7 Dokumentationspflichten in der DS-GVO[1]

Bisher galt das Prinzip, dass die Aufsichtsbehörde Verstöße eines Unternehmens gegen Datenschutzvorschriften belegen muss. Ein Unternehmen war nicht verpflichtet, anlasslos eine Dokumentation zu erstellen und zu pflegen, mit der es sein gesetzeskonformes Handeln nachweisen konnte. Dies wird sich mit der Geltung der Datenschutz-Grundverordnung grundlegend ändern. Dann müssen Unternehmen jederzeit in der Lage sein, die Rechtmäßigkeit ihrer Verarbeitung nachzuweisen. So kann zukünftig auch eine fehlende Dokumentation mit einem Bußgeld belegt werden – sogar dann, wenn die dazugehörige Verarbeitung rechtskonform erfolgt ist. Vor diesem Hintergrund sollte jedes Unternehmen ein Dokumentationssystem einführen oder das bereits vorhandene an die neue Rechtslage anpassen.

7.1 Einleitung

Der Dokumentation kommt in der Datenschutz-Grundverordnung (DS-GVO) eine größere Bedeutung zu als bisher. Die Bedeutung speist sich primär aus der in Art. 5 Abs. 2 DS-GVO eingeführten „Rechenschaftspflicht“:

„(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (‚Rechenschaftspflicht‘).“

Art. 24 Abs. 1 S. 1 DS-GVO konkretisiert die Anforderungen zur Erfüllung der Rechenschaftspflicht wie folgt:

„(1) Der Verantwortliche setzt […] geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. […]“

Die Nachweispflicht bezieht sich explizit auf die gesamte Verordnung und umfasst somit auch die folgenden Grundsätze der DS-GVO (Art. 5 Abs. 1 DS-GVO):

- Rechtmäßigkeit, Verarbeitung[2] nach Treu und Glauben und Transparenz,
- Zweckbindung,
- Datenminimierung,
- Richtigkeit,

1. Ursprünglich erschienen in RDV, Heft 4/2016, S. 197-203, Niels Lepperhoff, Dokumentationspflichten in der DS-GVO
2. Art. 4 Nr. 2 DS-GVO fasst unter „Verarbeitung“ alle Phasen von der Erhebung über die Nutzung bis zur Löschung zusammen. Die Trennung von Erhebung und Verarbeitung aus § 3 Abs. 3 und 4 BDSG wird aufgegeben.

© des Titels »Leitfaden zur Datenschutz-Grundverordnung « (ISBN 978-3-89577-798-1) 2017
by DATAKONTEXT GmbH, Frechen.
Nähere Informationen unter: http://www.datakontext.com

- Speicherbegrenzung sowie
- Integrität und Vertraulichkeit.

Diese Grundsätze werden durch die weiteren Vorschriften der DS-GVO konkretisiert, so dass ein nicht geführter Nachweis gemäß Art. 24 Abs. 1 DS-GVO regelmäßig auch den Nachweis nach Art. 5 Abs. 2 DS-GVO scheitern lässt. Ein Verstoß gegen Art. 5 DS-GVO ist mit einem Bußgeld bis zu 20 Mio. Euro oder – sofern höher – 4 Prozent des weltweiten Jahresumsatzes bewehrt.[3] Gelingt der Nachweis der Einhaltung nicht, ist bereits von einem Verstoß gegen Art. 5 Abs. 2 DS-GVO auszugehen. Die Frage, ob ein weitergehender Verstoß wie bspw. eine unzulässige Datenverarbeitung tatsächlich begangen wurde, kann dahinter zurücktreten.

Zusätzlich haften Auftraggeber und Auftragnehmer in einer Auftragsverarbeitung gesamtschuldnerisch, sofern ihnen der Nachweis des Unbeteiligtseins nicht gelingt.[4] Die DS-GVO bezeichnet mit dem Begriff „Auftragsverarbeitung“[5] die aus § 11 BDSG bekannte „Auftragsdatenverarbeitung“.

Die Dokumentation der Befolgung der DS-GVO in ihrer Gesamtheit wird von zentraler Bedeutung sein. Eine Betrachtung der DS-GVO, die sich auf wenige Artikel der DS-GVO konzentriert, neigt zum Verkennen der Sachlage.[6]

Im Folgenden werden die Anforderungen an die Dokumentation insbesondere für Unternehmen und andere nicht-öffentliche Stellen beleuchtet. Der Schwerpunkt der Betrachtung liegt auf den für alle Branchen geltenden Vorschriften, d.h. Bereichsregelungen bspw. aus Art. 89 DS-GVO bleiben unberücksichtigt. Für Unternehmen aus Drittstaaten gelten zusätzlich die Vorschriften nach Art. 27 DS-GVO zur Benennung eines Vertreters.

