EINFÜHRUNG IN DIE DOKUMENTATIONS-PFLICHTEN GEMÄSS DSGVO[1]

Dr. Niels Lepperhoff

Von der Rechenschaftspflicht zur Dokumentation

Der Gesetzgeber greift eine Forderung der Art. 29-Gruppe aus 2010[2] auf, indem er mit Art. 5 Abs. 2 DSGVO die »Rechenschaftspflicht« für Unternehmen, Behörden, Vereine usw. (im Folgenden mit Unternehmen bezeichnet) einführt:

»(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (»Rechenschaftspflicht«).«

Art. 24 Abs. 1 S. 1 DSGVO konkretisiert die Rechenschaftspflicht weiter:

»(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 Kombination aus Rechenschaftspflicht und Nachweispflicht wirkt ähnlich einer Beweislastumkehr, d.h. Unternehmen müssen ihre »Unschuld« gegenüber der Aufsichtsbehörde beweisen (können). Für die Aufsichtsbehörde entfällt die Notwendigkeit, die »Schuld« zu beweisen, d.h. es kommt zukünftig auf die Fähigkeit, den »Unschuldsnachweis« führen zu können, an. Die Frage, ob ein weitergehender Verstoß wie bspw. eine unzulässige Datenverarbeitung tatsächlich begangen wurde, kann dahinter zurücktreten. Zusätzlich führen die Informationspflichten der Artt. 13 und 14 DSGVO zu einer größeren Transparenz gegenüber Betroffenen und mittelbar der Aufsichtsbehörde (Stichwort: Speicherdauer).

Die Folgen dieses Cocktails sollte nicht unterschätzt werden, da sie zu deutlich hören Compliance-Kosten führen werden, und mit einem Bußgeld von bis zu 20 Mio. Euro oder – sofern

1 Eine ausführliche Darstellung des Themas findet sich in Lepperhoff, N. (2016): Dokumentationspflichten in der DSGVO in: RDV 4/2016

2 Article 29 Data Protection Working Party (2010): Opinion 3/2010 on the principle of accountability. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

höher – 4 % des weltweiten Jahresumsatzes ein Risiko insbesondere für kleine und mittlere Unternehmen darstellen.

Grenzen der Dokumentationspflicht

Die Mindestinhalte für die Dokumentation ergeben sich aus den Vorschriften der DSGVO und speisen sich aus zwei Quellen:

- Explizite Vorschriften wie z. B. das »Verzeichnis von Verarbeitungstätigkeiten« nach Art. 30 DSGVO und
- Implizite Anforderungen.

Unter eine implizite Anforderung fallen Vorschriften,

- deren Befolgung entweder durch eine Einzelvorschrift aus Haftungsgründen nachweisbar sein sollte, z. B. fristgerechte Reaktion auf Betroffeneneingaben, oder
- deren Ergebnis von anderen Normen benötigt wird, z. B. Nennung der Rechtsgrundlagen in den Informationsplichten der Artt. 13 und 14 DSGVO.

Ob Sachverhalte, die nicht zu den Mindestinhalten zählen, dokumentiert werden müssen, lässt sich durch die Abwägung nach Art. 24 Abs. 1 DSGVO prüfen. Wo genau die Grenze verläuft, hängt folglich vom Einzelfall ab.

Aufbau und Inhalte eines Dokumentationssystems

Die DSGVO trifft keine Aussagen, wie eine Dokumentation ausgestaltet sein soll. Das eröffnet 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[3] aus dem Standard BSI 100-1 und aus der ISO 27001 zur Strukturierung der Dokumentation verwendet. Der hier dargestellte Zyklus bezieht sich auf das Unternehmen als Ganzes. Im Folgenden wird exemplarisch ohne Anspruch auf Vollständigkeit aufgezeigt, welche Mindestinhalte sich für die einzelnen Phasen aus der DSGVO ableiten lassen.

3 »P« steht für Planung (»plan« im Englischen), »D« für Umsetzung (»do«), »C« für Kontrolle (»check«) und »A« für Mängelbeseitigung (»act«).

Phase Planung

Die Planung legt das Fundament, dass die Verarbeitung im Einklang mit der DSGVO erfolgt, sofern den Vorgaben der Planung entsprechend gehandelt wird.

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

Interessensabwägung
Eine Interessensabwägung 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) DSGVO offenzulegen.

Sicherheitskonzept
Das Sicherheitskonzept nach Art. 32 Abs. 1 DSGVO gehört ebenfalls zur Planungsphase. Ein Element des Sicherheitskonzepts, um nach Art. 32 Abs. 4 DSGVO »[…] 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 DSGVO mit Bezug zur Weisungsgebundenheit eine vergleichbare Vorgabe.

Das Protokollkonzept ist ein weiteres Element des Sicherheitskonzepts (siehe Abschnitt 3.2).

Beschreibung der Unternehmensprozesse
Eine Beschreibung der Unternehmensprozesse ist aus zwei Gründen angeraten:

Erstens verlangt Art. 32 Abs. 4 DSGVO 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 DSGVO stellt ebenfalls die Weisungen ins Zentrum, in-

dem 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 DSGVO formulierten Prinzipien sowie die Regelungen des Art. 25 DSGVO (»Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen«) für elektronisch ablaufende Prozesse. Eine entsprechend gestaltete Prozessbeschreibung hilft die Einhaltung nachweisen zu können.

