Rechenschafts- und Dokumentationspflichten als Teil der Datenschutzorganisation

1 Inhaltsverzeichnis

Andreas Hessel, Dellbornerstr. 42, 66679 Losheim am See
+ 49 176 805 420 79, andreas.hessel@privacy4b.de,
https://ds-ism.de
Steuernummer: 020 230 07684

2 Ausgangslage

Die DSGVO verlangt vom Verantwortlichen teilweise explizit eine Dokumentation bestimmter Vorgänge, so z.B. ein Verzeichnis der relevanten Verarbeitungstätigkeiten. An anderen Stellen der DSGVO ergibt sich eine implizite Dokumentationspflicht, weil der Verantwortliche nur auf diese Weise gegenüber den Prüfanforderungen der Aufsichtsbehörden die Einhaltung der Vorgaben der DSGVO nachweisen kann. Die Zwecke der Dokumentation bestehen also zum einen darin, die nach der DSGVO bestehenden Nachweispflichten zu erfüllen, und zum anderen darin, für Zwecke des Datenschutzmanagements jederzeit auf diese Dokumentation zurück greifen zu können. In der Praxis gehen Datenschutzorganisation und lückenlose Dokumentation Hand in Hand.

Gem. Art. 31 DSGVO werden Verantwortliche und Auftragsverarbeiter verpflichtet, auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten und gem. Art. 58 Abs.1 lit. a) und e) DSGVO alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Kommt man solchen aufsichtsbehördlichen Aufforderungen nicht nach, weil man keinerlei Dokumentation zu den zugrundeliegenden Verarbeitungsvorgängen hat, kann die nicht ausreichende oder gänzlich ausgebliebene Informationserteilung bußgeldbewährt sein (bei Verstößen gegen Art. 31 DSGVO nach Art. 83 Abs. 4 DSGVO und bei Verstößen gegen Art. 58 Abs.1 lit. a) und e) DSGVO nach Art. 83 Abs. 5 DSGVO).

Andere Verstöße gegen Dokumentationspflichten, wie etwa aus Art. 30 DSGVO (Erstellung von Verarbeitungsverzeichnissen) oder Art. 33 Abs. 5 DSGVO (Dokumentation eines Datenschutzvorfalls), können sogar direkt bußgeldbewährt sein (vgl. Art. 83 Abs. 4 lit. a) DSGVO).

Darüber hinaus kann eine lückenhafte Dokumentation der Datenverarbeitung ein Einfallstor für eine erfolgreiche Schadensersatzklage aufgrund eines materiellen oder immateriellen Schadens durch einen DSGVO-Verstoß sein.

Gem. Art. 82 Abs. 3 DSGVO muss der Verantwortliche oder Auftragsverarbeiter den Nachweis fehlenden Verschuldens führen. Eine fehlende Dokumentation wird dies unmöglich machen. Kann der Verantwortliche, etwa durch hinreichende Dokumentation nachweisen, dass er sämtliche Sicherheitsmaßnahmen definiert und auch eingesetzt hat (Art. 32 DSGVO) und kam es dennoch zu einem unbefugten Datenzugriff, wird es hingegen an einem Verschulden fehlen.

3 Dokumentationspflichten

Die Datenschutz-Grundverordnung (DS-GVO) betont die Verantwortlichkeit, die Unternehmen und öffentliche Stellen (auch „verantwortliche Stellen“ oder „Verantwortliche“ genannt) für die Einhaltung des Datenschutzes haben. Diese müssen nachweisen können, dass ihre Datenverarbeitung datenschutzkonform ist. Die umfangreichen Pflichten zur Dokumentation sollen dies sicherstellen. Die Aufzeichnungen dienen als Nachweis gegenüber der Datenschutzaufsicht, bei gerichtlichen Kontrollverfahren sowie für eine nachträgliche Information Betroffener. Eine erfolgreiche Umsetzung dieser Verpflichtung setzt die Entwicklung, Implementierung und Anwendung eines Datenschutz-Managementsystems voraus. Dabei müssen Verantwortliche eruieren, welche Dokumentationspflichten sie zu beachten haben, Umfang und Grenzen dieser Pflichten kennen und Prozesse einführen, die deren Einhaltung sicherstellen.

