Wo stecken die Defizite in Ihrem Datenschutzkonzept? Bessern Sie zügig nach. Denn die Behörden verhängen mittlerweile empfindliche Sanktionen.

WER NICHT LERNT, MUSS ZAHLEN – RISIKOBETRACHTUNG IM DATENSCHUTZ

Mit der Einführung der europäisch vereinheitlichten Datenschutz-Grundverordnung (DS-GVO) im Jahr 2018 ist der risikobasierte Ansatz in die bestehenden Datenschutzkonzepte eingebaut worden. Rechtsanwalt Stefan Strüwe und Betriebswirt Marco Eck, beide als Berater im Geschäftsfeld Datenschutz bei der Wirtschaftsprüfungs- und Beratungsgesellschaft Curacon tätig, ziehen für die Gesundheits- und Sozialwirtschaft eine Bilanz nach zwei Jahren DS-GVO.

Erfahrungen aus dem Qualitätsmanagement (QM) sind für die Einbettung eines risikobasierten Ansatzes in die Datenschutz-Grundverordnung hilfreich und nahezu unverzichtbar. Die Einrichtungen, die über ein gut strukturiertes QM-System verfügen, tun sich mit den notwendigen Anpassungen im Datenschutz in der Regel leichter als diejenigen, die nicht über ein solches System verfügen. Viele Unternehmen und Einrichtungen des Gesundheits- und Sozialwesens haben die Implementierung eines Datenschutzmanagementsystems unter Beachtung der DS-GVO erfolgreich durchgeführt oder sich zumindest auf den richtigen Weg begeben. Dabei wird die Datenschutzthematik organisatorisch entweder intern von einem Mitarbeitenden bearbeitet oder es wird ein externer Wegbegleiter hinzugezogen.

Datenschutz in COVID-19-Zeiten

In Zeiten der COVID-19-Pandemie ist zwar das Thema Datenschutz nicht im Fokus der medialen Berichterstattung, aber die Aufsichtsbehörden haben ihre Aktivitäten in den vergangenen Monaten deutlich intensiviert. Während sie bei der Umsetzung der DS-GVO anfänglich aufgrund von organisatorischen Hindernissen eher eine reaktive Haltung zeigten, agieren sie aktuell zunehmend proaktiv und sprechen erste Bußgeldbescheide aus.

So wurde im Dezember 2019 durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI) eine Geldbuße in Höhe von 105.000 Euro gegen ein Krankenhaus verhängt. Die bestandskräftige Sanktion beruhte dabei auf diversen datenschutzrechtlichen Defiziten. Beispielsweise wurden Patienten bei der Aufnahme verwechselt[1]. Da es sich hierbei nicht um einen einmaligen Vorfall handelte, kristallisierte sich ein organisatorisches und strukturelles Defizit heraus, aus dem jedoch kein erkennbarer Lernprozess abgeleitet wurde. Das Bußgeld von 105.000 Euro ist ein Warnsignal – auch an andere Einrichtungen – und sollte folgendermaßen interpretiert werden: „Überprüft eure Prozesse und passt sie gegebenfalls an, sodass es im Bereich der Daten nicht zu Verwechslungen kommen kann!“

1 Siehe https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/geldbusse-gegen-krankenhaus-aufgrund-von-datenschutz-defiziten-beim-patientenmanagement.

Hohes Bußgeld – ein Signal mit Wirkung?

Die angestrebte Signalwirkung der Aufsichtsbehörde ist erkennbar und lässt vermuten, dass Sachverhalte in ähnlicher Konstellation mit einer tendenziell höheren Geldbuße geahndet werden dürften. Hier bieten Artikel 83 der Datenschutz-Grundverordnung sowie das jüngst veröffentliche Konzept zur Bußgeldzumessung der Datenschutzkonferenz entsprechende Anhaltspunkte[2].

In der jüngsten Vergangenheit erfolgte unter anderem durch die Landesbeauftragte für den Datenschutz in Niedersachsen (LfD) eine sogenannte Querschnittsprüfung. Hierzu erhielten 50 Unternehmen einen Fragenkatalog, den sie bearbeiten und an die Aufsichtsbehörde zurücksenden sollten[3]. Der Fragenkatalog umfasste zehn Hauptfragegruppen und zielte nicht auf Ja/Nein- oder vorhanden-/nicht vorhanden-Antworten ab, sondern auf eine dynamische Beschreibung der Prozesse. Dies bietet den 50 Unternehmen die Chance, ihre Prozesse zu hinterfragen. Zudem bietet es der Aufsichtsbehörde die Möglichkeit, Soll-Ist-Abweichungen festzustellen und entsprechend ihrer Befugnisse zu reagieren.

Die folgenden drei Datenschutz-Themen stehen aktuell sowohl bei den konfessionellen Aufsichtsbehörden (zum Beispiel den Datenschutzbeauftragten der Kirchen) als auch bei denen der Länder im Fokus der Prüfung.

