO)

Die Transparenzverpflichtung unterscheidet sich, je nachdem, ob die personenbezogenen Daten direkt beim Betroffenen (Art. 13 DS-GVO) oder nicht bei ihm (Art. 14 DS-GVO) erhoben wurden. Die Umsetzung wird durch Einbindung der Informationen in Datenschutzhinweise bei Produkten und bei Prozessen auf Basis der jeweiligen Interessenten- und Kundenkontakte umgesetzt.

Im Hinblick auf die Accountability ist es entscheidend, dass der Verantwortliche festlegt, wer dabei welche Aufgabe wann wahrzunehmen hat (z.B. wer ist verantwortlich für die Erstellung der Information, wer bindet diese Person bzw. Abteilung wann ein, z.B. bei Aufnahme eines Kontaktformulars oder einer weiteren Trackingtechnologie auf einer Webseite oder bei Erstellung eines neuen Geschäftsprozesses bzw. Produktes). Dabei ist auch zu berücksichtigen, wie dokumentiert wird, dass die Information der betroffenen Person vor der Erhebung (Art. 13 DS-GVO) oder bei der Erhebung innerhalb der Frist des Art. 14 DS-GVO zur Verfügung gestellt wurde. Nicht erforderlich ist die Bestätigung über den Erhalt oder das Einverständnis mit dem Inhalt der Datenschutzinformation. Bei der Datenschutzinformation handelt es sich nicht um vertragliche Klauseln, die nur mit Einverständnis des Betroffenen wirksam sind.

18 Besonderheiten bei der Dokumentation von Einwilligungen sind insbesondere zu beachten bei Kindern, soweit Art. 8 DS-GVO einschlägig ist, bei Beschäftigten (§ 26 Abs. 2 BSG), bei Telefonwerbung (§ 7a UWG).

19 S.o. GDD-Praxishilfe DS-GVO - Transparenzpflichten

Auch die Beschäftigten in der Organisation sind transparent über die Verarbeitung ihrer personenbezogenen Daten zu informieren. Es bietet sich an, über die Verarbeitungsvorgänge mit Beschäftigtendaten in einer Datenschutzinformation zu informieren, die zusammen mit dem Arbeitsvertrag ausgehändigt wird. Für Aktualisierungen der einmal erteilten Datenschutzinformation kann dann auf eine Intranetseite verwiesen werden. Alternativ eignet sich eine Übersendung per E-Mail, welche entsprechend zur Dokumentation gespeichert wird.

Fristen für die Informationspflichten aus Artt. 13, 14 DS-GVO

Für Informationen gem. Art. 13 DS-GVO wird auf den Zeitpunkt der Erhebung abgestellt. Für Art. 14 DS-GVO gilt längstens eine Frist von einem Monat, wenn nicht mit der betroffenen Person kommuniziert wird oder die Daten anderweitig offengelegt werden (Art. 14 Abs. 3 DS-GVO). Für Status-Mitteilungen gem. Artt. 15 bis 22 DS-GVO gilt die Pflicht zur unverzüglichen Mitteilung, spätestens aber innerhalb eines Monats nach Eingang des Antrags (Art. 12 Abs. 3 DS-GVO).

Näheres in der GDD-Praxishilfe DS-GVO „Transparenzpflichten bei der Datenverarbeitung".

Wahrung der Rechte der betroffenen Person (Artt. 15 bis 22 DS-GVO)

Neben der Umsetzung der Transparenzpflichten stehen der betroffenen Person weitere Rechte gegenüber dem Verantwortlichen zu. Dies sind:

- **Art. 15 DS-GVO – Auskunftsrecht der betroffenen Person**
- **Art. 16 DS-GVO – Recht auf Berichtigung**
- **Art. 17 DS-GVO – Recht auf Löschung („Recht auf Vergessenwerden")**
- **Art. 18 DS-GVO – Recht auf Einschränkung der Verarbeitung**
- **Art. 20 DS-GVO – Recht auf Datenübertragbarkeit**
- **Art. 21 DS-GVO – Recht auf Widerspruch**
- **Art. 22 DS-GVO – Automatisierte Entscheidungen im Einzelfall einschließlich Profiling**
- **Art. 7 Abs. 3 DS-GVO – Recht auf Widerruf von Einwilligungen**

Für die Erfüllung der Betroffenenrechte sind die in Art. 12 Abs. 3 DS-GVO genannten Fristen einzuhalten. Entsprechend dem Accountability-Grundsatz ist der Verantwortliche hierfür nachweispflichtig. Hierzu empfiehlt es sich, den Versand entsprechender Mitteilungen an die betroffene Person zu dokumentieren.