3.1 Rechenschaftspflicht nach Art. 5 Abs. 2, 24 Abs. 1 DS-GVO

Wer personenbezogene Daten verarbeitet, ist verantwortlich für die Einhaltung aller in der DS-GVO aufgeführten Rechtsgrundsätze. Hierbei handelt es sich um Folgende: Rechtmäßigkeit der Verarbeitung, Verarbeitung nach Treu und Glauben, Transparenz, Zweckmäßigkeit, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit. Ein Verantwortlicher muss deren Einhaltung nachweisen können (sog. „Rechenschaftspflicht“). Ferner haben verantwortliche Stellen geeignete technische und organisatorische Maßnahmen zu ergreifen, um sicherzustellen und den Nachweis erbringen zu können, dass sie bei ihrer Datenverarbeitung vollumfänglich die DS-GVO beachten. Zudem haben sie ergriffene Maßnahmen zu überprüfen und zu aktualisieren.

3.2 Betroffenenrechte

Verantwortliche Stellen müssen die Rechte Betroffener kennen und Prozesse implementieren, um hierauf entsprechend reagieren zu können. So müssen z. B. Geschäftsprozesse geprüft und die Sachverhalte erfasst werden, an die Informationspflichten (z. B. bei einer Einwilligung oder bei einer Datenerhebung über Dritte) geknüpft sind. Ferner sollten Umfang und Grenzen von Betroffenenrechten und die Fristen bekannt sein, in denen verantwortliche Stellen Betroffenenrechte erfüllen müssen und deren Einhaltung sichergestellt sein.

3.3 Erfüllung der Auskunftsersuchen nach Art. 15 DS-GVO

Jede Person, deren Daten verarbeitet werden, hat das Recht, unentgeltlich binnen eines Monats (Fristverlängerung um max. zwei Monate möglich) von der verantwortlichen Stelle Auskunft darüber zu erhalten, welche Daten über sie verarbeitet werden. Generell empfiehlt es sich, Umfang und Grenzen von Auskunftsansprüchen zu kennen und intern entsprechende Festlegungen (z. B. wer darf Auskunftsansprüche bearbeiten, Mitarbeiter schulen und festlegen, was als Geschäftsgeheimnis anzusehen ist) zu treffen.

3.4 Recht auf Löschung nach Art. 17 DS-GVO

Sind Angaben über eine Person für eine Verarbeitung nicht mehr notwendig, so hat der Verantwortliche diese unverzüglich zu löschen. Dies gilt auch, wenn ein Betroffener aus diesem Grund die Löschung seiner Daten fordert. Betroffene können verlangen, dass Verantwortliche ihnen bestätigen, dass diese die Daten antragsgemäß gelöscht haben. Ferner sollten sie ein Löschkonzept (Dokumentation) haben und darin festlegen, wie lange bestimmte Daten aufgrund gesetzlicher bzw. unternehmensinterner Vorgabe aufbewahrt werden müssen.

3.5 Technisch-organisatorische Maßnahmen (TOM's) nach Art. 24 DS-GVO

Verantwortliche sind verpflichtet, geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten einzusetzen, um sicherzustellen und nachweisen zu können, dass sie die Vorgaben der DS-GVO einhalten. Bei der Festlegung von Maßnahmen sind Art, Umfang, Umstände, die Verarbeitungszwecke ebenso wie unterschiedliche Eintrittswahrscheinlichkeiten und die Schwere der Risiken zu berücksichtigen. Der Nachweis erfolgt über eine entsprechende Beschreibung/Dokumentation dieser Maßnahmen.

3.6 Sicherheit der Verarbeitung

Verantwortliche und Auftragsverarbeiter sind verpflichtet zu eruieren, welche Risiken eine Verarbeitung personenbezogener Daten für Betroffene hat (Risikoanalyse). Hierauf gestützt haben sie über geeignete technische und organisatorische Maßnahmen ein angemessenes technisches Schutzniveau für personenbezogene Daten zu gewährleisten. Eine Dokumentation sollte umfassen, dass zum einen bei der Festlegung der Schutzmaßnahmen der Stand der Technik, Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung sowie zum anderen die unterschiedlichen Eintrittswahrscheinlichkeiten und die Schwere des Risikos für von der Datenverarbeitung Betroffene berücksichtigt worden sind.

