Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO IX

Accountability

INHALT

Accountability

Gemäß Art. 5 Abs. 2 DS-GVO muss der für die Verarbeitung Verantwortliche die gesetzlich niedergelegten Grundsätze für die Datenverarbeitung einhalten und dies auch nachweisen können. Hieraus folgt eine umfassende Rechenschaftspflicht (engl.: „Accountability"), womit gegenüber dem bisherigen Recht zahlreiche zusätzliche Dokumentations- und Nachweispflichten entstehen. Die Accountability wird zukünftig einen gewichtigen Teil der betrieblichen Compliance darstellen.

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

1.1 Umfang

Die Rechenschaftspflicht 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)

Art. 5 DS-GVO wird ergänzt 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 ebenfalls als Gesichtspunkt herangezogen werden, um den geforderten Nachweis zu erbringen.

In Erwägungsgrund 78 wird ausgeführt, dass der Verantwortliche zu Nachweiszwecken interne Strategien 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 Rechenschaftspflichten stehen immer unter dem Vorbehalt einer Angemessenheitskontrolle und Risikobewertung, vgl. Art. 24 Abs. 1 DS-GVO bzw. Erwägungsgrund 74.

1.2 Behördliche Befugnisse

Die Rechenschaftspflichten dienen nicht allein internen Zwecken, sondern vor allem auch dem Nachweis gegenüber der jeweiligen Aufsichtsbehörde. Art. 5 Abs. 2 DS-GVO stellt 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. Ein Verstoß gegen Accountability-Pflichten ist gemäß Art. 83

1 Pötters in: Gola, DS-GVO, 2017, Art. 5 Rn. 34.

Abs. 5 lit. a DS-GVO mit einer Geldbuße von bis zu 20.000.000 € oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres bedroht.

2. Sicherstellung

2.1 Betriebliche Datenschutz-Policy

Eine betriebliche Datenschutz-Policy gibt den Mitarbeitern eine Orientierung über allgemein einzuhaltende Anforderungen. Eine generische Strukturierung könnte wie folgt aussehen.

Details können und sollten unternehmensspezifisch ergänzt werden.

Selbstbild des Unternehmens
Die Unternehmensleitung betrachtet die informationelle Selbstbestimmung und den Schutz der Daten als hohes Gut – sowohl in Hinsicht auf die Mitarbeiter, wie auch in Bezug auf andere Betroffene (Kunden, Geschäftspartner etc.).

Positive Darstellung der Ziele
Sie möchte den Verpflichtungen aus den rechtlichen Vorgaben zum Datenschutz (DS-GVO und nationale Normen) nachkommen und sorgt für ihre Durchsetzung im Unternehmen. Datenschutz-Compliance ist für das Unternehmen gegenüber Kunden und Mitarbeitern ein Qualitätsmerkmal.

Hierarchische Durchsetzung im Unternehmen
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 personenbezogenen Datenerfassung und -verwendung und Überprüfbarkeit durch korrekte Dokumentation
- >> Datensparsamkeit
- >> Umsetzung des „Datenschutzes durch Technik“ (Privacy by Design)
- >> Datenschutzfreundliche Voreinstellungen bei Verfahren und Produkten (Privacy by Default)
- >> Beachtung von Betroffenenrechten

Konkrete Ausprägung des Datenschutz-Managementsystems
Das Unternehmen führt ein Datenschutzmanagementsystem ein, bzw. betreibt bereits ein Datenschutzmanagementsystem, das auf die Anforderungen der europäischen Datenschutzgrundverordnung anzupassen ist. Dazu gehören:

- >> Schulungssystem, das an die Anforderungen der Tätigkeiten der Mitarbeiter angepasst ist und alle Ebenen entsprechend anspricht.
- >> Durchführung von Datenschutz-Folgenabschätzung vor der Einführung bzw. Änderung von Verfahren, wenn besondere Risiken für die Rechte und Freiheiten von Betroffenen zu erwarten sind.
- >> Ausrichtung der Vertragsbeziehungen mit internen und externen Dienstleistern auf die

DS-GVO

>> Risikobewertung und Risikomanagement
>> Bestellung/Einbindung eines/r Datenschutzbeauftragten

Generelle Anforderungen an Datensicherheit

Es ist unbedingt auf die Sicherheit der Datenverarbeitung zu achten.