Darüber hinaus besteht nach Art. 19 DS-GVO eine Mitteilungspflicht an Empfänger personenbezogener Daten bei Datenberichtigung, Löschung und Einschränkung der Verarbeitung.

Nachweis der Identität

Für alle Betroffenenrechte nach Artt. 15 bis 22 DS-GVO gilt: Der Verantwortliche muss im Rahmen der Geschäftsprozesse sicherstellen, dass tatsächlich nur der Berechtigte die Informationen und Mitteilungen erhält. Ein entsprechender Nachweis der Identität ist daher notwendig. Bei Zweifeln an der Identität des Anfragenden sind entsprechende Nachweise anzufordern, die zur Bestätigung der Identität erforderlich sind (Art. 12 Abs. 1, 2 und 6 DS-GVO). Hier bietet es sich an, Anforderungen zu definieren, was als Identitätsnachweis verlangt wird.

Fristen in der DS-GVO (Beispiele)

Frist	Fundort	Gegenstand
Unverzüglich	Art. 16, 17	**Erfüllung der Betroffenenrechte** Berichtigung, Löschung auf Antrag
	Art. 33 Abs. 2	Meldung von **Datenpannen durch Auftragsverarbeiter** an Verantwortlichen
	Art. 34 Abs. 1	Benachrichtigung des **Betroffenen bei Datenpannen** mit voraussichtlich hohem Risiko für Betroffene
Unverzüglich, möglichst binnen **72 Stunden** nach bekannt werden	Art. 33 Abs. 1	**Meldung von Datenpannen an Aufsichtsbehörden** Unverzüglich, möglichst binnen 72 Stunden nach bekannt werden der Datenpanne (Ausnahme, falls kein Risiko für Betroffene besteht) Bei späterer Meldung ist Begründung beizufügen Bei unzureichendem Inhalt der Meldung können Infos ohne unangemessene weitere Verzögerung (schrittweise) nachgeliefert werden
Ohne Verzögerung [max. **ein Monat**]	Art. 12 Abs. 4 Artt. 15 - 22	**Kein Tätigwerden bei Antrag zu Rechten Betroffener** Ohne Verzögerung, spätestens innerhalb eines Monats nach Eingang des Antrags (mit Angabe von Gründen und Widerspruchsmöglichkeit)
Unverzüglich, [max. **ein Monat**] [**Ein Monat** für Fristverlängerung um max. **zwei Monate**]	Art. 12 Abs. 3 Artt. 15 - 22	Antwort auf **Anträge zu Rechten Betroffener** Unverzüglich, spätestens ein Monat nach Eingang des Antrags Ein Monat für Unterrichtung über Fristverlängerung mit Angabe von Gründen Verlängerung um max. zwei weitere Monate (komplexe Fälle oder hohe Anzahl)
angemessene Frist [max. ein Monat nach Erlangung]	Art. 14 Abs. 3 lit a)	Erfüllung der **Informationspflichten** bei Datenerhebung nicht beim Betroffenen Innerhalb einer angemessenen Frist, höchstens jedoch einen Monat nach Erlangung der Daten
Zeitpunkt der Erhebung	Art 13. Abs. 1 und 2	Erfüllung der **Informationspflichten** bei Datenerhebung beim Betroffenen
Vor Weiterverarbeitung	Art. 13 Abs. 3	Erfüllung der **Informationspflichten** bei Weiterverarbeitung zu anderem Zweck
	Art. 14 Abs. 4	Erfüllung der **Informationspflichten** bei Weiterverarbeitung zu anderem Zweck
Erste Kommunikation	Art. 21 Abs. 4	Hinweis an den Betroffenen auf das **Widerspruchsrecht** bei der Datenverarbeitung Spätestens zum Zeitpunkt der ersten Kommunikation
Erste Offenlegung	Art. 14 Abs. 3 lit b)	Erfüllung der **Informationspflichten** bei Datenerhebung nicht beim Betroffenen, wenn Daten zur Offenlegung an anderen Empfänger bestimmt Spätestens zum Zeitpunkt der ersten Offenlegung
Erste Mitteilung	Art. 14 Abs. 3 lit b)	Erfüllung der **Informationspflichten** bei Datenerhebung nicht beim Betroffenen, wenn Daten zur Kommunikation mit Betroffenem bestimmt Spätestens zum Zeitpunkt der ersten Mitteilung