7.2 Anforderungen an ein Dokumentationssystem

Mit Blick auf eine praktische Umsetzung stellt sich die Frage nach Inhalt und Grenzen der Dokumentationspflicht. Art. 24 Abs. 1 DS-GVO umreißt die Grenzen mittels einer Abwägung zwischen

- den Implementierungskosten auf der einen Seite und
- der Verarbeitungsart,
- dem Verarbeitungsumfang,
- den Umständen und den Zwecken der Verarbeitung sowie

3. Art. 83 Abs. 5 Lit. a DS-GVO
4. Art. 82 Abs. 3 DS-GVO
5. Art. 28 DS-GVO
6. So Hansen-Oest, St. (2016): Datenschutzrechtliche Dokumentationspflichten nach dem BDSG und der Datenschutz-Grundverordnung. In: PinG, 02/2016, S. 84

© des Titels »Leitfaden zur Datenschutz-Grundverordnung « (ISBN 978-3-89577-798-1) 2017
by DATAKONTEXT GmbH, Frechen.
Nähere Informationen unter: http://www.datakontext.com

- der Wahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen (Mitarbeiter, Nutzer, Kunden, Lieferanten usw.) auf der anderen Seite.

Wo genau die Grenze verläuft, hängt folglich vom Einzelfall ab. Weiter spielt die Haftungsvermeidung, d.h. das Risiko zu minimieren, den Nachweis der Normbefolgung nicht erbringen zu können, eine nicht unerhebliche Rolle.

Aus den Vorschriften der DS-GVO lassen sich Mindestinhalte der Dokumentation ableiten. Diese speisen sich aus zwei Quellen:

- explizite Vorschriften wie z.B. das „Verzeichnis von Verarbeitungstätigkeiten“ nach Art. 30 DS-GVO und
- implizite Anforderungen.

Unter eine implizite Anforderung fallen Normen,

- deren Befolgung entweder durch eine Einzelvorschrift aus Haftungsgründen nachweisbar sein sollte oder
- deren Ergebnis von anderen Normen benötigt wird.

Ein Beispiel für den ersten Fall ist die Einhaltung der Reaktionsfrist bei einer Betroffenenanfrage von grundsätzlich einem Monat gemäß Art. 12 Abs. 3 DS-GVO. Eine Fristüberschreitung stellt einen bußgeldbewehrten Verstoß dar.[7]

Die Informationspflichten nach Art. 13 und 14 DS-GVO sind ein Beispiel für den zweiten Fall, da sie auch die Nennung der Rechtsgrundlagen umfassen, die deshalb bei der Umsetzung von Art. 6 DS-GVO dokumentiert werden sollten. Abbildung 7.1 zeigt – ohne Anspruch auf Vollständigkeit – zur Illustration eine Übersicht der Normen, die Auswirkungen auf die Dokumentation haben.

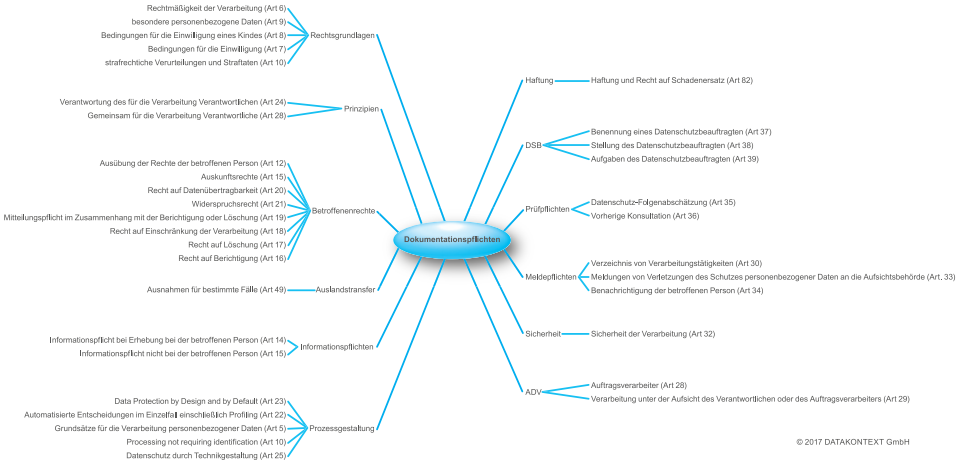

***Abb. 7.1:** Übersicht über Normen mit Auswirkungen auf die Dokumentation*

7. Art. 83 Abs. 5 Lit. b DS-GVO

© des Titels »Leitfaden zur Datenschutz-Grundverordnung « (ISBN 978-3-89577-798-1) 2017
by DATAKONTEXT GmbH, Frechen.
Nähere Informationen unter: http://www.datakontext.com