3.7 Datenpannen und Meldepflichten

Verantwortliche sollten Vorkehrungen (Notfall-Management) treffen, um auf Datenpannen sachgemäß reagieren zu können. Sie müssen insoweit bestehende Melde- und Informationspflichten kennen. Ferner sollten sie einen Prozess etablieren und so sicherstellen, dass Mitarbeiter Datenpannen erkennen und über entsprechende Vorfälle den Datenschutzbeauftragten oder die Geschäftsleitung (falls kein Datenschutzbeauftragter bestellt ist) informieren, so dass geprüft werden kann, ob eine Meldepflicht besteht und weitere Schritte veranlasst werden können. Festgelegt werden muss auch, wer in einer verantwortlichen Stelle zu dem Team gehört, das intern Datenpannen prüft und bearbeitet.

4 Fazit Dokumentationspflichten

Diese Dokumentation soll in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form in klarer und einfacher Sprache erfolgen. Die Erstellung, Verwaltung sowie Wahl der Struktur dieser Dokumentation obliegt dem Verantwortlichen.

Nach der Intention der DSGVO dient diese Dokumentation folgenden Zwecken:

- Schaffung von Transparenz und Effizienz intern und extern
- Sensibilisierung und Schulung von Mitarbeitern
- Nachvollziehbares Prozessmanagement
- Sicherstellung der Datenschutzkonformität nach der DSGVO
- Bestandteil von möglichen Audits
- Grundlage für eine etwaige Zertifizierung
- Kommunikationsmittel und Nachweis gegenüber der Aufsichtsbehörde
- Vertragsmanagement
- Kommunikationsmittel gegenüber Dritten (Auftragsverarbeitung, Vergabe, usw.)

5 Umfang der Überprüfung durch Aufsichtsbehörden

Diese Dokumentations- und Nachweispflichten nach der DSGVO sollen den Aufsichtsbehörden eine Prüfung der Unternehmen „am Schreibtisch der Behörde“ ermöglichen. Im Rahmen der Nachweispflicht gegenüber den Landes-Datenschutzaufsichts-Behörden muss man daher im Falle einer Prüfung beispielsweise mit folgenden Fragen rechnen:

- Gibt es ein dokumentiertes Konzept im Unternehmen, wer bezogen auf den Datenschutz für was zuständig ist (z.B. Schulung der Mitarbeiter, Meldung von Datenschutzverletzungen, ...)?
- Mit welcher Software führen Sie die automatisierten Backups durch?
- Wurden Awareness - Schulungen durchgeführt, die Internetbedrohungen (z.B. Schadcode, Phishing, ...) zum Inhalt hatten?
- Gibt es bei Ihnen Verarbeitungen, die Sie auf die Rechtsgrundlage „Interessenabwägung“ nach Art. 6 Abs. 1 f DSGVO stützen? Wenn ja, sind dafür dokumentierte Begründungen vorhanden?
- Existiert ein Löschkonzept (z.B. nach DIN 66398), das auch den Umgang mit Archiven und Backups regelt? Wenn ja, bitte senden Sie uns eine Kopie dieses Konzepts zu.
- Werden geeignete Security-Maßnahmen zur Sicherstellung der Verfügbarkeit, Vertraulichkeit und Integrität nach Art. 32 DSGVO getroffen? Wenn ja, senden Sie uns bitte das IT-Sicherheitskonzept bzw. eine Zusammenfassung davon zu.
- Ist ein dokumentierter Prozess vorhanden, wie mit Auskunftsansprüchen nach Art. 15 DSGVO umgegangen wird? Wenn ja, bitte beschreiben Sie diesen Prozess kurz.
- Ist ein Verfahren vorhanden, mit dem die Antwortzeiten auf Fristeinhaltung bezüglich der Betroffenenrechte gemäß Art. 14 bis 22 DSGVO sichergestellt werden? Wenn ja, bitte beschreiben Sie dieses Verfahren kurz.

