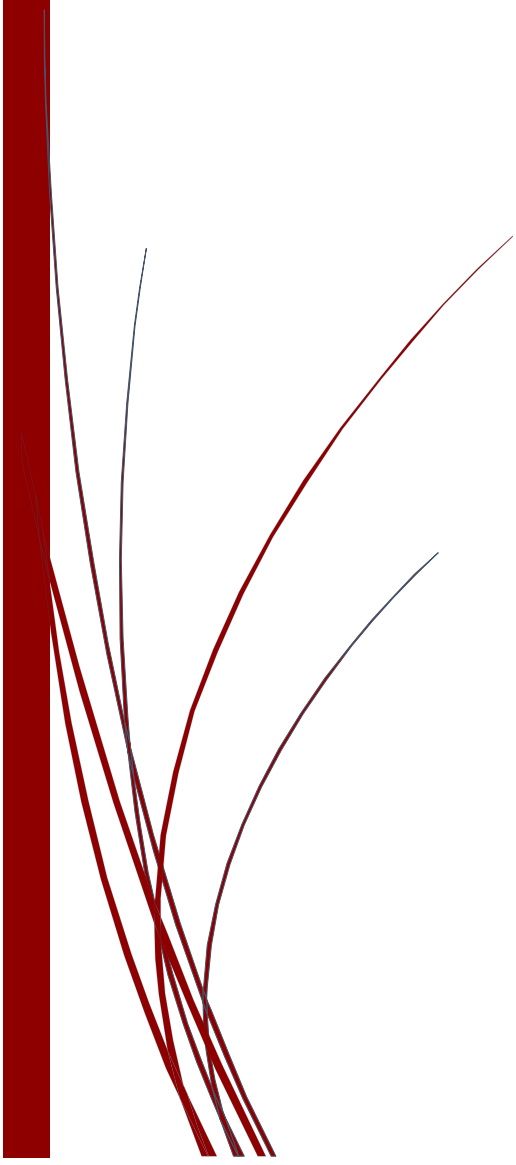
30.6.2019

Dokumentations-pflichten

Der Umfang der Nachweis- und Dokumentationspflichten nach der DSGVO



Wolf-Dieter Czap
RECHTSANWALT & EXTERNER DSB

Zum Umfang der Dokumentations- und Nachweispflichten des Verantwortlichen für die Datenverarbeitung.

INHALTSVERZEICHNIS

Dokumentationspflichten nach der DSGVO

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.

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 auf Information und Einwirkung auf automatisierte Entscheidungen nach Artikeln 20, 21, 22 DSGVO		Der Verantwortliche muss die von ihm festgelegten Prozesse und durchgeführten Maßnahmen (Informationen) 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.).

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.)

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 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?

(Quelle LDA Bayern, Muster-Fragebögen bei Prüfungen)