7.3 Inhalte der Dokumentation

Die DS-GVO trifft keine Aussagen, wie eine Dokumentation ausgestaltet sein soll. Das eröffnet Unternehmen Spielräume, vorhandene Systeme und Normen wie z.B. ISO 9001 für das Qualitätsmanagement oder ISO 27001 für das Informationssicherheitsmanagement einzubeziehen und im Rahmen eines unternehmensweiten Dokumentationssystems zu harmonisieren.

Im Folgenden wird exemplarisch der PDCA-Zyklus[8] aus dem Standard BSI 100-1 und der ISO 27001 zur Strukturierung der Dokumentation verwendet. Der hier dargestellte Zyklus bezieht sich auf das Unternehmen als Ganzes. Abbildung 7.2 zeigt beispielhaft welche Arten von Dokumenten welcher Phase zugeordnet werden können. Im Folgenden wird erläutert, welche Mindestinhalte sich für die einzelnen Phasen aus der DS-GVO ableiten lassen.

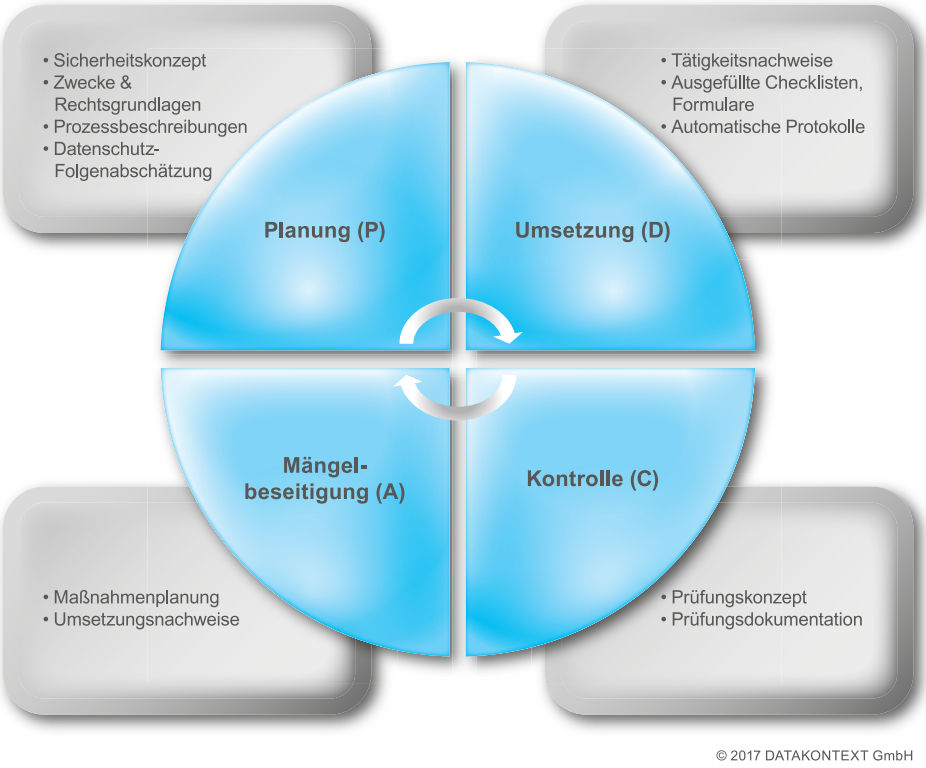

***Abb. 7.2:** PDCA-Zyklus als Strukturierungshilfe*

8. „P“ steht für Planung („plan“ im Englischen), „D“ für Umsetzung („do“), „C“ für Kontrolle („check“) und „A“ für Mängelbeseitigung („act“).

© des Titels »Leitfaden zur Datenschutz-Grundverordnung « (ISBN 978-3-89577-798-1) 2017 by DATAKONTEXT GmbH, Frechen.
Nähere Informationen unter: http://www.datakontext.com

7.4 Phase Planung

Die Planung legt das Fundament, dass die Verarbeitung im Einklang mit der DS-GVO erfolgt, sofern den Vorgaben der Planung entsprechend gehandelt wird. Aus Sicht der DS-GVO ist Folgendes zu dokumentieren:

- Zwecke,
- Rechtsgrundlagen insbesondere nach Art. 6-10 und die Datenübermittlung in Drittstaaten nach Art. 44-50 DS-GVO,
- etwaige Interessenabwägungen,
- das Sicherheitskonzept und
- Beschreibungen von Unternehmensprozessen.