- Sind Schulungsunterlagen vorhanden, mit denen die Personen, die an den Prozessen zur Sicherstellung der Betroffenenrechte mitarbeiten, sachgerecht informiert werden? Wenn ja, bitte senden Sie uns eine Kopie dieser Unterlagen zu.
- Gibt es einen (dokumentierten) Prozess, um Datenschutzverletzungen innerhalb 72 Stunden (auch an Wochenenden/Feiertagen) bei der zuständigen Aufsichtsbehörde zu melden?

6 Anlage Überblick Dokumentationspflichten

Den Verantwortlichen treffen nach der DSGVO folgende umfangreiche Dokumentationspflichten:

Regelung der DSGVO	**Dokumentation explizit gefordert**	**Dokumentation implizit gefordert**
Rechenschaftspflicht nach Artikel 5 (2) DSGVO	Der Verantwortliche muss die Einhaltung der Prinzipien der Verarbeitung gemäß Artikel 5 (1) DSGVO nachweisen können.	Festlegen bzw. Erstellen einer Datenschutzleitlinie, der Datenschutzziele, der Verantwortlichkeiten, von Richtlinien, von Arbeitsanweisungen, von Aufzeichnungen.
Rechtmäßigkeit der Verarbeitung nach Artikel 6 DSGVO		Der Verantwortliche muss die Rechtsgrundlage der Verarbeitung benennen können.
Einwilligungen nach Artikel 7 und 8 DSGVO	Der Verantwortliche muss die Einwilligung gemäß Artikel 7 (1) DSGVO nachweisen können.	Bei Einwilligung von Kindern muss der Verantwortliche angemessene Anstrengungen zur Identifikation der Erziehungsberechtigten unternehmen.
Verarbeitung von Daten besonderer Kategorien nach Artikel 9 DSGVO	Der Verantwortliche muss eine Einwilligung nach Artikeln 9 (2) a), 7 (1) DSGVO nachweisen können.	Der Verantwortliche muss nachweisen können, auf welche sonstige Rechtsgrundlage nach Artikel 9 (2) DSGVO er seine Verarbeitung stützt.
Verarbeitung von Daten über Verurteilungen und Straftaten nach Artikel 10 DSGVO		Der Verantwortliche muss gemäß Artikel 10 DSGVO eine behördliche Aufsicht nachweisen können.

Einholung zusätzlicher Informationen zur Identifizierung einer Person nach Artikel 11 DSGVO	Der Verantwortliche muss gemäß Artikel 11 (2) DSGVO nachweisen können, dass er nicht zur Identifikation der Person in der Lage war.	
Vorgaben zur Information, Kommunikation und Modalitäten für die Ausübung der Rechte des Betroffenen nach Artikel 12 DSGVO	Der Verantwortliche muss gemäß Artikel 12 (5) S.3 DSGVO den Nachweis offensichtlich unbegründeter oder exzessiver Anträge erbringen.	Der Verantwortliche muss nachweisen können, dass er zur Erfüllung der Anforderungen des Artikel 12 DSGVO in Verbindung mit den Regelungen in den Artikeln 13, 14, 15 bis 22 und 34 DSGVO geeignete Maßnahmen getroffen hat und die Anforderungen des Artikel 12 DSGVO einhält (Identifikation des Betroffenen, Fristeinhaltung, Unterrichtung des Betroffenen, usw.).
Informationspflichten bei Erhebung von Daten bei dem Betroffenen nach Artikel 13 DSGVO		Der Verantwortliche muss die Informationserteilung nachweisen können.
Informationspflichten bei Erhebung von Daten nicht bei dem Betroffenen nach Artikel 14 DSGVO		Der Verantwortliche muss die Informationserteilung nachweisen können.
Antrag auf Auskunft nach Artikel 15 DSGVO		Der Verantwortliche muss die von ihm festgelegten Prozesse und durchgeführten Maßnahmen nachvollziehbar nachweisen können.
Antrag auf Berichtigung, Löschung oder Sperrung nach Artikeln 16, 17, 18, 19 DSGVO		Der Verantwortliche muss die von ihm festgelegten Prozesse und durchgeführten Maßnahmen nachvollziehbar nachweisen können.
Antrag auf Datenübertragung, Widerspruch gegen Verarbeitung oder Antrag		Der Verantwortliche muss die von ihm festgelegten Prozesse und durchgeführten Maßnahmen (Informationen)