>> Ggf. Zertifizierungsverfahren durchführen
>> Regelmäßige Datenschutzaudits durch DSB oder Dritte, generelle Anforderungen an die Datensicherheit

Besondere Verfahrensabläufe

Anordnungen für besondere Verfahrensabläufe

>> z.B. Erstellung des Verzeichnisses für Verarbeitungstätigkeiten (VVT)

Zum VVT siehe unten Punkt 3 bzw. die GDD-Praxishilfe V.

>> Datenschutz-Folgenabschätzung
>> Datenpannen

Datenschutzbeauftragte(r)

Die Unternehmensleitung hat zur Unterstützung dieser Vorgaben eine/n Datenschutzbeauftragte/n für das Unternehmen bestellt. Er/sie berät die Unternehmensleitung und Abteilungen bei der Entwicklung spezifischer Handlungsleitlinien (z.B. für Werbung, Mitarbeiterdatenschutz) und überprüft deren Einhaltung. Er/Sie erhält dafür von allen Organisationseinheiten die notwendige Unterstützung und wird frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängende Fragen eingebunden. Er/Sie ist unter [Kommunikationsdaten des/der DSB] für alle Abteilungen und betroffenen Personen ansprechbar.

Eine entsprechende Muster-Policy finden Sie in der GDD-Praxishilfe VIII.

2.2 Schulung/Unterweisung

Eine Sensibilisierung der mit Verarbeitungsvorgängen befassten Mitarbeiter und – besser noch – eine zielorientierte Schulung zum Datenschutz stellen generell eines der wichtigsten Mittel der Datenschutzorganisation dar, um präventiv auf datenschutzkonformes Handeln hinzuwirken. Inhaltlich sollte eine Erläuterung der Unternehmensrichtlinie zum Datenschutz am Anfang stehen und im Weiteren sollten schwerpunktmäßig alle Grundsätze für die Verarbeitung personenbezogener Daten abgedeckt werden.

Dabei empfiehlt sich ein zielgruppenspezifisches Training: Für Mitarbeiter, die „nur“ im betrieblichen Alltag mit personenbezogenen Daten zu tun haben, reicht wohl im Allgemeinen eine Sensibilisierungsmaßnahme, z.B. ein webbasiertes, anschauliches Informationsvideo. Dies ist auch deshalb sinnvoll, da jeder Mitarbeiter selbst ein Betroffener ist, und somit Datenschutz eben nicht nur Pflichten, sondern auch Rechte für den Mitarbeiter bedeutet. Jedes Unternehmen verarbeitet personenbezogene Daten von seinen Mitarbeitern und im Privatumfeld ist jeder ein Betroffener in vielfältigem Kontext. Mitarbeiter, die z.B. im Personalbereich, im Gesundheitsbereich oder sonst mit den Daten der besonderen Kategorien des Art. 9 DS-GVO zu tun haben, sollten deutlich intensiver geschult werden. Aber auch für diese Zielgruppe kann ein anspruchsvolles, webbasiertes Training geeignet sein.

Für besondere Gruppen oder spezifische Themen sollte man auch nicht den Aufwand eines Präsenz-

trainings scheuen. Themen, wie beispielsweise „Wie erfolgt eine haltbare Interessenabwägung?“, „Was sind angemessene Sicherheitsmaßnahmen?“, „Wie ist eine Risiko- und Datenschutzfolgeabschätzung durchzuführen?“, „Was heißt Privacy by Design/Default?“, „Was ist bei Datenübermittlungen in Drittstaaten zu beachten?“ werden bei den Verantwortlichen zu einem größeren Lernerfolg führen, wenn sie in einer Präsenzveranstaltung mit einem sachkundigen „Datenschützer“ diskutiert werden. Wichtig ist auch, dass die Teilnahme an den jeweiligen Schulungsmaßnahmen für die Teilnehmer verpflichtend ist und im Sinne der Nachweisbarkeit dokumentiert wird. Auch ist sicherzustellen, dass neue Mitarbeiter zeitnah geschult werden und Trainingsmaßnahmen in einem festgelegten Intervall, z. B. alle drei Jahre, stattfinden.