2.6 Verletzungen des Schutzes personenbezogener Daten

Bei einer Verletzung des Schutzes personenbezogener Daten betroffener Personen sieht die DS-GVO grundsätzlich eine Meldung an die Aufsichtsbehörde und – bei einem hohen Risiko - an betroffene Personen (Artt. 33 und 34 DS-GVO) vor. Nur wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, ist keine Meldung erforderlich.

Die interne Meldung potenzieller Datenschutzverletzungen, die Analyse der internen Meldungen und die Meldung von „Datenpannen" bzw. von Sicherheitsvorfällen ist wesentlicher Teil der Umsetzung der Accountability. Mit der Etablierung entsprechender Prozesse und der Dokumentation und Bewertung solcher Vorgänge, kann der Verantwortliche den Nachweis eines verantwortungsvollen Umgangs mit personenbezogenen Daten auch im Fall von Fehlverhalten erbringen.

Unabhängig davon, wie entschieden wurde, ist es zur Herstellung der Accountability notwendig, jede Verletzung des Schutzes personenbezogener Daten angemessen zu dokumentieren, einschließlich der getroffenen Entscheidung, keine Meldung abzugeben. In der Praxis hat es sich bewährt, ggf. in Abstimmung mit der lokalen Datenschutzaufsichtsbehörde, zu klären, in welcher Form das zu geschehen hat.

Unabhängig von einer Meldepflicht an die Aufsichtsbehörde ist jede Datenschutzverletzung inkl. zum Umgang mit ihr getroffenen Entscheidung, angemessen zu dokumentieren.

Die Meldefrist (unverzüglich, spätestens innerhalb von 72 Stunden) nach Art. 33 Abs. 1 DS-GVO stellt dabei regelmäßig eine besondere Herausforderung dar.

Weitere Informationen über die Voraussetzungen und Maßnahmen zur Erfüllung der Melde- und Benachrichtigungspflichten (inkl. Checklisten und Muster) finden Sie im GDD-Ratgeber Datenpannen (https://www.gdd.de/gdd-arbeitshilfen/gdd-ratgeber/datenpannen).

2.7 Löschkonzept und Datenlöschung

Im VVT sowie auch im Rahmen der Informationspflichten sind Angaben zur Dauer der Speicherung der verarbeiteten personenbezogenen Daten zu machen. Insoweit ist es erforderlich, ein Löschkonzept verfügbar zu haben, in dem die Aufbewahrungsfristen für die personenbezogenen Daten unter Berücksichtigung gesetzlicher und betrieblicher Vorgaben definiert sind. Darüber hinaus bedarf es entsprechender Dokumentationen, dass die Löschung personenbezogener Daten prozessual gewährleistet ist und auch tatsächlich durchgeführt wird.

Es gibt eine DIN-Norm für Löschkonzepte (DIN 66398), die bei der Etablierung des Konzepts und der entsprechenden Umsetzungsmaßnahmen hilfreich sein kann. Weitere Informationen – auch zur DIN 66398 – bietet der GDD-Ratgeber „Datenschutzgerechte Datenträgervernichtung - nach dem Stand der Technik"[20].

2.8 Technische und organisatorische Maßnahmen (TOMs)

Art. 32 Abs. 1 DS-GVO fokussiert auf die klassischen Schutzziele der IT-Sicherheit wie Vertraulichkeit, Integrität und Verfügbarkeit, ergänzt um die Belastbarkeit. Um beurteilen zu können, was ein angemessenes Schutzniveau nach Art 32. Abs. 1 DS-GVO ist, muss allerdings vorab geklärt

20 4. Auflage, 2019, https://www.gdd.de/gdd-arbeitshilfen/gdd-ratgeber/datenschutzgerechte-datentraegervernichtung-4-aufl-2019-1

werden, welchen Schutzbedarf die relevanten personenbezogenen Daten besitzen.