auf Information und Einwirkung auf automatisierte Entscheidungen nach Artikeln 20, 21, 22 DSGVO		nachvollziehbar nachweisen können.
Anordnung technischer und organisatorischer Maßnahmen nach Artikeln 24, 25 DSGVO		Der Verantwortliche muss die von ihm festgelegten und durchgeführten Maßnahmen nachvollziehbar nachweisen können.
Gemeinsame Datenverarbeitung durch Verantwortliche nach Artikel 26 DSGVO	Die Verantwortlichen müssen nach Artikel 26 (1) DSGVO eine Vereinbarung in transparenter Form treffen.	
Benennung eines Vertreters von nicht in der EU niedergelassenen Verantwortlichen nach Artikel 27 DSGVO	Die Benennung hat nach Artikel 27 (1) DSGVO schriftlich zu erfolgen.	
Auftragsverarbeitung nach Artikel 28 DSGVO	Der Auftragsverarbeiter darf die Daten gemäß Artikel 28 (3) a) DSGVO nur auf dokumentierte Weisung des Verantwortlichen verarbeiten. Der Vertrag ist nach Artikel 28 (9) DSGVO schriftlich oder in einem elektronischen Format abzuschließen.	Der Verantwortliche muss die von ihm gemäß Artikel 32 DSGVO getroffenen Maßnahmen nachvollziehbar nachweisen können.
Verarbeitung unter Aufsicht des Verantwortlichen nach Artikel 29 DSGVO		Der Verantwortliche muss die von ihm erteilten Weisungen nachweisen können.
Verzeichnis von Verarbeitungen nach Artikel 30 DSGVO	Der Verantwortliche ist nach Artikel 30 (1) DSGVO zur Führung dieses Verzeichnisses verpflichtet.	
Sicherheit der Verarbeitung nach Artikel 32 DSGVO		Der Verantwortliche muss die von ihm gemäß Artikel 32 DSGVO getroffenen Maßnahmen nachvollziehbar nachweisen können.

Meldung von Datenschutzverletzungen nach Artikel 33 DSGVO	Der Verantwortliche dokumentiert die Verletzung nach Artikel 33 (5) DSGVO und meldet den Verstoß an die Aufsichtsbehörde.	Der Verantwortliche muss die von ihm festgelegten Prozesse nachweisen können.
Benachrichtigung eines Betroffenen nach Artikel 34 DSGVO		Der Verantwortliche muss die von ihm festgelegten Prozesse und durchgeführten Maßnahmen nachvollziehbar nachweisen können.
Datenschutzfolgenabschätzung nach Artikel 35 DSGVO	Eine Datenschutzfolgenabschätzung enthält nach Artikel 35 (7) DSGVO eine Beschreibung und Bewertung bestimmter Mindestinhalte	Der Verantwortliche muss die von ihm festgelegten Prozesse und durchgeführten Beurteilungen nachvollziehbar nachweisen können, insbesondere die Durchführung einer Analyse, ob eine DSFA durchzuführen ist oder nicht.
Konsultationen nach Artikel 36 DSGVO	Eine Konsultation erfordert die Zusammenstellung der nach Artikel 36 DSGVO bestimmten Informationen.	Der Verantwortliche muss die von ihm festgelegten Prozesse und durchgeführten Beurteilungen nachvollziehbar nachweisen können.
Benennung eines Datenschutzbeauftragten nach Artikeln 37, 38, 39 DSGVO	Der Verantwortliche veröffentlicht die Kontaktdaten des DSB und teilt diese der Aufsichtsbehörde gemäß Artikel 37 (7) DSGVO mit.	Die Benennung und die Tätigkeit des DSB ist zu dokumentieren.
Datenübermittlung in Drittländer nach Artikeln 44 bis 50 DSGVO		Der Verantwortliche muss nachweisen können, dass er zur Erfüllung der Anforderungen an eine Datenübermittlung in ein Drittland geeignete Maßnahmen getroffen hat und die Anforderungen der Artikel 44 ff DSGVO einhält (angemessenes Schutzniveau, Garantien, Einwilligung des Betroffenen, usw.).