Leitfaden zur Erstellung einer datenschutzrechtlichen Risikobewertung

Im Verzeichnis über Verarbeitungstätigkeit (kurz VVT) ist unter *Punkt II – 12.* Eine Risikobewertung unter Betrachtung der vorhandenen technischen und organisatorischen Maßnahmen durchzuführen.
Diese Bewertung besteht zu einem Teil aus den Aspekten der Informationssicherheit und zum anderen Teil aus den Aspekten des Datenschutzes.
Die Risiken werden im Datenschutz aus der Sicht der von der Datenverarbeitung betroffenen Person betrachtet.

Bei einer Risikobewertung geht es darum, potentielle Risiken für die Verursachung von Schäden bei der betroffenen Person zu identifizieren, eine mögliche Schadenshöhe zu bestimmen und unter Berücksichtigung aller ergriffenen technischen und organisatorischen Maßnahmen (kurz TOMs) das Risiko insgesamt einzustufen.

Zur Bewertung des Risikos werden im ersten Schritt die Eintrittswahrscheinlichkeit eines Schadens bzw. Risikoszenarios sowie die Schwere der Folgen/des möglichen Schadens aus Sicht der betroffenen Person definiert.

Eintrittswahrscheinlichkeit eines Schadens/Risikoszenarios

Eintrittswahrscheinlichkeit	Beschreibung	Beispiel
gering	Vorfall tritt frühestens in 6 Jahren oder später ein	Befall durch Schadsoftware bei einem Stand-Alone-Rechner, der an keinem Netzwerk angeschlossen ist und an den keine weiteren Medien angeschlossen werden können
mittel	Vorfall tritt in den nächsten 4 - 6 Jahren ein	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit einer Anti-

		Viren-Software ausgestattet und nur mit einem sicheren Firmennetzwerk verbunden ist
hoch	Vorfall tritt in den nächsten 1 – 3 Jahren ein	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit einer Anti-Viren-Software ausgestattet und direkt mit dem Internet verbunden ist
sehr hoch	Vorfall tritt im nächsten Jahr ein	Befall durch Schadsoftware bei einem Rechner, der nicht aktuell gehalten (z.B. älteres Betriebssystem als Windows 10), mit einer Anti-Viren-Software ausgestattet und direkt mit dem Internet verbunden ist

Beurteilung der Schwere möglicher Folgen/Schäden

Schadensklasse	Beschreibung für Betroffenen & Verantwortlichen	Beispiel für Betroffene & Verantwortliche
gering	Betroffene erleiden eventuell Unannehmlichkeiten, die sie überwinden können	Leichte Verägerung, Zeitverlust, vorübergehende Kopfschmerzen

	Vorfall ist nur internen Mitarbeitern bekannt	Finanzieller Schaden unter 5000€, keine bis kaum mediale Auswirkungen
mittel	Betroffene erleiden signifikante Unannehmlichkeiten, die sie mit einigen Schwierigkeiten überwinden können	Geringe aber objektiv nachweisbare psychische Beschwerden, deutlich spürbarer Verlust an privatem Komfort, minderschwere körperliche Schäden (z.B. nicht existenzgefährdender finanzieller Schaden)
	Vorfall ist auch außerhalb der Institution bekannt	Finanzieller Schaden zwischen 5000€ und 20.000€, regionale mediale Auswirkungen
Hoch	Betroffene erleiden signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können	Schwere psychische Beschwerden, finanzielle Schwierigkeiten, schwere körperliche Beschwerden (z.B. Identitätsdiebstahl, Diskriminierung)
	Vorfall ist landesweit bekannt, negatives Image	Finanzieller Schaden zwischen 20.000€ und 50.000€, nationale mediale Auswirkungen
Sehr hoch	Betroffene erleiden signifikante und unumkehrbare Konsequenzen	Dauerhafte schwere psychische Beschwerden, erhebliche Schulden, dauerhafte körperliche Beschwerden

	Vorfall ist international bekannt	Finanzieller Schaden über 50.000€, internationale mediale Auswirkungen, Verlust von Kunden

Im zweiten Schritt wird unter Berücksichtigung aller getroffenen technischen und organisatorischen Maßnahmen (z.B. Zugriffsbeschränkung, Verschlüsselung, Pseudonymisierung, ...) ein verbleibendes Restrisiko als Gesamtbewertung definiert und im Anschluss im VVT notiert.