Wer letztendlich im Unternehmen für die Umsetzung dieser Sensibilisierungs- und Schulungsaufgaben verantwortlich ist, erschließt sich nicht unmittelbar aus der DS-GVO. Art. 24 DS-GVO weist dem für die Verarbeitung Verantwortlichen eine allgemeine Verantwortung zu, die geeigneten technischen und organisatorischen Maßnahmen umzusetzen, um eine verordnungskonforme Verarbeitung sicherzustellen. Zu solchen organisatorischen Maßnahmen zählt zweifellos auch ein zielgerichtetes Schulungskonzept.

Direkt spricht die DS-GVO das Thema der Sensibilisierung und Schulung der an Verarbeitungsvorgängen beteiligten Mitarbeitern an einer Stelle an: Art. 39 Abs. 1 lit. b DS-GVO weist dem Datenschutzbeauftragten die Aufgabe zu, die „Strategien“ des Unternehmens/Verantwortlichen zu überwachen, insbesondere auch in Bezug auf die Sensibilisierung und Schulung der Mitarbeiter. Das spricht dafür, dass der für die Verarbeitung Verantwortliche solche Schulungen zu organisieren hat. Andererseits hat der Datenschutzbeauftragte aber auch nach Art. 39 Abs. 1 lit. a DS-GVO die Aufgabe, die Beschäftigten zu der Verarbeitung von personenbezogenen Daten zu unterrichten und zu beraten.

Es bedeutet keine Interessenkollision, wenn der Verantwortliche „seine(n)“ Datenschutzbeauftragte(n) mit der Durchführung der Sensibilisierung und Schulung der Beschäftigten beauftragt.

2.3 Gewährleistung von Betroffenenrechten

Das Herstellen einer umfassenden Transparenz der Verarbeitung der personenbezogenen Daten ist wesentliche Verpflichtung der Accountability nach Art. 5 DS-GVO.

Hierzu gehört, dass zu jedem der folgenden Artikel der Nachweis erbracht wird, wie die Umsetzung im Unternehmen erfolgt ist. Zum Nachweis der Umsetzung der Accountability ist unternehmensbezogen und risikoorientiert zu jedem einzelnen Element der Betroffenenrechte zu prüfen und zu dokumentieren, welche Prozesse und Maßnahmen bestehen.

Art. 12 DS-GVO – Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

Diese Vorschrift ist als Leitlinie für die Umsetzung der Betroffenenrechte zu verstehen und legt Grundlagen für die Umsetzung der einzelnen Artikel fest.

Sprache und Form

Die Informationen und Mitteilungen sind gem. Art. 12 Abs. 1 DS-GVO in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln", insbesondere bei sich speziell an Kinder richtende Informationen. Es kann die schriftliche oder eine andere Form gewählt werden, „gegebenenfalls auch elektronisch". Die mündliche Information ist zulässig, sofern die Identität des Empfängers nachgewiesen wurde.

Nachweis der Identität

Für alle Betroffenenrechte 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).

Fristen

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. Art. 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).

Grundsatz der Unentgeltlichkeit

Gem. Art. 12 Abs. 5 DS-GVO gilt der Grundsatz der Unentgeltlichkeit hinsichtlich der Informationen und Mitteilungen, von dem nur ausnahmsweise bei offenkundig unbegründeten oder exzessiven Anträgen abgewichen werden kann. Wer sich auf die Ausnahme beruft, muss den Nachweis für die Unbegründetheit, bzw. den exzessiven Charakter erbringen.

Verwendung standardisierter Bildsymbole

Gem. Art. 12 Abs. 8 DS-GVO wurde der Kommission die Befugnis übertragen, die Herstellung der Transparenz durch Bereitstellung standardisierter Bildsymbole zu unterstützen. Hier gilt es, die weitere Entwicklung abzuwarten.