In der Praxis findet dabei häufig eine Orientierung an den Risikoklassen der IT-Sicherheit (kein, normales, hohes, sehr hohes Risiko) statt, die dann im Hinblick auf die Risikostufen der DS-GVO zu bewerten sind. Natürlich sind auch andere Risikobewertungsmodelle denkbar. Auf dieser Grundlage kann dann die Angemessenheit der technischen und organisatorischen Maßnahmen (TOMs) beurteilt werden.

Bei der Festlegung der TOMs sind neben Art, Umfang, Umstand und Zweck der Verarbeitung und den damit verbundenen Risiken für die betroffenen Personen auch der Stand der Technik und die Implementierungskosten zu berücksichtigen.

Der Verantwortliche ist im Rahmen der Accountability-Anforderungen verpflichtet, über die Beurteilung der Angemessenheit nach dem Stand der Technik entsprechende Nachweise zu erbringen. Im Rahmen einer dokumentierten Bestandsaufnahme ist daher zunächst der Status der implementierten TOMs festzustellen und gegenüber den definierten Risiken aus Sicht der betroffenen Personen zu bewerten und gegebenenfalls anzupassen. Diese Aufgabe obliegt dem Prozessverantwortlichen aus dem Fachbereich, der hierzu die fachlichen Vorgaben liefern muss. Ebenfalls ist zu prüfen, ob TOMs dem Stand der Technik entsprechen. Letztlich muss ein Prozess implementiert werden, der diese Kontroll- und Bewertungsmaßnahmen des Verantwortlichen regelmäßig wiederholt. Sofern ein Informationssicherheitsbeauftragter in der Organisation tätig ist, können diese Aufgaben von dieser Person wahrgenommen werden. Besteht eine solche Stelle nicht, bietet es sich an, dass die o.a. Aufgaben an entsprechend qualifizierte Beschäftigte (meist wohl aus der IT) oder qualifizierte Dienstleister übertragen werden. Entsprechende Überprüfungsmaßnahmen und Ergebnisse sind zur Erfüllung der Nachweispflichten zu dokumentieren. Gem. Art. 32 Abs. 1 lit. d DS-GVO ist zudem zur regelmäßigen Überprüfung ein Verfahren gefordert, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Datenschutz muss schon bei der Planung, Entwicklung und Gestaltung von Produkten, Diensten und Anwendungen Berücksichtigung finden (Data Protection by Design). Durch geeignete technische und organisatorische Maßnahmen ist zudem sicherzustellen, dass durch Voreinstellungen nur erforderliche personenbezogene Daten für den bestimmten Verwendungszweck verarbeitet werden (Data Protection by Default). Zum Nachweis der Erfüllung der Prinzipien Data Protection by Design und by Default empfiehlt es sich Checklisten zu erarbeiten, die bereits in der Konzeptions- und Entwicklungsphase von Produkten, Diensten und Anwendungen von den verantwortlichen Fachbereichen oder Projektgruppen genutzt und als Nachweis einer frühzeitigen und ganzheitlichen Berücksichtigung datenschutzrechtlicher Belange dient. Zur Erfüllung der Nachweispflichten sollten die ausgefüllten Checklisten dem VVT als Dokument beigefügt werden.

2.9 Zusammenarbeit mit Dienstleistern, Partnern und Lieferanten

Zum transparenten und effizienten Datenschutz-Management gehört auch der Überblick über die Vertragsbeziehungen mit Lieferanten, Auftragnehmern und sonstigen Geschäftspartnern, mit denen auch die jeweils datenschutzrechtlich gebotenen Vereinbarungen zu treffen sind, insbesondere Auftragsverarbeitungsverträge[21] oder auch Joint Controller-Vereinbarungen[22], Vertraulichkeitsvereinbarungen o.a.

21 S. a. GDD-Praxishilfe DS-GVO - Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO, Version 2.1, Stand Juni 2021, https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ds-gvo-mustervertrag-zur-auftragsverarbeitung-gemaess-art-28-ds-gvo

22 S. a. GDD-Praxishilfe DS-GVO - Joint Controllership, Version 1.0, Stand Dezember 2019, https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ds-gvo-joint-controllership

Insbesondere im Hinblick auf die vertraglich von Auftragsverarbeitern zugesagten TOMs kommt es zu Überschneidungen, da sie auch im Rahmen des VVT zu beschreiben sind. Unter anderem deshalb bietet es sich an, die Dokumentation des Vertragsmanagements an das VVT „anzudocken". Das gilt auch für die Überprüfung, ob der Vertragspartner angemessene Garantien für die Einhaltung der TOMs zur Verfügung gestellt hat. Elektronische Verarbeitungsverzeichnisse können diese Verzahnung der Dokumentation anbieten.