1. Trackingdienste auf Webseiten

Bei der Nutzung von Drittanbietern, die ein Tracking der Besucher auf Webseiten ermöglichen oder die das Nutzungsverhalten analysieren und an Dritte weiterleiten können, muss eine Einwilligung durch den jeweiligen Webseitenbesucher erfolgen[3]. Dies kann in Form eines Consent-Banners (Cookie-Banner) und dem Verweis auf die Datenschutzerklärung abgebildet werden. Die bisherigen undifferenzierten Hinweise reichen nach der Entscheidung des Europäischen Gerichtshofs (EuGH) nicht mehr aus[4]. Im Fokus der Aufsichtsbehörden stehen vor allem Webseiten und Apps, bei denen sensible personenbezogene Daten verarbeitet werden[5].

2. Rollen- und Berechtigungskonzept

Ein Rollen- und Berechtigungskonzept bietet einerseits die Möglichkeit festzulegen, welche Personen Zutritt zu Räumlichkeiten mit sensiblen Daten erhalten – beispielsweise Server- oder Archivräume. Andererseits regelt es den Zugriff auf die IT-Laufwerke und Ordner. Das Rollen- und Berechtigungskonzept stellt somit eine essenzielle Grundlage für ein Datenschutzmanagement unabhängig von der Größe der Einrichtung dar[6], denn ein Datenschutzverstoß liegt auch vor, wenn Mitarbeitende Zutritt zu beziehungsweise Zugriff auf Daten erhalten, zu deren Einsicht sie im Rahmen ihrer originären Tätigkeit nicht befugt sind[7]. Ein Rollen- und Berechtigungskonzept wird nicht einmalig erstellt, sondern ist ein dynamisches Konzept, das bei Veränderungen der Arbeitsfelder oder der Organisationsstrukturen neu bewertet und angepasst werden muss. Wichtig ist, dass in einer Prozessbeschreibung die Anpassungen des Konzeptes festgehalten werden, um langfristig dessen Funktionsweise sicherzustellen.

3. Verfahren zur sicheren Datenübertragung

Die DS-GVO sieht in Artikel 25 vor, dass die Technikgestaltung nach dem aktuellen Stand der Technik gewählt werden muss. Darunter fällt unter anderem die Übertragung von Daten – beispielsweise in Form von E-Mails. Den Stand der Technik stellt hierbei aktuell die Ende-zu-Ende-Verschlüsselung in Form einer PGP-Verschlüsselung (Pretty Good Privacy) dar. Die Aufsichtsbehörden haben bereits angekündigt, die Datenübertragung im Gesundheitswesen verstärkt zu beobachten, da die verschlüsselte Datenübertragung in der Kommunikation mit Kostenträgern und Vor-, Mit- und Weiterbehandlern diesen Standard erfüllen sollte[8].

Fazit

Es lässt sich festhalten, dass bei erkannten Defiziten die Einstellung: „Das haben wir aber immer schon so gemacht!“ überdacht werden muss. Für den Verantwortlichen gilt, die richtigen Mittel zu finden, um den Anforderungen im jeweiligen Kontext gerecht zu werden. Mehr denn je müssen bestehende Prozesse in enger Abstimmung mit dem Datenschutzbeauftragten hinterfragt und aus Datenschutzvorfällen die richtigen Schlüsse gezogen werden. Außerdem sollten die Verantwortlichen die rechtlichen/gesetzlichen Entwicklungen verfolgen sowie auf Veröffentlichungen der Aufsichtsbehörden achten, um zeitnah auf neue Vorgaben reagieren zu können. Wenn Sie diese Entwicklungen im Blick behalten, befinden Sie sich in ruhigeren Gewässern und können sich auf Ihre Kerntätigkeit fokussieren.

Stefan Strüwe, Marco Eck

Weitere Artikel zu Datensicherheit, DS-GVO, Cybersicherheit:
➥ siehe www.ecclesia.blog

2 Siehe https://www.datenschutzkonferenz-online.de/media/ah/20191016_bußgeldkonzept.pdf.
3 Siehe https://lfd.niedersachsen.de/startseite/datenschutzreform/dsgvo/kriterien-querschnittspruefung-179455.html.
4 Siehe https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190125de.pdf.
5 Siehe https://www.datenschutzkonferenz-online.de/media/en/20191106_entschließung_gesundheitswebseiten_dsk.pdf.
6 Siehe https://www.datenschutzkonferenz-online.de/media/en/20191106_entschließung_gesundheitseinrichtungen_dsk.pdf.
7 Siehe https://www.datenschutz-praxis.de/fachartikel/welche-anforderungen-benutzerrollen-erfuellen-sollten.
8 Siehe https://www.datenschutz-praxis.de/fachnews/dsgvo-konformer-e-mail-versand.

Alle Dokumente am 25. März 2020 abgerufen.