Herstellung der Anweisungslage

In allen Fällen ist bei einer unternehmensbezogenen Umsetzung der Betroffenenrechte für eine klare Anweisungslage hinsichtlich der Prozesse, der Verantwortlichkeiten der Fachbereiche und Mitarbeiter zu sorgen. Dies kann durch Geschäftsanweisungen, Bereichsrichtlinien, Prozessbeschreibungen und vieles mehr erfolgen. Wichtig hierbei ist im Sinne von Art. 24 Abs. 1 DS-GVO, dass die Maßnahmen risikoorientiert erfolgen, regelmäßig überprüft und aktualisiert werden.

Art. 13 und 14 DS-GVO – Transparenz

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, z.B. auch in AGBs, und bei Prozessen auf Basis der jeweiligen Interessenten- und Kundenkontakte umgesetzt. Wichtig ist die Berücksichtigung der Mitarbeiter von Unternehmen, die ebenfalls transparent über die Datenverarbeitungen bezogen auf die Mitarbeiterdaten einzubeziehen sind.

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

Art. 15 DS-GVO – Auskunftsrecht der betroffenen Person

Die bestehenden Auskunftsprozesse sind zu prüfen und entsprechend der neuen Regelungen, insbesondere auch der nun vorgegebenen Fristen, anzupassen.

Art. 16 DS-GVO – Recht auf Berichtigung

Es sind Prozesse bzw. Verfahren und Vorgehensweisen festzulegen, wie die betroffene Person die sie betreffenden Daten berichtigen (lassen) kann. Hierbei bietet es sich an gleichzeitig auch den Grundsatz der Richtigkeit der Daten gem. Art. 5 Abs. 1 lit. d DS-GVO in seiner Umsetzung zu dokumentieren. Eine angemessene Maßnahme kann sein, dem Betroffenen im Rahmen allgemeiner Vertragsbedingungen die Pflicht aufzuerlegen, bei Namens- oder Adressänderungen unverzüglich dem Verantwortlichen Mitteilung mit entsprechenden aussagekräftigen Nachweisen zu machen, damit die Daten korrigiert werden können.

Art. 17 DS-GVO – Recht auf Löschung („Recht auf Vergessenwerden")

Auch hier ist festzulegen, wie die betroffene Person ihr Recht auf Löschung wahrnehmen kann und insbesondere, wie im Einzelnen von dem Verantwortlichen geprüft wird, ob ein entsprechender Antrag begründet ist. Die Zulässigkeitsvoraussetzungen der Umsetzung eines Rechts auf Löschung ergibt sich aus Art. 17 Abs. 1 DS-GVO. Spezialregeln gelten gem. Art. 17 Abs. 2 DS-GVO für die Veröffentlichung von personenbezogenen Daten im Internet. Art. 17 Abs. 3 DS-GVO verneint ein Recht auf Löschung beim Vorliegen bestimmter Voraussetzungen. Es empfiehlt sich, die Vorgehensweise durch das Unternehmen als verantwortliche Stelle schriftlich festzulegen 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.

Art. 18 und 19 DS-GVO – Recht auf Einschränkung der Verarbeitung und Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung

In bestimmten Fällen ist gem. Art. 18 Abs. 1 DS-GVO das Recht auf Einschränkung der Verarbeitung gegeben. Auch hierzu sind betriebsintern anhand der jeweiligen Unternehmensstruktur die Umsetzung der jeweiligen Prozesse einschließlich Zuständigkeiten festzulegen.

Art. 20 DS-GVO – Recht auf Datenübertragbarkeit

Eine praxistaugliche Abgrenzung zur Ausübung der Auskunftsrechte gem. Art. 15 DS-GVO fehlt. Wichtig ist hier der Ansatz, zu prüfen, was die betroffene Person tatsächlich „bereitgestellt" hat. Hier bildet sich in der Praxis die Formel Input gleich Output heraus. Nur das, was der Betroffene tatsächlich bereitgestellt hat, muss herausgegeben werden.

Die Art. 29-Datenschutzgruppe hat hierzu das Working Paper 242 herausgegeben.