7.5 Zwecke und Rechtsgrundlagen

Die Zwecke und Rechtsgrundlagen werden nicht nur zum Nachweis der Rechtmäßigkeit benötigt, sondern u.a. auch im Rahmen der Informationspflicht nach Art. 13 Abs. 1 Lit. c und 14 Abs. 1 Lit. c DS-GVO sowie für die Erstellung des Sicherheitskonzepts nach Art. 32 Abs. 1 DS-GVO. Weiterhin legen die Zwecke und Rechtsgrundlagen fest, ab wann die Löschpflicht nach Art. 5 Abs. 1 Lit. e DS-GVO greift.

7.6 Interessenabwägung

Eine Interessenabwägung sollte aus Nachweisgründen dokumentiert werden. Die Interessen des Verantwortlichen sind im Rahmen der Informationspflichten nach Art. 13 Abs. 1 Lit. d und Art. 14 Abs. 2 Lit. b DS-GVO offenzulegen.

7.7 Sicherheitskonzept

Das Sicherheitskonzept nach Art. 32 Abs. 1 DS-GVO gehört ebenfalls zur Planungsphase. Ein Element des Sicherheitskonzepts, um nach Art. 32 Abs. 4 DS-GVO „[…] sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten[…]“ ist das Berechtigungskonzept. Für Auftragsverarbeiter normiert Art. 29 DS-GVO mit Bezug zur Weisungsgebundenheit eine vergleichbare Vorgabe.

Das Protokollkonzept ist ein weiteres Element des Sicherheitskonzepts.

© des Titels »Leitfaden zur Datenschutz-Grundverordnung « (ISBN 978-3-89577-798-1) 2017
by DATAKONTEXT GmbH, Frechen.
Nähere Informationen unter: http://www.datakontext.com

7.8 Beschreibung der Unternehmensprozesse

Eine Beschreibung der Unternehmensprozesse ist aus zwei Gründen angeraten: Erstens verlangt Art. 32 Abs. 4 DS-GVO, sicherzustellen, dass Mitarbeiter oder andere Personen mit Zugang zu personenbezogenen Daten diese nur innerhalb der Weisungen des Unternehmens verarbeiten, sofern das europäische oder nationale Recht nicht zur Verarbeitung verpflichtet. Die spiegelbildliche Vorschrift in Art. 29 DS-GVO stellt ebenfalls die Weisungen ins Zentrum, indem sie den mit der Datenverarbeitung betrauten Personen eine Verarbeitung ohne Weisung untersagt. Prozessbeschreibungen und Arbeitsanweisungen stellen solche „Weisungen" zur Verarbeitung dar. Damit der Nachweis des „Sicherstellens" gelingen kann, empfiehlt es sich, alles zu dokumentieren, was als „Weisung" gewertet werden kann.

Zweitens gelten die in Art. 5 DS-GVO formulierten Prinzipien sowie die Regelungen des Art. 25 DS-GVO („Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen") für elektronisch ablaufende Prozesse. Eine entsprechend gestaltete Prozessbeschreibung hilft, die Einhaltung nachweisen zu können.

Um die Überwachung der Einhaltung von Datenschutzvorschriften nach Art. 39 Abs. 1 Lit. b DS-GVO zu planen, muss der Datenschutzbeauftragte eine Risikobetrachtung durchführen.[9] Im Rahmen der Prozessbeschreibung kann eine solche Risikobewertung zumindest vorbereitet werden.

Um die Betroffenenrechte in Bezug auf Einschränkung der Verarbeitung[10] und Widerspruch[11] umsetzen zu können, bietet es sich an, zu dokumentieren, wie Sperrmöglichkeiten für die jeweiligen Verarbeitungen auf Feld- und Personenebene umgesetzt werden.

Für automatische Einzelfallentscheidungen und Profiling sind weiterhin die Vorschriften aus Art. 22 DS-GVO im Rahmen der Dokumentation zu beachten.

