Datenschutz-Folgenabschätzung

Was ist zu beachten?

Kurz bevor die Datenschutzgrundverordnung (DSGVO) im Mai 2018 in Kraft trat, war die Verunsicherung bei vielen groß. Inzwischen ist es wieder ruhiger um das Thema geworden. Dennoch dürfen Unternehmen den Datenschutz nicht aus den Augen verlieren. Eine Risikobewertung in Form der Datenschutz-Folgenabschätzung gehört dabei zum Pflichtprogramm.

Was gehört in die Datenschutz-Folgenabschätzung

Wer die im Unternehmen verarbeiteten Daten schützen will, muss erst einmal die eingesetzten Verarbeitungsprozesse und ihre Risiken kennen. Im ersten Schritt gilt es daher, die Prozesse genau zu beschreiben. Dargestellt werden muss dabei auch der Zweck dieser Datenverarbeitung und das dahinterstehende berechtigte Interesse des Unternehmens. Bei einer Videoüberwachung könnten dies zum Beispiel Sicherheitsaspekte sein, bei besonderen personenbezogenen Daten wären gesetzliche Vorschriften der Aufzeichnung als Grund denkbar.

Sind die Verarbeitungsprozesse genau bekannt, muss das Unternehmen ermitteln, ob sie in dieser Form tatsächlich notwendig und verhältnismäßig sind. Maßgeblich dafür ist immer der Zweck, den es mit der Erhebung der Daten verfolgt. Während zum Beispiel bei einem Online-Handel mit alkoholischen Getränken die Erfassung und Verarbeitung des Geburtsdatums eines Bestellers zur Kontrolle des gesetzlich festgelegten Mindestalters zulässig wäre, ist dies bei der Bestellerin von Dekoartikeln nicht der Fall.

Ebenfalls ermitteln muss das Unternehmen die Risiken, die durch die geplanten Verarbeitungsprozesse für die Betroffenen entstehen. Zu beurteilen ist dabei konkret, wie wahrscheinlich ein solches Risiko eintritt und wie schwer es in die Persönlichkeitsrechte eingreift. Eingeteilt sind die Risiken in die Klassen „normaler Schutzbedarf", „hoher Schutzbedarf" und „sehr hoher

Schutzbedarf", wobei die höchste Risikoklasse die größten Schutzmaßnahmen erfordert. In die höchste Schutzklasse fallen zum Beispiel sensible Kranken- oder Steuerdaten. Daten mit normalem Schutzbedarf sind dagegen die Anschrift einer Person oder öffentliche Telefonverzeichnisse. Abschließend muss das Unternehmen in der Datenschutz-Folgenabschätzung die Maßnahmen fixieren, mit denen es die ermittelten Risiken bewältigen kann. Dazu zählen sämtliche eingesetzten Verfahren – online und offline, die für eine sichere Verarbeitung der persönlichen Daten sorgen.

Technische und organisatorische Maßnahmen

Zusammengefasst werden in den Sicherheitsmaßnahmen die technischen und organisatorischen Maßnahmen (TOM). Beschrieben sind sie in Artikel 32 DSGVO. Dabei beziehen sich die technischen Maßnahmen auf den Vorgang der Datenverarbeitung. Dazu zählen alle Maßnahmen, die sich physisch umsetzen lassen. Beispiele dafür sind die Installation einer Alarmanlage, die Nutzung abschließbarer Schränke oder das Einrichten eines sicheren Passworts am Rechner. Organisatorische Maßnahmen dagegen beziehen sich auf die Rahmenbedingungen des Datenverarbeitungsprozesses. Dazu gehören Vorgaben und Handlungsanweisungen, die die Mitarbeiterinnen und Mitarbeiter des Unternehmens beim Umgang mit Daten befolgen müssen.

Für Unternehmen wirken gut umgesetzte TOM als rechtliche Absicherung und können damit vor hohen Bußgeldforderungen oder Strafen bewahren. Sollten nämlich zum Beispiel Behörden oder Betroffene den korrekten Umgang mit persönlichen Daten anzweifeln, können sie als Nachweis der etablierten Standards dienen. Festgelegt wird in den TOM zum Beispiel, wer im Unternehmen Zugang zu Datenverarbeitungsanlagen hat, Daten ein- oder weitergeben oder Aufträge zur Auftragsdatenverarbeitung erteilen und kontrollieren darf. Auch die Kontrolle über die Verfügbarkeit der Daten und ihre Zweckbindung ist Teil der Regelungen.

Ziel der zu treffenden Maßnahmen ist es, die Vertraulichkeit von Daten und ihre Verfügbarkeit sicherzustellen. Das bedeutet auch, dass die Systeme der Unternehmen belastbar gegenüber möglichen Störungen sein müssen. Hinzu kommt, dass nach einem Zwischenfall technischer oder physischer Art die Daten vollständig wiederherstellbar sein müssen.

Was Unternehmen tun sollten

Wer bisher noch keine Datenschutz-Folgeabschätzung erstellt hat, sollte dies dringend nachholen. Dabei gilt es, bestehende Prozesse genauso einzubeziehen wie neue. Im Zeitablauf sollten Unternehmen außerdem prüfen, ob die einmal erfassten Vorgänge dem aktuellen Stand entsprechen und ihre Datenschutz-Folgeabschätzung bei Bedarf anpassen.

Die TOM sollten ebenfalls daraufhin geprüft werden, ob sie alle Verarbeitungsprozesse erfassen und auf dem neuesten Stand sind. Wichtig ist auch, die einmal festgelegten technischen und organisatorischen Maßnahmen regelmäßig auf ihre Wirksamkeit zu kontrollieren. Denn nur so stellen Unternehmen sicher, dass sie alles Machbare zum Schutz persönlicher Daten umsetzen. Wirtschaftlich kann dies im Schadenfall existenzsichernd wirken.

Martina Schäfer
FINIS Kommunikation

Ihr IHK-Rechtsexperte:

Detlev Langer
Telefon 0228 2284 -134
E-Mail: langer@bonn.ihk.de