Die weitere, vor allem auch praxistaugliche Umsetzung des Rechts auf Datenübertragbarkeit bleibt abzuwarten. Hier muss jedes Unternehmen risikoorientiert entscheiden, wie die Umsetzung erfolgt.
Oftmals wird missverständlich behauptet, die Art. 29 Arbeitsgruppe hätte den Einsatz von PDF als unzulässig angesehen.[2]

Es kann hilfreich sein zu prüfen, wo für das jeweilige Unternehmen bereits Regelungen zu Informationspflichten im Sinne einer Datenübertragbarkeit bestehen – z.B. beim sog. Kontowechselservice der Banken gibt es bereits eine gesetzliche Vorgabe.[3]

Es bietet sich an, gegenüber Kunden die Möglichkeit einzuräumen, durch Downloads von Daten aus dem Kundenbereich in gängigen Formaten die Datenportabilität umzusetzen.

Art. 21 DS-GVO – Widerspruchsrecht
Es bietet sich an, die Umsetzung des Widerspruchsrechts zusammen mit den Verpflichtungen aus Art. 13 und 14 DS-GVO abzuarbeiten. Hierbei ist zu beachten, dass gem. Art. 21 Abs. 4 DS-GVO der Hinweis auf das Widerspruchsrecht u.a. in einer von anderen Informationen getrennten Form zu erfolgen hat.

Hier bietet es sich an, diese Trennung durch drucktechnische Hervorhebung umzusetzen.

Art. 22 DS-GVO – Automatisierte Entscheidungen im Einzelfall einschließlich Profiling
Es ist zu prüfen, ob automatisierte Entscheidungen einschließlich Profiling gem. Art. 22 Abs. 1 DS-GVO erfolgen und ob ggf. gem. Art. 22 Abs. 2 DDS-GVO Ausnahmen vorliegen- Die ergänzenden Maßnahmen aus Art. 22 Abs. 3 DS-GVO (u.a. Darlegung des eigenen Standpunkts und Anfechtung der Entscheidung) sind umzusetzen.

Vor allem ist das Verbot zu beachten, automatisierte Entscheidungen auf bestimmte besondere Kategorien personenbezogener Maßnahmen nach Art. 9 Abs. 1 DS-GVO zu stützen. Eine Ausnahme greift gem. Art. 22 Abs. 4 DS-GVO, wenn Art. 9 Abs. 2 lit. a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

Es ist jeweils unternehmensbezogen festzulegen, wie diese Vorgaben umzusetzen sind (Festlegung der Anweisungslage hinsichtlich Verantwortlichkeiten und Umsetzung).

2 WP 242, S. 14: „As an example, providing an individual with .pdf versions of an email inbox would not be sufficiently structured. E-mail data must be provided in a format which preserves all the meta-data, to allow the effective re-use of the data". Hieraus lässt sich nicht grundsätzlich ein Verbot des Einsatzes von PDF ableiten.
3 Gesetz zur Umsetzung der Richtlinie über die Vergleichbarkeit von Zahlungskontoentgelten, den Wechsel von Zahlungskonten sowie den Zugang zu Zahlungskonten mit grundlegenden Funktionen vom 11.04.2016, BGBl I 2016, S. 720 ff.

Art. 34 DS-GVO – Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person
Dieser Aspekt wird unter Punkt 2.4 gesondert behandelt.

2.4 Datenpannen

Mit der DS-GVO wird die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und an betroffene Personen (Art. 33 und 34 DS-GVO) auf alle verantwortlichen Stellen ausgedehnt. Die Meldung solcher „Datenpannen", bzw. von solchen Sicherheitsvorfällen ist wesentlicher Teil der Umsetzung der Accountability, denn nur so kann die verantwortliche Stelle den Nachweis des verantwortlichen Umgangs mit personenbezogen Daten auch für die Fälle erbringen, in denen Fehler auftreten, die „voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen" führen. Bei einem hohen Risiko sind auch die betroffenen Personen zu informieren.

Wer bislang unter die Mitteilungspflicht gem. § 42a BDSG a.F. gefallen ist, muss die bestehenden Meldeprozesse, insbesondere die Anweisungslage, aktualisieren und auf die neuen Anforderungen umstellen. Hier ist die Meldefrist von 72 Stunden nach Art. 33 Abs. 1 DS-GVO eine besondere Herausforderung.