2.10 Übermittlung personenbezogener Daten an Drittländer

Die DS-GVO stellt besondere Anforderungen an die Übermittlung personenbezogener Daten an Drittländer (Drittlandstransfer), um ein der DS-GVO entsprechendes Schutzniveau sicherzustellen. Sofern ein Drittland kein auf Grundlage eines Angemessenheitsbeschlusses der EU-Kommission angemessenes Schutzniveau bietet, bedarf es geeigneter Garantien (i.d.R. Standard-Datenschutzklauseln oder Binding Corporate Rules).

In Reaktion auf das Schrems II-Urteil des EuGH und unter Geltung der Standardvertragsklauseln der EU von 2021 sind ggf. ergänzende, z.B. technische Schutzmaßnahmen zu treffen und zu dokumentieren, um unter Geltung dieser Standardvertragsklauseln ein angemessenes Datenschutzniveau beim Empfänger sicherzustellen.[23]

Um das Vorhandensein dieser Garantien nachweisen zu können, ist es erforderlich, im Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren, in welche Drittländer die personenbezogenen Daten transferiert werden und welche Garantien dafür vorliegen. Sofern der Abschluss von EU-Standardvertragsklauseln aufgrund der lokalen Rechtslage im Land des Datenimporteurs nicht ausreichend ist[24], sind die zusätzlich ergriffenen, insbesondere technisch-organisatorischen und vertraglichen Schutzmaßnahmen ebenfalls zu dokumentieren.

Das Vorhandensein der Garantien kann dann z.B. über das Vertragsmanagement nachgewiesen werden.

Je genauer der Verantwortliche die Informationen im Verzeichnis der Verarbeitungstätigkeiten pflegt, wohin die Daten transferiert werden und welche technischen und organisatorischen Maßnahmen zum Schutz der Daten umgesetzt sind, umso einfacher ist die Umsetzung neuer bzw. geänderter rechtlicher Anforderungen (z.B. infolge des Schrems II-Urteils identifizieren, welche Prozesse und in Anspruch genommene Dienstleister von dem Urteil betroffen sind und Risikominimierungsmaßnahmen ergriffen werden müssen).

Sofern der Drittlandstransfer allein auf eine Einwilligung gestützt wird, sind die unter Punkt 2.4 genannten Voraussetzungen zu beachten.

2.11 Schulungs- und Awareness-Maßnahmen

Wesentliche Voraussetzungen für eine funktionierende Datenschutz-Organisation ist die Schulung und Sensibilisierung der Beschäftigten in der Organisation. Daher sind die Herstellung und Bewahrung der Datenschutz-Awareness wesentliche Bausteine zur wirksamen Umsetzung des Datenschutzes beim Verantwortlichen und seiner Rechenschaftspflicht.

23 GRUR-Prax 2020, 436, 437 f.; NZBau 2021, 355, 359 f.
24 EuGH, Urteil vom 16.7.2020 – C-311/18 – DPC/Facebook Ireland Ltd. u. Schrems, NJW 2020, 2613.

