UNION
Versicherungsdienst GmbH

MIT EINEM BEIN IM GEFÄNGNIS

Strafe ist nicht auszuschließen: Die Gefahr, gegen die Datenschutz-Grundverordnung zu verstoßen, ist groß.

Seit dem 25. Mai herrscht große Unklarheit in Unternehmen der Wohlfahrtspflege und des Gesundheitswesens, denn seitdem gilt die europäische Datenschutz-Grundverordnung (DS-GVO), und die Frage lautet: Welche Anforderungen müssen wir erfüllen und wie? Unsicherheit besteht zum einen, weil sich die Datenschutzbehörden in der Vergangenheit häufig nicht verbindlich zu Problemfragen geäußert haben. Zum anderen sieht die Verordnung hohe Geldbußen bei Verstößen vor. Der Jurist Dr. Michael Fortmann aus dem Unternehmensbereich Financial Lines geht der Frage nach: Welche Gefahren ergeben sich für Einrichtungen und deren Management aus der DS-GVO und wie kann man sich dagegen wappnen?

Sensible Gesundheitsdaten müssen geschützt werden

In Europa sind die Anforderungen an die Einhaltung des Datenschutzes und an die Sicherheit von Datenbeständen in den vergangenen Jahren immer mehr verschärft worden. Da Einrichtungen der Wohlfahrtspflege und des Gesundheitswesens zum Teil mit hoch sensiblen und damit zwingend schützenswerten Daten arbeiten (zum Beispiel Gesundheitsdaten von Personen), spielen Datenschutz und Datensicherheit gerade hier in der täglichen Arbeit eine immer größere Rolle.

Aufgrund der DS-GVO können verschiedene Haftungsrisiken für Einrichtungsträger, aber auch für deren Management entstehen:

Haftungsrisiken für die Einrichtungsträger

Wird die DS-GVO nicht eingehalten, ergeben sich für die Einrichtungsträger die Risiken im Wesentlichen aus zwei Bereichen: Zum Ersten kann die Datenschutzbehörde ein Bußgeld gegen die Einrichtung verhängen – was allerdings in der Praxis nicht der Regelfall sein dürfte. Zum Zweiten können Dritte, etwa Patientinnen und Patienten oder Bewohnerinnen und Bewohner, Ersatz für einen materiellen oder immateriellen Schaden einfordern.

Vielfältige Schadenszenarien möglich

Gerade immaterielle Schäden bei Datenschutzverletzungen (zum Beispiel Ansehensverluste, weil sensible persönliche Gesundheitsdaten im Internet veröffentlicht worden sind) können Betroffene dank DS-GVO nunmehr einfacher als zuvor geltend machen. Insbesondere bei Verlust einer größeren Datenmenge (zum Beispiel einer Patienten- oder Bewohnerdatenbank) tragen Einrichtungen das Risiko, mitunter hohen Schadenersatzforderungen ausgesetzt zu sein.

Daneben besteht die Gefahr, dass eine Datenschutzverletzung die Einrichtung selbst finanziell schädigt: Es können Kosten für die Einschaltung eines Spezialisten für Öffentlichkeitsarbeit entstehen, etwa weil in der Presse über die Datenschutzpanne umfassend berichtet wird. Oder es fallen Kosten an für die gesetzlich geforderte Benachrichtigung von Betroffenen, deren Daten abhandengekommen sind.

Des Weiteren sind bei einer Datenschutzpanne Vermögensschäden durch Umsatzeinbrüche denkbar.

Zwei große Risiken für Entscheidungsträger

Neben der Einrichtung sind auch deren Entscheidungsträger erheblichen Risiken ausgesetzt. Derzeit ist allerdings noch ungeklärt, ob diese im Sinne der DS-GVO selbst als Verantwortliche angesehen werden können. Noch offen ist also die Frage: Kann gegen die Entscheidungsträger persönlich ein Bußgeld verhängt werden beziehungsweise können Dritte (beispielsweise Patienten und Patientinnen oder Bewohnerinnen und Bewohner) sie persönlich auf Schadenersatz in Anspruch nehmen?