Wer bislang noch keinen Meldeprozess für Datenpannen hat, sollte folgende Punkte beachten und unternehmensintern zur Dokumentation der Accountability des Unternehmens bei Verletzungen des Schutzes personenbezogener Daten regeln:

>> Klärung der Verantwortlichkeiten – d.h. Aufstellen eines Sicherheitsvorfall-Teams
> Erstellung, bzw. Verwendung eines von der zuständigen lokalen Datenschutzaufsicht vorgegebenen Meldeformulars, das die Anforderungen aus Art. 33 Abs. 3 DS-GVO abbildet
> Sicherstellen der Einhaltung der Frist von 72 Stunden

>> Abstimmung eventuell bestehender weiterer Verpflichtungen zum Melden von Sicherheitsvorfällen z.B. durch Informationssicherheit

>> Anweisungslage für alle Mitarbeiter herstellen durch Geschäftsanweisung, bzw. Arbeitsanweisung

>> Erstellung einer Dokumentation der Verletzungen des Schutzes personenbezogener Daten gem. Art. 33 Abs. 5 DS-GVO hinsichtlich Fakten, Auswirkungen und getroffener Abwehrmaßnahmen

>> Berücksichtigung von Outsourcing-Situationen
> Prüfung der Anweisungslage gegenüber den bisherigen Auftragsdatenverarbeitern gem. § 11 BDSG a.F.
> risikoorientierte Betrachtung vornehmen, insbesondere Meldefrist 72 Stunden berücksichtigen
> ggf. vertraglich bei Update von ADV gem. § 11 BDSG a.F. auf AV gem. Art. 33, 34 DS-GVO nachbessern

>> Information der Betroffenen gem. Art. 34 Abs. 1 DS-GVO
> Kommunikation der Verletzung inkl. der getroffenen Maßnahmen in klarer und einfacher Sprache
> Ergreifen vorbeugender Maßnahmen, um eine Pflicht zur Information der Betroffenen im Sinne von Art. 34 Abs. 3 DS-GVO entfallen zu lassen durch
> Ergreifen technisch-organisatorischer Maßnahmen, z.B. Verschlüsselung, um Daten unzu gänglich zu machen;

> Ergreifen nachgelagerter Maßnahmen, wenn das hohe Risiko aller Wahrscheinlichkeit nicht mehr besteht.

Da die verantwortliche Stelle Adressat der Meldepflichten gegenüber der Datenschutzaufsicht und den Betroffenen ist, sollte nach Klärung der Sachlage letztlich die Geschäftsleitung über die Meldung entscheiden.

Unabhängig davon, wie entschieden wurde, ist es zur Herstellung der Accountability notwendig, jeden Sicherheitsvorfall 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. Es ist zu erwarten, dass sich nach Einführung der DS-GVO europaweite Standards herausbilden werden, die vor allem auch Regelfälle umfassen in denen zu melden ist und solche, bei denen auf eine Meldung zu verzichten ist.

3. Nachweis

Herzstück eines transparenten und effizienten Datenschutzmanagements ist, wie schon bislang das Verfahrensverzeichnis, ein vollständiges, aktuell gehaltenes Verzeichnis der Verarbeitungstätigkeiten („VVT“).

Ein entsprechendes Muster-VVT finden Sie in der GDD-Praxishilfe V.

Die gem. 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“.

3.1 Rechtmäßigkeit

Das VVT umfasst alle Verarbeitungstätigkeiten, mit denen die Geschäftsprozesse im Unternehmen, 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. Es empfiehlt sich, in diesem Zusammenhang zusätzlich auch die jeweilige(n) Rechtsgrundlage(n) in das interne Erfassungsformular mit aufzunehmen. So kann an dieser Stelle auch die zentrale Vorgabe der Rechtmäßigkeit der Verarbeitung dokumentiert werden. Speziell die Rechtsgrundlage der Einwilligung muss strengen Rechtmäßigkeitsvorgaben entsprechen. Um die Umsetzung zu dokumentieren, kann das Muster der verwendeten Einwilligungserklärung dem entsprechenden VVT beigefügt werden.