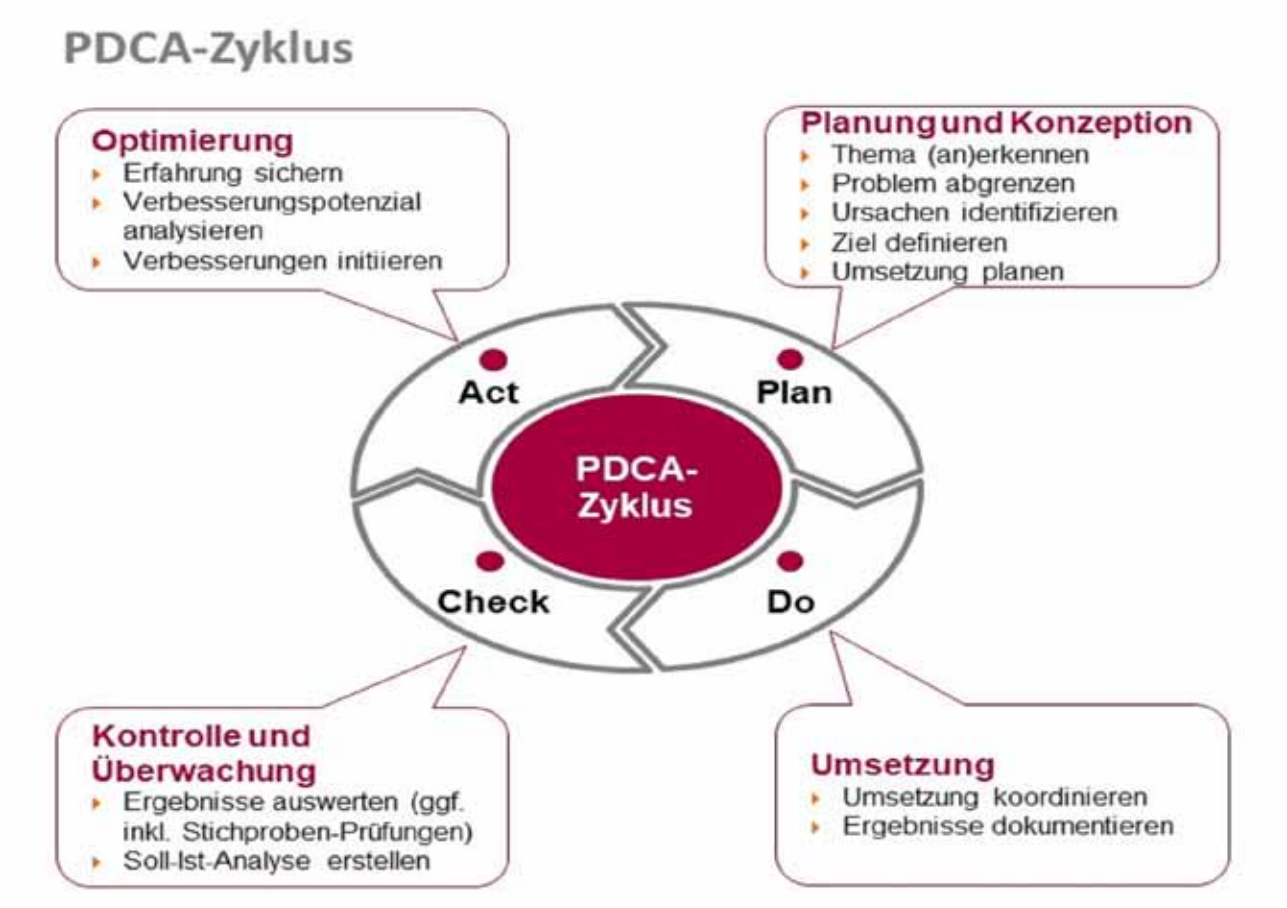
Die Organisation hat durch Schulung und Information sicherzustellen, dass sowohl neu eingestellte als auch schon länger beschäftigte Mitarbeiter/-innen nachweislich in die Thematik des Datenschutzes sowie in die datenschutzrelevanten Aspekte an ihrem Arbeitsplatz eingeführt werden.

Es empfiehlt sich ein modulares Schulungskonzept aufzusetzen, das sowohl allgemeine Basiskenntnisse im Datenschutz als auch fach- bzw. prozessspezifische Sachverhalte der Organisation berücksichtigt. Entsprechende Trainingsmaßnahmen können digital (z.B. eLearning-Programme, Informationen im Intranet, Datenschutz-Newsletter) oder in Präsenzveranstaltungen durchgeführt werden. In Abhängigkeit des Trainingskanals ist die Teilnahme der Beschäftigten elektronisch (z.B. in der Bildungshistorie des Beschäftigten) oder über Teilnehmerverzeichnisse und ggf. zusätzlich Teilnahmebescheinigungen zu dokumentieren.

3. Überprüfung der Maßnahmen

3.1 Kontinuierliche Verbesserung

Der sog. PDCA-Zyklus („Plan-Do-Check-Act“) nach Deming beschreibt einen kontinuierlichen Verbesserungsprozess und ist die Grundlage aller Managementsysteme. PDCA findet sich z.B. auch in der Norm ISO 27001 und der datenschutzrechtlichen Ergänzung ISO 27701. Zur Umsetzung datenschutzrechtlicher Anforderungen und der Erfüllung der Accountability genügt die einmalige Einführung eines Datenschutz-Managementsystems nicht. Es ist vielmehr eine regelmäßige Kontrolle der Einhaltung der Anforderungen sowie die Definition und Umsetzung von Verbesserungsmaßnahmen erforderlich. Nur so kann sichergestellt und nachgewiesen werden, dass jederzeit angemessene und wirksame Maßnahmen zur Einhaltung der datenschutzrechtlichen Vorgaben getroffen und vom Verantwortlichen ergriffen wurden.