Die DS-GVO setzt die Existenz einiger Prozesse zur Erfüllung ihrer Anforderungen voraus. Diese Prozesse sollten sowohl aus den oben genannten Gründen dokumentiert werden als auch als Nachweis, dass die Anforderungen aus der DS-GVO umgesetzt werden. Aus Platzgründen muss auf Detailbeschreibungen der folgenden Prozesse verzichtet werden:

- Umsetzung der Betroffenenrechte auf Information[12], Auskunft[13], Berichtigung[14], Löschung[15] und Einschränkung der Verarbeitung[16], Datenportabilität[17], Wider-

9. Art. 39 Abs. 2 DS-GVO
10. Art. 18 DS-GVO
11. Art. 21 DS-GVO
12. Art. 12 mit generellen und Art. 13 und 14 DS-GVO mit spezifischen Vorgaben
13. Art. 12 mit generellen und Art. 15 DS-GVO mit spezifischen Vorgaben
14. Art. 12 mit generellen und Art. 16 DS-GVO mit spezifischen Vorgaben
15. Art. 12 mit generellen und Art. 17 DS-GVO mit spezifischen Vorgaben
16. Art. 12 mit generellen und Art. 18 DS-GVO mit spezifischen Vorgaben
17. Art. 12 mit generellen und Art. 20 DS-GVO mit spezifischen Vorgaben

© des Titels »Leitfaden zur Datenschutz-Grundverordnung « (ISBN 978-3-89577-798-1) 2017
by DATAKONTEXT GmbH, Frechen.
Nähere Informationen unter: http://www.datakontext.com

spruch und Information der Datenempfänger[18] und die korrespondierenden Meldepflichten[19],

- Umsetzung der Sicherheitsanforderungen hinsichtlich Wirksamkeitsprüfung aller technischen und organisatorischen Maßnahmen[20], Dokumentation von Sicherheitsvorfällen[21], Meldung von Sicherheitsvorfällen an die Aufsichtsbehörde[22] und an den Betroffenen[23],
- Überprüfung der technischen und organisatorischen Maßnahmen zur Technikgestaltung und durch datenschutzfreundliche Voreinstellungen[24],
- Durchführung von Datenschutz-Folgenabschätzungen[25] ggf. mit vorheriger Konsultation der Aufsichtsbehörde[26],
- Information der Aufsichtsbehörde über Drittstaatentransfer[27],
- Information der Aufsichtsbehörde über und Veröffentlichung der Bestellung eines Datenschutzbeauftragten[28] und
- Dokumentation der erteilten Weisungen an den Auftragnehmer im Rahmen einer Auftragsverarbeitung durch den Auftraggeber[29].
- Im Rahmen von Auftragsverarbeitungen nach Art. 28 DS-GVO, im BDSG Auftragsdatenverarbeitungen genannt, kommen auf Seiten des Auftragnehmers folgende Prozesse zusätzlich zu den oben genannten hinzu:
- Meldung von Sicherheitsvorfällen an den Auftraggeber,[30]
- Auswahl eines (Unter-)Auftragnehmers,[31]
- Information des Auftraggebers über neuen Unterauftragnehmer[32] und
- Dokumentation der erhaltenen Weisungen[33].

18. Art. 12 mit generellen und Art. 21 DS-GVO mit spezifischen Vorgaben
19. Art. 12 mit generellen und Art. 19 DS-GVO mit spezifischen Vorgaben
20. Art. 24 Abs. 1 DS-GVO und Art. 32 Abs. 1 Lit. d DS-GVO
21. Art. 33 Abs. 5 DS-GVO. Die Dokumentationspflicht erstreckt sich auch auf Sicherheitsvorfälle, die keine Meldepflicht auslösen, da Abs. 5 keine Einschränkung wie Abs. 1 vorsieht.
22. Art. 33 Abs. 1-4 DS-GVO
23. Art. 34 DS-GVO
24. Konsequenz aus der in Art. 25 Abs. 1 und 2 DS-GVO genannten Forderung nach Sicherstellung
25. Art. 35 DS-GVO
26. Art. 36 DS-GVO
27. Art. 49 Abs. 1 DS-GVO
28. Art. 37 Abs. 6+7 DS-GVO
29. Art. 28 Abs. 3 Lit. a DS-GVO verlangt „dokumentierte“ Weisungen und Art. 29 DS-GVO bindet den Auftragsverarbeiter an diese Weisungen; im Rahmen der gesamtschuldnerischen Haftung können dokumentierte Weisungen zu einer Freistellung führen (Art. 82 Abs. 2 DS-GVO).
30. Art. 33 Abs. 2 DS-GVO
31. Art. 28 Abs. 1 und 4 DS-GVO
32. Art. 28 Abs. 2 DS-GVO
33. Art. 28 Abs. 3 Lit. a DS-GVO verlangt „dokumentierte“ Weisungen und Art. 29 DS-GVO bindet den Auftragsverarbeiter an diese Weisungen; Im Rahmen der gesamtschuldnerischen Haftung können dokumentierte Weisungen zu einer Freistellung führen (Art. 82 Abs. 2 DS-GVO).