3.2 Datenschutz-Folgenabschätzung (DSFA), bzw. sonstige Risikoabschätzungen

Verarbeitungen, mit denen voraussichtlich ein hohes Risiko für die Persönlichkeitsrechte von Betroffenen verbunden ist, bedürfen der Datenschutz-Folgenabschätzung (DSFA). Auch um zum Ergebnis zu kommen, dass/wo solche Risiken nicht vorliegen, bedarf es eines systematischen Ansatzes zur datenschutzrechtlichen Risikoanalyse. 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.

3.3 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. Für Verantwortliche gilt es demnach künftig auch die Belastbarkeit der Systeme und Dienste, die in Zusammenhang mit der Verarbeitung stehen, zu gewährleisten. Eine Orientierung an den bisherigen Kontrollpflichten gemäß § 9 BDSG a.F. nebst Anlage dürfte wohl weiterhin zulässig sein. Um beurteilen zu können, was ein angemessenes Schutzniveau nach Art 32. Abs. 1 DS-GVO ist, muss allerdings vorab geklärt werden, welchen Schutzbedarf die relevanten personenbezogenen Daten besitzen. Hierbei bietet es sich an, die Verarbeitungen in die Risikoklassen normal, hoch und sehr hoch einzuordnen. Natürlich sind auch andere Risikobewertungsmodelle denkbar. Auf dieser Grundlage kann dann die Angemessenheit der technischen und organisatorischen Maßnahmen (TOMs) beurteilt werden.

Die DS-GVO verlangt, dass bei den TOMs der Stand der Technik und die Implementierungskosten zu berücksichtigen sind.

Der Verantwortliche ist im Rahmen der Accountability-Anforderungen verpflichtet, über die Beurteilung der Angemessenheit sowie den 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 zu bewerten und gegebenenfalls anzupassen. 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 im Unternehmen 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 einen entsprechend qualifizierten Mitarbeiter (meist wohl aus der IT) übertragen werden. Entsprechende Überprüfungsmaßnahmen und Ergebnisse sind zur Erfüllung der Nachweispflichten zu dokumentieren.

3.4 Löschkonzept

Im VVT sowie auch im Rahmen der Informationspflichten sind Angaben zur Dauer der Speicherung zu machen. Insoweit ist es erforderlich, zumindest ein Löschkonzept verfügbar zu haben, welches die Grundsätze der im Hause praktizierten Löschungsroutinen widerspiegelt. Darüber hinaus bedarf es natürlich entsprechender Dokumentationen, dass die Löschung personenbezogener Daten prozessual gewährleistet ist und auch tatsächlich durchgeführt wird.

Es gibt inzwischen auch eine DIN-Norm für Löschkonzepte (DIN 66398), die bei der Etablierung des Konzepts und der entsprechenden Umsetzungsmaßnahmen hilfreich sein kann.

3.5 Datenminimierung

Die Datenminimierung ist ein wesentlicher Bestandteil des Privacy by Design und der datenschutzfreundlichen Voreinstellungen. Datenschutz muss schon bei der Planung, Entwicklung und Implementierung von IT-Systemen, -Prozessen,

Produkten und Dienstleistungen berücksichtigt werden. Bereits bei der Konzeption ist darauf zu achten, dass nur die personenbezogenen Daten verarbeitet werden, die für den verfolgten Zweck erforderlich sind (Datenminimierung). Im Rahmen der Entwicklung/Konzeption von IT-Systemen, -Prozessen, Produkten und Dienstleistungen sollte daher eine Checkliste bearbeitet werden. Zur Erfüllung der Nachweispflichten sollte die ausgefüllte Checkliste dem VVT als Dokument beigefügt werden.

3.6 Vertragsmanagement

Zum transparenten und effizienten Datenschutzmanagement gehört auch der Überblick über die Vertragsbeziehungen mit Kunden, Lieferanten und Auftragnehmern, mit denen auch die jeweils datenschutzrechtlich gebotenen Vereinbarungen zu treffen sind, insbesondere Auftragsverarbeitungsverträge oder auch Datenübermittlungsverträge, Vertraulichkeitsvereinbarungen o.a. 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.