Für die Planung der Überwachung der Einhaltung von Datenschutzvorschriften nach Art. 39 Abs. 1 Lit. b) DSGVO muss der Datenschutzbeauftragte eine Risikobetrachtung durchführen.[4] Im Rahmen der Prozessbeschreibung kann eine solche Risikobewertung zumindest vorbereitet werden.

Die DSGVO setzt die Existenz einiger Prozesse, z. B. zu den Betroffenenrechte[5] und Wirksamkeitsprüfungen[6] zur Erfüllung ihrer Anforderungen voraus. Diese Prozesse sollten sowohl aus den obengenannten Gründen dokumentiert werden, als auch als Nachweis, dass die Anforderungen aus der DSGVO umgesetzt werden.

Phase Umsetzung

Prozessbeschreibungen, Arbeitsanweisungen aber auch in Softwaresystemen hinterlegte Workflows lassen sich als Weisungen i.S.v. Art. 29 DSGVO 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 DSGVO dar, aber auch einen Verstoß der Sicherstellungspflicht nach Art. 32 Abs. 4 DSGVO durch das Unternehmen. Es ist zudem nicht ausgeschlossen, dass Auftragsverarbeiter mit einem Verstoß über Zwecke oder Mittel der Datenverarbeitung bestimmen, wodurch diese nach Art. 28 Abs. 10 DSGVO 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 DSGVO und die Prüf- und Nachweispflichten bei der Einwilligung von Kindern im Rahmen des Angebots von Diensten der Informationsgesellschaft nach Art. 8 DSGVO. Die erfolgten Informationen nach Artt. 13 und 14 DSGVO sollten genauso für jeden Betroffenen protokolliert werden, wie die Einhaltung der Meldepflichten nach Artt. 33 und 34 DSGVO. 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 DSGVO und andererseits auch als Grundlage für die Wirksamkeitsüberprüfung nach Art. 32 Abs. 1 Lit. d) DSGVO.

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.[7] Für die Sicherheitsmaßnahmen normiert Art. 32 Abs. 1 Lit. d) DSGVO 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. ▶

[4] Art. 39 Abs. 2 DSGVO

[5] Art. 13-21 DSGVO

[6] Art. 32 Abs. 1 Lit. d DSGVO

[7] Art. 39 Abs. 1 Lit. b) DSGVO und Jaspers, A.; Reif, Y. (2016): Der Datenschutzbeauftragte nach der Datenschutzgrundverordnung: Bestellpflicht, Rechtsstellung und Aufgaben. In: RDV, 2/20165, S. 66.

Auf zwei Aspekte sei besonders hingewiesen:

- Softwareanwendungen und Geräte, die mehr Daten verarbeiten als erforderlich, sind regelmäßig nicht konform mit der DSGVO einsetzbar[8], so dass die Nutzung gegen Art. 25 Abs. 2 verstößt. Werden Daten, die nicht erforderlich sind, verarbeitet, liegt regelmäßig keine Rechtsgrundlage nach Artt. 6–10 DSGVO vor. Bereits durch die Nutzung verstößt das Unternehmen gegen die DSGVO, sodass die Frage, ob die Daten auch ausgewertet oder angeschaut werden, zurücktreten kann. Deaktivierte Funktionen sind hingegen unkritisch, da sie nicht ausgeführt werden. Es gilt deshalb Softwareanwendungen und Geräte anhand ihrer Dokumentation und durch Funktionstest vor der Nutzung und nach Funktionsändernden Updates zu überprüfen. Diese Kontrolle sollte auch Software as a Service und andere Clouddienste umfassen, da für die Rechtmäßigkeit (auch) der Auftraggeber verantwortlich ist.[9] Ob es sich um eine Auftragsverarbeitung i.S.v. Art. 28 DSGVO handelt, ist unerheblich.
- Die Datenschutz-Folgenabschätzung umfasst auch eine gesonderte Prüfpflicht, »ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird«.[10]

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 DSGVO 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.

Das Verzeichnis von Verarbeitungstätigkeiten

Auch wenn das »Verzeichnis von Verarbeitungstätigkeiten« nach Art. 30 DSGVO auf dem ersten Blick als eine zusätzliche Dokumentationspflicht angesehen werden kann, stellt es bei näherer Betrachtung eine besondere Zusammenstellung vorhandener Angaben dar.

Die Pflicht zur Führung des Verzeichnisses entfällt, wenn jedes der folgenden Kriterien erfüllt ist:[11]

- weniger als 250 Mitarbeiter werden beschäftigt und
- die Verarbeitung birgt kein Risiko für die Rechte und Freiheiten der betroffenen Personen und
- die Verarbeitung erfolgt nur gelegentlich und
- es werden keine besonderen Datenkategorien nach Art. 9 Abs. 1 DSGVO und keine Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten nach Art. 10 DSGVO 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.[12] 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.

Über den Autor

Niels Lepperhoff
Geschäftsführer der Xamit Bewertungsgesellschaft mbH und der DSZ Datenschutz Zertifizierungsgesellschaft mbH (einem Gemeinschaftsunternehmen des BvD e.V und der GDD e.V.).

▶ www.xamit.de

[8] Lepperhoff, N.; Müthlein, Th. (2016): Neue Vorschriften auch für den CISO. In: KES, 2/2016. S. 19.

[9] Müthlein, Th. (2016): ADV 5.0 – Neugestaltung der Auftragsdatenverarbeitung in Deutschland. In: RDV, 2/2016. S. 74-87.

[10] Art. 35 Abs. 11 DSGVO.

[11] Art. 30 Abs. 5 DSGVO 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.

[12] Vgl. 1. Erwägungsgrund der DSGVO