© des Titels »Leitfaden zur Datenschutz-Grundverordnung « (ISBN 978-3-89577-798-1) 2017
by DATAKONTEXT GmbH, Frechen.
Nähere Informationen unter: http://www.datakontext.com

Da sich die Anforderungen gegenüber dem BDSG bspw. im Bereich der Betroffenenrechte oder Meldepflichten verändert haben, empfiehlt es, sich bestehende Prozesse auf Übereinstimmung mit den Vorgaben aus der DS-GVO zu überprüfen.

7.9 Phase Umsetzung

Prozessbeschreibungen, Arbeitsanweisungen, aber auch in Softwaresystemen hinterlegte Workflows lassen sich als Weisungen i.S.v. Art. 29 DS-GVO auffassen, die die mit der Verarbeitung der personenbezogenen Daten betrauten Personen – typischerweise Mitarbeiter – binden. Eine Verarbeitung ohne Weisung stellt einerseits einen Verstoß der Person gegen Art. 29 DS-GVO dar, aber auch einen Verstoß der Sicherstellungspflicht nach Art. 32 Abs. 4 DS-GVO durch das Unternehmen. Es ist zudem nicht ausgeschlossen, dass Auftragsverarbeiter mit dem Verstoß über Zwecke oder Mittel der Datenverarbeitung bestimmen, wodurch diese nach Art. 28 Abs. 10 DS-GVO zum für die Verarbeitung Verantwortlichen mit allen damit verbundenen Pflichten werden. Insofern ist es wesentlich, belegen zu können, dass die durch Prozessbeschreibungen, Arbeitsanweisungen und in Softwaresystemen hinterlegten Workflows gegebenen Weisungen befolgt werden. Solche Belege werden im Weiteren Protokolle und Protokollierung genannt.

Zu den Protokollen zählen weiterhin eingeholte Einwilligungen nach Art. 7 DS-GVO und die Prüf- und Nachweispflichten bei der Einwilligung von Kindern im Rahmen des Angebots von Diensten der Informationsgesellschaft nach Art. 8 DS-GVO. Die erfolgten Informationen nach Art. 13 und 14 DS-GVO sollten genauso für jeden Betroffenen protokolliert werden wie die Einhaltung der Meldepflichten nach Art. 33 und 34 DS-GVO. Diese Aufzählung ließe sich fortsetzen. Verallgemeinert zählt jeder Beleg im Rahmen der operativen Tätigkeit zu den Protokollen.

Protokolle werden häufig durch Protokollierungsfunktionen der verwendeten Programme, abgehakte Checklisten oder gespeicherte E-Mail-Korrespondenz auch heute schon bspw. im Rahmen von Qualitätsmanagementsystemen gesammelt. Auch Logfiles und andere Protokolle, die im Rahmen der IT-Sicherheit verarbeitet werden, sind ebenfalls zu berücksichtigen. Sie dienen einerseits der Umsetzung der Sicherheitsmaßnahmen nach Art. 32 DS-GVO und andererseits auch als Grundlage für die Wirksamkeitsüberprüfung nach Art. 32 Abs. 1 Lit. d DS-GVO.

Eine Protokollierung benötigt regelmäßig selbst einen Personenbezug, da für jede Person nachweisbar sein sollte, dass sie innerhalb der Weisungen handelt. Der Gesetzgeber hat zwar die Nachweispflicht – wie gezeigt – in der DS-GVO verankert, aber keine korrespondierende Rechtsgrundlage zur Protokollierung geschaffen. Somit verbleibt der Rückgriff auf die allgemeinen Normen des Art. 6 DS-GVO. Theoretisch denkbar wäre auch eine Einwilligung nach Art. 7 oder in bestimmten Fällen auch Art. 8 DS-GVO. In der Praxis ist eine Einwilligung jedoch keine geeignete Rechtsgrundlage für eine Dokumentation, da sie jederzeit widerrufen werden kann. Sie würde die Nachweisbarkeit damit in das Belieben der überwachten Person stellen. Es empfiehlt sich deshalb, in einem Protokollierungskonzept die für die einzelnen Protokolle einschlägigen Rechtsgrundlagen festzuhalten.