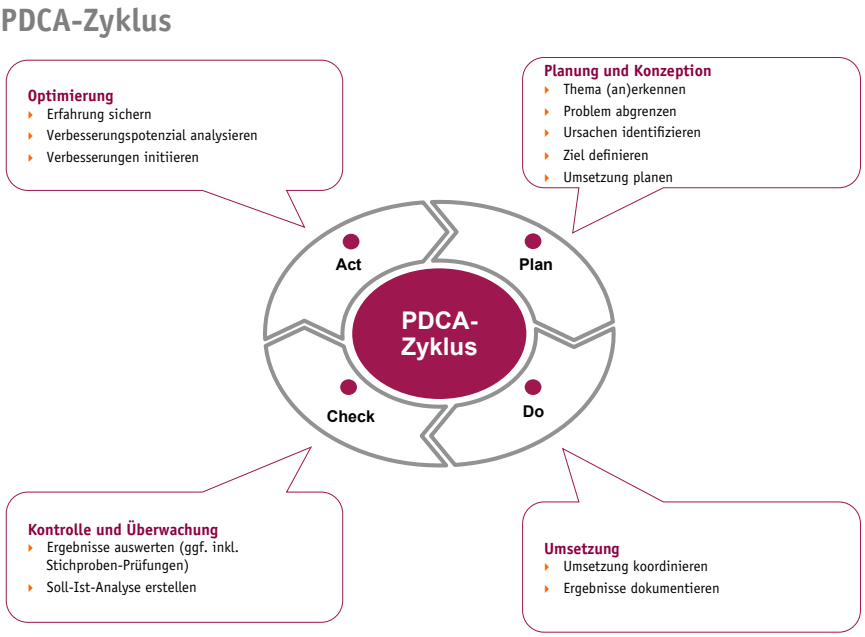
4 Überprüfung

4.1 PDCA

Der sog. PDCA-Zyklus („Plan-Do-Check-Act") nach Deming beschreibt einen kontinuierlichen Verbesserungsprozess und ist die Grundlage aller Qualitätsmanagement-Systeme. PDCA findet sich z.B. auch in der ISO 27001.

Gem. Art. 35 Abs. 11 DS-GVO führt der Verantwortliche Überprüfungen durch, um fortlaufend zu bewerten, ob die Verarbeitung gem. der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest dann, wenn hinsichtlich des Risikos Änderungen eingetreten sind. Gem. Art. 32 Abs. 1 lit. d DS-GVO ist zudem ein Verfahren gefordert zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Details zum PDCA-Zyklus finden Sie in der GDD-Praxishilfe DS-GVO II - Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung.



4.2 Softwarelösung zur Umsetzung der Rechenschaftspflicht?

Jeder Verantwortliche muss sich Gedanken machen, mit welcher IT-Applikation er seinen Dokumentationspflichten nachkommen will. Ab einer gewissen Größenordnung sollten sich Unternehmen und sonstige Organisationen deshalb auch die Frage stellen, ob sie nicht auf eine der marktgängigen Datenschutzmanagement-Softwarelösungen zurückgreifen wollen. Diese Angebote werben damit, die Umsetzung der unternehmensweiten 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 nach ISO 27001 (Compliance) entspricht, durchaus empfehlenswert.

Dennoch kann auch mit marktüblicher Software, z.B. durch Einsatz eines Tabellenkalkulationssystems mit entsprechenden Referenzen oder Verlinkungen zu den jeweiligen gesondert dokumentierten Prozessen (bzw. Applikationen) die Rechenschaftspflicht dokumentiert werden. Hierbei können die typischen Besonderheiten der jeweiligen Unternehmen 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. Marktübliche Softwarelösungen sollten diese Anforderungen schon von Haus aus abbilden.

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Die Inhalte dieser Praxishilfe wurden im Rahmen des GDD-Arbeitskreises „DS-GVO Praxis“ erstellt.

Satz: C. Wengenroth, GDD-Geschäftsstelle, Bonn

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 2 28 96 96 75-00
Fax: +49 2 28 96 96 75-25
www.gdd.de
info@gdd.de

Stand:
Version 1.0 (Oktober 2017)