Information zur Risikobeurteilung
Datenschutz-Folgenabschätzung
gemäß Art. 35 DSGVO

Beachten Sie bitte im Zusammenhang mit der Erforderlichkeit einer Datenschutz-Folgenabschätzung auch das Formular „Hinweis zur Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO“.

Werden hohe Risiken bei der Verarbeitung von personenbezogenen Daten verwirklicht, muss der Verantwortliche eine Datenschutz-Folgenabschätzung durchführen, um die Risiken festzustellen, zu dokumentieren und zu reduzieren.

Ist eine Beherrschung des hohen Risikos durch technische oder organisatorische Maßnahmen in einem angemessenen Umfang nicht zu erreichen, muss sogar eine Genehmigung der das Risiko auslösenden Datenverarbeitung durch die zuständige Datenschutzbehörde eingeholt werden. Im weiteren Verlauf ist dann eine kontinuierliche Überprüfung des Risikos erforderlich.

Positiv ist, dass eine bereits nach dem alten Bundesdatenschutzgesetz durchgeführte „Vorabkontrolle“, die als Vorläufer der Folgenabschätzung bezeichnet werden kann, ihre Gültigkeit auch nach dem Wirksamwerden der DSGVO am 25. Mai 2018 behält und keine erneute Datenschutz-Folgeabschätzung für den betroffenen Prozess durchgeführt werden muss.

Um über die Erforderlichkeit einer Datenschutz-Folgenabschätzung zu entscheiden, muss der Verantwortliche zunächst eine Risikobewertung vornehmen. Ergibt die Bewertung, dass durch Risiken der Datenverarbeitung lediglich geringfügige Auswirkungen auf die Rechte und Freiheiten einer Person entstehen können, handelt es sich um einen normalen Schutzbedarf, der keine Datenschutz-Folgenabschätzung erfordert.

Würde aus einem Datenmissbrauch ein erheblicher wirtschaftlicher oder sozialer Nachteil entstehen, unter Umständen sogar durch Beeinträchtigung der persönlichen Unversehrtheit der von der Datenverarbeitung betroffenen Person (z. B. Daten der Privatsphäre, große Nachteile bei Veröffentlichung), wird ein hoher Schutzbedarf angenommen. Ein sehr hoher Schutzbedarf ist dagegen anzunehmen, wenn der mögliche Datenmissbrauch für die betroffene Person den wirtschaftlichen oder sozialen Ruin bedeutet oder eine massive Beeinträchtigung der persönlichen Unversehrtheit verursacht. Bei einem sehr hohen Schutzbedarf ist eine Datenschutz-Folgenabschätzung in der Regel erforderlich.

Die Datenschutz-Folgeabschätzung erfolgt in folgenden Schritten:

<u>Risikobewertung</u>

Bewertung des Datenschutzrisikos der von der Datenverarbeitung betroffenen Person (durch Berücksichtigung objektiver Kriterien wie z. B. Art, Umfang, Umstände und Zwecke der Verarbeitung).

Für das Verfahren zur Risikobestimmung gibt es keine einheitliche und vom Gesetz vorgeschriebene Methode. Eine Risikobestimmung sollte daher nach einem gängigen Verfahren (z. B. Standard-Datenschutzmodell) oder der Vorgabe der zuständigen Datenschutzaufsicht erfolgen.

Beeinträchtigung

Es muss geprüft werden, ob die geplante Datenverarbeitung die von der Datenverarbeitung betroffene Person bei einem Datenmissbrauch schädigen kann (z. B. Diskriminierung, Identitätsdiebstahl, Rufschädigung, finanzieller Verlust, Hinderung der Kontrolle über eigene Daten, Profilbildung mit Standortdaten)

Minimierung des Risikos

Der Verantwortliche ist bei der Verarbeitung von personenbezogenen Daten dazu verpflichtet, im Verhältnis zum Risiko Maßnahmen zu treffen, die nach dem Stand der Technik den Schutz der Daten sicherstellen können. Diese Maßnahmen müssen angemessen sein, also nicht die neuesten und teuersten sein. Regelmäßig handelt es sich um organisatorische Maßnahmen (z. B. interne Regelungen zum Datenschutz, Notfallkonzept, Datenschutzschulung) und technischen Maßnahmen (z. B. Einsatz von Firewall, Virenscanner, Verschlüsselung von Daten).

Dokumentation der Maßnahmen

Der Verantwortliche muss eine Dokumentation der datenschutzrechtlichen Maßnahmen vornehmen, damit er gegenüber der Aufsichtsbehörde die Umsetzung der Vorgaben der DSG-VO und des Bundesdatenschutzgesetzes ausreichend nachweisen kann. Die Dokumentation umfasst die Durchführung einer Risikobewertung, Analyse-Ergebnis und eine deshalb gegebenenfalls erfolgende Datenschutz-Folgenabschätzung.

Inhalt einer Datenschutz-Folgenabschätzung

Hierzu gehören die systematische Beschreibung der Verarbeitungsvorgänge und Zwecke, die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung im Verhältnis zum Zweck der Verarbeitung, die Risikobewertung und die geplanten Abhilfemaßnahmen zur Bewältigung der Risiken.

Einbeziehung der Aufsichtsbehörde

Hat der Verantwortliche eine Datenschutz-Folgenabschätzung durchzuführen, muss er vor der Durchführung der betreffenden Datenverarbeitung die zuständige Aufsichtsbehörde einbeziehen und mit dieser ggf. erforderliche weitere Schutzmaßnahmen klären.

Der der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern hat zu der Notwendigkeit einer Datenschutz-Folgenabschätzung in Arztpraxen in einem im Ärzteblatt veröffentlichten Beitrag wie folgt Stellung genommen:

„Eine Datenschutz-Folgenabschätzung kann bei einer umfangreichen Verarbeitung von Gesundheitsdaten erforderlich sein. Verarbeiten in einer Praxis weniger als 10 Personen personenbezogene Daten (Mitarbeiter und Ärzte), wird in der Regel nicht von einer umfangreichen Verarbeitung von Gesundheitsdaten auszugehen sein. Allerdings können auch andere Risikofaktoren, wie beispielsweise die Speicherung von Patientendaten in einer Cloud, die Einbindung von Gesundheitsapps, die Übermittlung von Gesundheitsdaten in Drittstaaten im Rahmen von Forschungsvorhaben oder die Teilnahme an Gesundheitsnetzwerken eine Datenschutz-Folgenabschätzung erforderlich machen. Im Rahmen der gemeinsamen Verantwortlichkeit, beispielsweise bei Netzwerken, besteht allerdings auch die Möglichkeit, dass nur ein Verantwortlicher eine Datenschutz-Folgenabschätzung für alle vornimmt. Eine Datenschutz-Folgenabschätzung kann für bestimmte Produkte auch bereits vorliegen. Mit zuverlässigen Partnern ist mehr Digitalisierung in der Arztpraxis also nicht zwingend mit Mehraufwand durch eine Datenschutz-Folgenabschätzung verbunden.“