Aber auch unabhängig davon bestehen für das Management von Einrichtungen vor allem zwei Gefahren:

Zum einen könnte die Einrichtung versuchen, sich für sämtliche aus einer Datenschutzverletzung resultierenden Schäden schadlos zu halten (zum Beispiel für gezahlte Bußgelder oder für an Dritte geleistete Schadenersatzzahlungen), und den Entscheidungsträger in Regress nehmen. Hierbei könnte sie diesem beispielsweise vorwerfen, nicht alle notwendigen Vorkehrungen für die Einhaltung der Datenschutzvorschriften getroffen und damit die sogenannte Legalitätspflicht verletzt zu haben, also die

Die neue Datenschutz-Grundverordnung bringt Haftungsrisiken mit sich.

Bei Fragen zu Datenrisiken oder zur EVH Data Risk sprechen Sie uns gerne an.

Pflicht, für die Einhaltung sämtlicher Rechtsvorschriften zu sorgen.

Zum anderen laufen Entscheidungsträger beim Vorwurf schwerer Datenschutzverletzungen Gefahr, dass ein strafrechtliches Ermittlungsverfahren gegen sie eingeleitet wird. Im Bundesdatenschutzgesetz sind Straftatbestände enthalten, die in bestimmten Fällen eine Geldstrafe oder sogar eine Freiheitsstrafe von zwei bzw. drei Jahren nach sich ziehen. Zum Beispiel dann, wenn Angaben zu Krankheiten oder andere personenbezogene Daten, die nicht öffentlich bekannt sind, verkauft und weiterverarbeitet wurden, und zwar ohne entsprechende Berechtigung. Dieses Risiko verwirklicht sich aber nicht nur dann, wenn eine Straftat tatsächlich vorliegt. Allein der Vorwurf, solch eine Straftat begangen zu haben, kann schon ausreichen, um ein Ermittlungsverfahren in Gang zu bringen und damit teilweise sehr hohe Kosten für einen Strafverteidiger aufbringen zu müssen.

Absicherungsmöglichkeiten

Die finanziellen Nachteile, die aus Datenschutzverletzungen entstehen, können Einrichtungen und Management durch Versicherungsprodukte absichern.

Für Einrichtungen besteht die Möglichkeit, eine Cyberversicherung abzuschließen. Da sich die Produktangebote der einzelnen Versicherer aber inhaltlich teilweise erheblich unterscheiden, lohnt sich hier ein genauer Vergleich. Zu beachten ist: In den meisten dieser Produkte können nur elektronische Daten abgesichert werden. Für Datenschutzverletzungen, die zum Beispiel aus dem Verlust von Papierakten resultieren, bestünde also kein Deckungsschutz.

Bester Schutz für Entscheidungsträger

Entscheidungsträger können einen Teil der sie treffenden Datenschutzrisiken über eine D&O-Versicherung (Directors-and-Officers-Versicherung) absichern. Allerdings erbringt der Versicherer die Leistung hier nur dann, wenn ein Entscheidungsträger auf Schadenersatz in Anspruch genommen wird. Zudem zahlt der Versicherer keine Entschädigung bei Beschädigung, Zerstörung oder Abhandenkommen von Daten.

Einen umfassenden Schutz sowohl für Einrichtungsträger als auch für das Management bietet das von unserem Haus entwickelte Versicherungsprodukt EVH* Data Risk, das am deutschen Markt einzigartig ist. Um eine Entschädigungsleistung zu erhalten, ist nicht erforderlich, dass der Schädiger (zum Beispiel der Geschäftsführer) in Anspruch genommen wird. Schäden werden vielmehr direkt und diskret zwischen der betroffenen Einrichtung und dem Versicherer abgewickelt.

Zudem sind sämtliche Datenrisiken umfassend abgesichert, also auch Schäden durch Beschädigung, Zerstörung oder Abhandenkommen von Daten – auch von nicht-elektronischen. Versicherungsschutz besteht für das Unternehmen ebenso wie für alle Mitarbeitenden und die Organmitglieder, für die beiden Letztgenannten auch im Falle einer Inanspruchnahme durch das Unternehmen selbst. Die EVH Data Risk schützt damit bei Datenschutzverletzungen auch das Privatvermögen der Mitarbeitenden und der Entscheidungsträger umfassend.

**EVH = Erweiterte Vermögensschaden-Haftpflichtversicherung*

Dr. Michael Fortmann
michael.fortmann@union-paritaet.de

Auszug aus dem Informationsdienst
Ausgabe 3/2018

UNION Versicherungsdienst GmbH
Klingenbergstraße 4
32758 Detmold
Telefon +49 (0) 5231 603-0
E-Mail info@union-paritaet.de