© des Titels »Leitfaden zur Datenschutz-Grundverordnung « (ISBN 978-3-89577-798-1) 2017
by DATAKONTEXT GmbH, Frechen.
Nähere Informationen unter: http://www.datakontext.com

7.10 Phase Kontrolle

Die Notwendigkeit zur Kontrolle, ob und in welchem Maß die datenschutzrechtlichen und unternehmensinternen Vorgaben eingehalten werden, ergibt sich bereits sachlogisch aus der Überlegung, dass Vorgaben, deren Einhaltung nicht überprüft, und Protokolle, die nicht ausgewertet werden, wirkungslos und damit überflüssig sind. Die Überwachung der Einhaltung gehört zu den gesetzlich festgelegten Überwachungsaufgaben des Datenschutzbeauftragten.[34] Für die Sicherheitsmaßnahmen normiert Art. 32 Abs. 1 Lit. d DS-GVO darüber hinaus eine eigenständige Prüfvorgabe für das Unternehmen.

Die Einhaltungskontrolle beschränkt sich nicht nur auf die zulässige Datenverarbeitung, sondern auch auf die unzulässige. Deshalb empfiehlt es sich, die Kontrolltätigkeiten so zu konzipieren, dass Regelübertretungen erkannt werden. Die Kontrollhandlungen und ergebnisse sollten als Nachweis dokumentiert werden.

Auf zwei Aspekte sei besonders hingewiesen:

Eine besondere Herausforderung sind Softwareanwendungen und Geräte, die mehr Daten verarbeiten als erforderlich. Diese sind regelmäßig nicht konform mit der DS-GVO einsetzbar,[35] so dass die Nutzung gegen Art. 25 Abs. 2 verstößt. Werden Daten, die nicht erforderlich sind, verarbeitet, liegt regelmäßig keine Rechtsgrundlage nach Art. 6-10 DS-GVO vor. Damit wird u.U. in der Folge zusätzlich gegen Art. 14 DS-GVO verstoßen. Bereits durch die Nutzung verstößt das Unternehmen gegen die DS-GVO, so dass die Frage, ob die Daten auch ausgewertet oder angeschaut werden, zurücktreten kann. Deaktivierte Funktionen sind hingegen unkritisch, da sie nicht ausgeführt werden, d.h. keine Wirkung zeigen. Es gilt deshalb, Softwareanwendungen und Geräte anhand ihrer Dokumentation und durch Funktionstest zu überprüfen. Diese Kontrolle erfolgt idealerweise vor der Beschaffung. Diese Kontrolle sollte auch Software as a Service und andere Clouddienste umfassen, da für die Rechtmäßigkeit (auch) der Auftraggeber verantwortlich ist.[36] Ob es sich um eine Auftragsverarbeitung i.S.v. Art. 28 DS-GVO handelt, ist unerheblich. Da Updates den Funktionsumfang verändern können, sollte nach einem Update die betroffene Anwendung oder das Gerät erneut auf unerlaubte Datenverarbeitung überprüft werden.

Die Datenschutz-Folgenabschätzung umfasst auch eine gesonderte Prüfpflicht, „ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird“[37].

34. Art. 39 Abs. 1 Lit. b DS-GVO und s. Kapitel 8.
35. Lepperhoff, N; Müthlein, Th. (2016): Neue Vorschriften auch für die Security. In: KES, 2/2016, S. 54 ff. und s. a. Kapitel 19
36. Müthlein, Th. (2016): ADV 5.0 – Neugestaltung der Auftragsdatenverarbeitung in Deutschland. S. Kapitel 23 und in RDV, 2/2016, S. 74-87.
37. Art. 35 Abs. 11 DS-GVO

© des Titels »Leitfaden zur Datenschutz-Grundverordnung « (ISBN 978-3-89577-798-1) 2017
by DATAKONTEXT GmbH, Frechen.
Nähere Informationen unter: http://www.datakontext.com

7.11 Phase Mängelbeseitigung

Der Unternehmensführung obliegt es, zusammen mit den Fachbereichen die festgestellten Mängel zu beheben. Sofern sich Änderungen bspw. in Software, Prozessen oder Konzepten ergeben, sind die jeweiligen Dokumente zu aktualisieren. Explizite Aktualisierungspflichten nennt die DS-GVO u.a. in Art. 24 Abs. 1 für die allgemeinen Maßnahmen, in Art. 32 Abs. 1 Lit. d für die Sicherheitsmaßnahmen und in Art. 35 Abs. 11 für die Datenschutz-Folgenabschätzung.

7.12 Das Verzeichnis von Verarbeitungstätigkeiten

Auch wenn das „Verzeichnis von Verarbeitungstätigkeiten“ nach Art. 30 DS-GVO auf den ersten Blick als eine zusätzliche Dokumentationspflicht angesehen werden kann, stellt es bei näherer Betrachtung eine besondere Zusammenstellung vorhandener Angaben dar. Tabelle 7.1 stellt den Inhalten dieses Verzeichnisses von Verarbeitungstätigkeiten die Vorschriften gegenüber, nach denen die jeweilige Information unabhängig von diesem Verzeichnis vorhanden sein muss.