3.2 Kontrollen und Audits

Zur Überprüfung der Einhaltung und der Wirksamkeit der Maßnahmen ist es unerlässlich, diese zu kontrollieren. Die Implementierung und Durchführung geeigneter prozessimmanenter Kontrollen zur Gewährleistung der Einhaltung der gesetzlichen und internen Vorgaben zum Datenschutz obliegt dabei den Fachbereichen (z.B. Prozesskontrollen, Kontrolle von Lieferanten). Abweichungen und Schwachstellen sollten dazu genutzt werden, erforderliche Anpassungsmaßnahmen zu initiieren und umzusetzen.

Auch Audits der internen Revision oder anderer Fachbereiche bzw. externer Auditoren können Aussagen über den Status und mögliche Verbesserungsmaßnahmen im Datenschutz liefern.

Sofern ein/e Datenschutzbeauftragte/r in der Organisation benannt wurde, gehört die kontinuierliche Überwachung der Einhaltung der jeweils aktuellen Datenschutzvorgaben auch seinen/ihren Aufgaben. Der/Die DSB kann dieser Aufgabe durch Nutzung und Auswertung der in der Organisation vorhandenen Kontrollinstrumente und Kennzahlen oder aber auch durch Verifizierung im Rahmen eigener Stichproben nachkommen und dies durch ein entsprechendes Reporting an die Leitung nachweisen.

4. Softwarelösung zur Umsetzung der Rechenschaftspflicht?

Jeder Verantwortliche muss sich Gedanken machen, mit welcher IT-Applikation er seinen Dokumentationspflichten nachkommen will. Ab einer gewissen Größenordnung stellen sich Unternehmen und sonstige Organisationen deshalb auch die Frage, ob sie nicht auf eine der marktgängigen Datenschutz-Management-Softwarelösungen zurückgreifen wollen. Diese Angebote werben damit, die Umsetzung der organisationsweiten Datenschutz-Maßnahmen zu vereinfachen und den Verantwortlichen bei der gesetzeskonformen Umsetzung zu unterstützen. Vor dem Hintergrund möglicher Audits und Prüfungen der Aufsichtsbehörde erscheint ein Dokumentenmanagementsystem, das gleichzeitig auch den Anforderungen der Aufsichtsbehörde sowie einer Zertifizierung bspw. nach ISO 27001 und 27701 entspricht, durchaus empfehlenswert. Dennoch können auch mit marktüblicher Software, z.B. durch Einsatz eines Tabellenkalkulationssystems mit entsprechenden Referenzen oder Verlinkungen zu den jeweiligen gesondert dokumentierten Prozessen (bzw. Applikationen) die Dokumentations- und Nachweispflichten erfüllt werden. Hierbei können die typischen Besonderheiten der jeweiligen Organisation individuell berücksichtigt werden.

Bei allen Lösungen ist zu beachten, dass die Ergebnisse sicher vor nachträglicher Veränderung gespeichert werden, was durch entsprechende Versionierung und Ablage auf vor Zugriffen und Veränderungen geschützten Laufwerken erfolgen kann. Auch sollte eine regelmäßige Sicherung und Archivierung der Daten - inkl. der Anwendung eines entsprechenden Löschkonzepts - erfolgen.

