



DSGVO: Die Rechenschaftspflicht im Datenschutz

DSGVO: Die Rechenschaftspflicht im Datenschutz

Dokumentation gehört nicht nur im Datenschutz zu den eher unbeliebten Aufgaben. Doch wer seine Datenschutz-Maßnahmen nicht nachweisen kann, erfüllt auch nicht die Rechenschaftspflicht nach der Datenschutz-Grundverordnung (DSGVO). Was gehört alles zur Nachweis- bzw. Rechenschaftspflicht?

Was sagt die DSGVO zur Rechenschaftspflicht?

Unternehmen und öffentliche Einrichtungen wie Behörden sind dafür verantwortlich, die Vorgaben aus der DSGVO einzuhalten. Und das müssen sie auch nachweisen, so sagt Artikel 5 DSGVO zur Rechenschaftspflicht (Accountability).

Auch Artikel 24 DSGVO enthält eine entsprechende Nachweispflicht: anach muss der Verantwortliche den Nachweis dafür erbringen, dass die Verarbeitung personenbezogener Daten gemäß der Datenschutz-Grundverordnung erfolgt.

Was gehört alles zur Rechenschaftspflicht?

Um der Rechenschafts- oder Nachweispflicht nachzukommen, empfehlen die Datenschutz-Aufsichtsbehörden, wesentliche Aktivitäten und Arbeitsergebnisse, die dazu dienen, die DSGVO umzusetzen, festzuhalten.

Zur Rechenschaftspflicht gehört also, die umgesetzten technischen und organisatorischen Datenschutz-Maßnahmen zu dokumentieren. So muss der Verantwortliche zum Beispiel nachweisen, dass ihm eine informierte Einwilligung vorliegt, sofern er sie als Rechtsgrundlage heranzieht.

Ein weiteres Beispiel: Unternehmen, also nicht-öffentliche Einrichtungen, müssen ebenso wie öffentliche Institutionen ihre Beschäftigten im Datenschutz schulen. Zudem müssen sie sie darauf verpflichten, die datenschutzrechtlichen Anforderungen der DSGVO einzuhalten. Um hier ihrer Rechenschaftspflicht nachzukommen, müssen Verantwortliche beides ausreichend dokumentieren.

Welche weiteren Dokumentationen sind wichtig?

Die DSGVO sieht an mehreren Stellen Dokumentationspflichten vor, die die Rechenschaftspflicht umsetzen. Dazu gehören

- das Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 DSGVO,
- die Dokumentation von Datenschutzverletzungen nach Artikel 33 DSGVO und
- die Dokumentation von Weisungen, die ein Verantwortlicher im Rahmen einer Auftragsverarbeitung nach Artikel 28 DSGVO vornimmt.

So ist beispielsweise zu dokumentieren, wenn bei einer Datenschutzverletzung das Risiko für die Betroffenen als gering oder nicht vorhanden eingestuft wird. Dabei reicht allerdings die bloße Feststellung nicht, es gehört schon eine Begründung dazu.

Gemäß Artikel 58 DSGVO kann die Aufsichtsbehörde Verantwortliche und Auftragsverarbeiter dazu verpflichten, ihr auf Anfrage alle Informationen bereitzustellen, die erforderlich sind, um ihre Aufgaben zu erfüllen. Verantwortliche und Auftragsverarbeiter müssen in der Lage sein, diese Verpflichtungen zu erfüllen. Das gelingt nur mit den entsprechenden Dokumentationen.

Verhaltensregeln und Zertifizierungen sind Beispiele für freiwillige Instrumente, mit denen sich die Rechenschaftspflicht nach DSGVO erfüllen lässt.

Ein Beispiel der Aufsichtsbehörden für die Rechenschaftspflicht

Die nordrhein-westfälische Datenschutz-Aufsichtsbehörde nennt die [Übermittlung von Kundenkontaktdaten](#) zwecks Rückverfolgbarkeit von Infektionsketten im Zusammenhang mit der Rechenschaftspflicht.

Liste oder Auszüge aus Listen mit den Kundenkontaktdaten sollten Verantwortliche ausschließlich bei schriftlicher Aufforderung etwa durch das Gesundheitsamt oder

durch eine andere öffentliche Stelle übermitteln. Ein Verantwortlicher muss jede Aufforderung, eine Liste zu übermitteln, und die Übermittlung selbst dokumentieren, um der Rechenschaftspflicht gegenüber der Datenschutzaufsicht nachzukommen: Welche Liste hat er an wen wann wie übermittelt?

Was hat die Datenschutz-Folgenabschätzung mit der Rechenschaftspflicht zu tun?

Auch wer eine Datenschutz-Folgenabschätzung (DSFA) durchführt, muss dies dokumentieren. So fordert es Artikel 35 DSGVO. Die Aufsichtsbehörden für den Datenschutz empfehlen, dass Verantwortliche ihre Entscheidung, eine Verarbeitung trotz bestimmter Risiken durchzuführen, genau begründen und dokumentieren.

Das gilt auch, wenn sich der Verantwortliche im Rahmen der DSFA den Rat des oder der Datenschutzbeauftragten einholt. Falls der oder die Verantwortliche sich dazu entscheiden sollte, vom Rat der oder des Datenschutzbeauftragten abzuweichen, sollte sie oder er die Gründe für die Abweichung schriftlich dokumentieren.

Welche Rolle spielt das Verzeichnis von Verarbeitungstätigkeiten?

Das Verzeichnis von Verarbeitungstätigkeiten ist die wesentliche Grundlage für eine strukturierte Datenschutzdokumentation. Sie hilft dem Verantwortlichen dabei, gemäß Artikel 5 DSGVO nachzuweisen, dass er die Vorgaben aus der DSGVO einhält.

Das Verzeichnis ist also kein Dokumentationsballast, sondern ein zentrales Datenschutz-Instrument und Mittel, um die Rechenschaftspflicht umzusetzen.

Wie hängen Transparenz und Rechenschaftspflicht zusammen?

Transparenz ist untrennbar mit dem Grundsatz der Rechenschaftspflicht verbunden: Der Verantwortliche muss stets den Nachweis erbringen können, dass er die personenbe-

zogenen Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet.

Der Grundsatz der Rechenschaftspflicht erfordert in diesem Zusammenhang transparente Verarbeitungsvorgänge.

Quelle:

www.datenschutz-praxis.de