Angaben in der Verarbeitungsübersicht für Verantwortliche[a]	**Bereits vorhanden wegen (Beispiel)**
Kontaktdaten des Datenschutzbeauftragten	Art. 37 DS-GVO
Zwecke der Verarbeitung	Art. 5 Abs. 1 Lit. b DS-GVO
Kategorien betroffener Personen	Art. 6 DS-GVO
Kategorien personenbezogener Daten	Art. 6 DS-GVO
Kategorien von Empfängern	Art. 6 DS-GVO
Drittstaatentransfer: Empfängerland oder internationale Organisation	Art. 44-46 DS-GVO
Drittstaatentransfer: Garantien	Art. 45-47 DS-GVO
Löschfristen	Art. 5 Abs. 1 Lit. e DS-GVO
allgemeine Beschreibung der technischen und organisatorischen Maßnahmen	Art. 32 DS-GVO

Tabelle 7.1: *Das Verzeichnis von Verarbeitungstätigkeiten kombiniert vorhandene Informationen*

a. Art. 30 Abs. 1 DS-GVO

© des Titels »Leitfaden zur Datenschutz-Grundverordnung « (ISBN 978-3-89577-798-1) 2017
by DATAKONTEXT GmbH, Frechen.
Nähere Informationen unter: http://www.datakontext.com

Die Pflicht zur Führung des Verzeichnisses entfällt, wenn jedes der folgenden Kriterien erfüllt ist:[38]

- weniger als 250 Mitarbeiter werden beschäftigt,
- die Verarbeitung birgt kein Risiko für die Rechte und Freiheiten der betroffenen Personen,
- die Verarbeitung erfolgt nur gelegentlich und
- es werden keine besonderen Datenkategorien nach Art. 9 Abs. 1 DS-GVO und keine Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten nach Art 10 DS-GVO verarbeitet.

Die Ausnahmen sind bei Licht betrachtet tatsächlich Ausnahmen. Regelmäßige Verarbeitungen scheitern an der Hürde „gelegentlich“. Weiterhin birgt die Verarbeitung personenbezogener Daten grundsätzlich ein Risiko für die Rechte und Freiheiten der betroffenen Personen, da in deren Persönlichkeitsrechte eingegriffen wird.[39] Es müssen deshalb grundsätzlich alle Verarbeitungen im Rahmen von definierten Prozessen in dem Verzeichnis aufgeführt werden, auch wenn das Unternehmen weniger als 250 Mitarbeiter beschäftigt.[40]

7.13 Fazit

Die Einhaltung der DS-GVO nachweisen zu können, sowie zahlreiche Vorgaben machen eine umfassende Dokumentation erforderlich. Die Herausforderung für eine praktische Umsetzung liegt in dem Erschließen und systematischen Zugänglichmachen bereits vorhandener Dokumente, die typischerweise in einzelnen Unternehmensbereichen mehr oder weniger als Insellösung vorhanden sind. Beispiele sind: Qualitätsmanagementsystem, IT-Betriebsdokumente, Protokolle von Anwendungen und Servern, Workflowdokumentation, Richtlinien, Prozessbeschreibungen, Checklisten und Arbeitsanweisungen.

Ein solches Dokumentationssystem wurde im BDSG nicht gefordert und stellt deshalb eine einschneidende Neuerung für Unternehmen dar.

38. Art. 30 Abs. 5 DS-GVO formuliert die Ausnahmen in negierter Form mit „oder“ verknüpft. Negiert man „Nicht A oder Nicht B“, ergibt sich „A und B“. Nach diesem Schema wurden die Kriterien in eine besser verständliche Form transformiert.
39. Vgl. 1. Erwägungsgrund der DS-GVO
40. So auch die Beurteilung des LDA Bayern, EU-Datenschutz-Grundverordnung (DS-GVO) – Das BayLDA auf dem Weg zur Umsetzung der Verordnung – V – Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO, Stand: 02.08.2016 (aktualisiert am 17.08.2016), *https://www.lda.bayern.de/media/baylda_ds-gvo_5_processing_activities.pdf*

© des Titels »Leitfaden zur Datenschutz-Grundverordnung « (ISBN 978-3-89577-798-1) 2017
by DATAKONTEXT GmbH, Frechen.
Nähere Informationen unter: http://www.datakontext.com