Anlage

Beispiele für direkte Dokumentations-pflichten

Fundort	Gegenstand
Art. 5 Abs. 2	Allgemeiner Grundsatz der **Accountability (Rechenschaftspflicht)** bei der Verarbeitung personenbezogener Daten nach den Prinzipien Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit
Art. 7 Abs. 1	Nachweis, dass eine rechtskonforme **Einwilligung** zur Datenverarbeitung vorliegt
Art. 24 Abs. 1	Nachweis erbringen, dass die Verarbeitung gemäß Verordnung (risikoadäquat) sichergestellt ist (**Datenschutz-Organisation**)
Art. 28 Abs. 3 lit. a)	Dokumentation von **Weisungen** des Auftraggebers
Art. 28 Abs. 3 lit. h)	Nachweise des Auftragsverarbeiters über die **Einhaltung des Art. 28 DS-GVO**
Art. 30 Abs. 1	Erstellen und Führen eines Verzeichnisses von Verarbeitungstätigkeiten – Verantwortlicher (**VVT**)
Art. 30 Abs. 1	Erstellen und Führen eines Verzeichnisses von Verarbeitungstätigkeiten – Auftragsverarbeiter (**VVT-AV**)
Art. 33 Abs. 5	Dokumentation von **Datenpannen** und deren Risiken und ergriffenen Maßnahmen
Art. 35 Abs. 7	Erstellen einer **Datenschutz-Folgenabschätzung** bei gegebenen Voraussetzungen
Art. 36 Abs. 3	**Vorherige Konsultation** der Aufsichtsbehörden bei hohem Risiko in der Verarbeitung und Bereitstellen von Informationen

Anlage

Beispiele für indirekte Dokumentations-pflichten

Fundort	Gegenstand
Art. 6, 8, 9, 10	**Rechtmäßigkeit der Verarbeitung** personenbezogener Daten muss nachgewiesen werden können
Art. 13, 14	**Informationspflichten** bei der Datenerhebung beim Betroffenen oder Dritten
Art. 12, 15, 16, 17, 18, 19, 20, 21	Dokumentation der effektiven Ausübbarkeit der **Betroffenenrechte**
Art. 22, 25	Nachweis der **datenschutzfreundlichen Prozessgestaltung** und **Produktanwendung**
Art. 28, 29	Dokumentation der korrekten Durchführung der **Auftragsverarbeitung** (beinhaltet Auswahl des Auftragsverarbeiters, vertragliche Regelung, Unterauftragsverhältnisse etc.)
Art. 32	Nachweis des Einsatzes geeigneter risikoadäquater **technisch-organisatorischer Maßnahmen** um angemessenes Schutzniveau zu gewährleisten
Art. 37, 38, 39	Korrekte Auswahl, Benennung, Stellung und Einbindung des betrieblichen **Datenschutzbeauftragten**
Art. 46, 47	Dokumentation geeigneter Garantien oder verbindlicher interner Datenschutzvorschriften bei **Datenübermittlung in Drittland**
Art. 82 Abs. 3	Haftungsentbindung für Schadensersatz bei Nachweis der rechtskonformen Verarbeitung (**Beweislastumkehr**)

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Mitglied werden? Mehr Informationen?

https://www.gdd.de/service/mitglied-werden oder eine E-Mail an: info@gdd.de

Eine Mitgliedschaft bietet wesentliche Vorteile:

>> Mitglieder-Nachrichten mit aktuellen Fachinformationen
>> Bezug der Fachzeitschrift RDV (Recht der Datenverarbeitung)
>> Beratung bei konkreten Einzelfragen
>> Zugriff auf Rechtsprechungs- und Literaturarchiv
>> Online-Service „Dataagenda Plus“ (Muster, Checklisten, RDV ONLINE Archiv, Arbeitspapiere etc.)
>> Mitarbeit in Erfahrungsaustausch- und Arbeitskreisen
>> Teilnahme an den kostenfreien GDD-Informationstagen sowie Vergünstigungen bei Seminaren u.v.m.

Schließen Sie sich unseren mehr als 3.800 Mitgliedern an. Eine Mitgliedschaft erhalten Sie schon ab 150,- EUR/Jahr für Privatpersonen und ab 300,- EUR/Jahr für Firmen.

Die Inhalte dieser Praxishilfe wurden im Rahmen des GDD-Arbeitskreises „DS-GVO Praxis“ erstellt unter Mitwirkung von:

- Dr. Ann-Katrin Dittschar, CLAAS KGaA mbH
- Michael Letter, 5medical-management GmbH
- Uwe Bargmann, Berater Datenschutzmanagement
- Thomas Müthlein, DMC - Datenschutz Management & Consulting; GDD-Vorstand

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 228 96 96 75-00
Fax: +49 228 96 96 75-25
www.gdd.de
info@gdd.de
Satz: C. Wengenroth (GDD-Geschäftsstelle)
Ansprechpartnerin: Yvette Reif, LL.M. (GDD-Geschäftsstelle)
Stand: Version 2.0 (Februar 2022)