Datenschutzfolgeabschätzung im Gesundheitswesen

Mit der **Revision des Bundesgesetzes** über den Datenschutz (DSG), welche per 1. September in Kraft treten wird, ist bei vielen Unternehmen das Bewusstsein für den Datenschutz gewachsen. Dazu beigetragen haben auch verschiedene Schreckensszenarien von Beratern. Der Verein SHPP hat sich zum Ziel gesetzt, das Thema Datenschutz und Datensicherheit im Gesundheitswesen pragmatisch anzugehen.

▶ URSULA UTTINGER

FOTO: PIXABAY

Gesetzliche Grundlage für Datenschutz-Folgenabschätzung (DSFA)

Die Revision des DSG fördert und fordert verstärkt einen risikobasierten Ansatz bei der Datenbearbeitung. In diesem Sinne verlangt das revDSG in Art. 22 eine Datenschutz-Folgenabschätzung (DSFA). Eine solche ist vorgängig durchzuführen, wenn eine Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen kann.

Der Artikel führt weiter aus, dass sich ein hohes Risiko ergibt bei der Verwendung neuer Technologien, aus Art, Umfang etc. insbesondere ist dies gegeben, wenn umfangreich besonders schützenswerte Personendaten bearbeitet werden. Und dies dürfte im Gesundheitswesen mehrheitlich der Fall sein.

Von einer DSFA kann jedoch abgesehen werden, wenn der private Bearbeiter zur Bearbeitung gesetzlich verpflichtet ist. Ebenfalls kann davon abgesehen werden, wenn ein System, ein Produkt oder eine Dienstleistung eine Datenschutz-Zertifizierung hat oder es einen Verhaltenskodex in der Branche gibt, der auf einer DSFA beruht.

Weiter gilt es zu beachten, dass je nach Dienstleister ein kantonaler Leistungsauftrag besteht, sodass die kantonalen Gesetze anwendbar sind, und diese wiederum verlangen je nach Kanton unabhängig von der Risikoeinschätzung eine DSFA. Mit anderen Worten, als Unternehmen ist man gut beraten, sich mit der DSFA einmal auseinanderzusetzen – ohne dass deswegen gleich ein Studium absolviert werden muss.

Workshop DSFA

SHPP hat deshalb einen Workshop angeboten und durchgeführt. Dieser Workshop war aufgeteilt in einen theoretischen Teil, anschliessend haben die Teilnehmenden eine DSFA für einen konkreten Fall ihres Unternehmens erstellt.

Idealerweise ist die DSFA ein Schritt im Rahmen des Projektmanagements – und sobald Personendaten bearbeitet werden, stellt man sich die Frage, ob die Bearbeitung der Daten für die Betroffenen ein hohes Risiko darstellt. (Achtung: Im Kanton Zürich müssen Unternehmen mit Leistungsauftrag unabhängig von der Höhe des Risikos eine DSFA durchführen).

Schwellenwertanalyse

Als Schwellenwertanalyse bezeichnet man die Beurteilung, ob eine DSFA durchgeführt werden muss. Gemäss revDSG ist eine DSFA immer durchzuführen, wenn der Bearbeiter besonders schützenswerte Personendaten umfangreich bearbeiten will oder wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.

Im Gesundheitswesen dürfte Ersteres häufig der Fall sein. Wobei umfangreich wiederum im konkreten Einzelfall zu interpretieren ist: Umfangreich kann in Bezug auf die Menge der Daten pro Person, eine grosse Menge von Personen oder geografisch umfangreich sein. Im Zweifel empfiehlt es sich, eine DSFA durchzuführen – oder wenn nicht, zu dokumentieren, warum man zum Entschluss gekommen ist, dass es keine umfangreiche Bearbeitung sei.

Ein Hilfsmittel kommt aus der EU: Die Arbeitgruppe Artikel 29 hat eine Leitlinie erstellt, die auf die europäische Datenschutz-Grundverordnung (DSGVO) ausgerichtet ist, aber eine Orientierungshilfe auch in der Schweiz ist. Als Faustregel gilt, wenn zwei oder mehr Kriterien gegeben sind, sollte in der Regel eine DSFA durchgeführt werden.

Kriterien sind, wenn die Datenbearbeitung Folgendes umfasst:

- Evaluation oder Scoring
- Automatisierte Entscheidfindungen mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
- Systemische Überwachung
- Vertrauliche Daten oder höchst persönliche Daten
- Verarbeitung von Daten in grossem Umfang
- Abgleich oder Zusammenführen von Datensätzen
- Daten betreffend schutzbedürftige Personen
- Innovative Nutzung oder Anwendung technischer oder organisatorischer Lösungen
- Verarbeitungen, welche die Ausübung von Rechten oder die Inanspruchnahme von Leistungen oder den Abschluss von Verträgen durch die betroffene Person verhindern

Verfahrensschritte

Zur Theorie gehören die einzelnen Schritte einer DSFA und auch das Wissen, wo es welche Hilfsmittel bereits gibt. In einem ersten Schritt ist die geplante Bearbeitung zu beschreiben und das «Brutto-Risiko» zu definieren: Also: Welche Risiken beinhaltet eine Bearbeitung für die betroffenen Personen.

Dann sind die Risiken zu bewerten – wie hoch ist die Eintretenswahrscheinlichkeit und wie hoch ist das Risiko für die betroffene Person. Bei der Bewertung ist ebenfalls eine Einschätzung mitenthalten, ob die Datenschutzvorschriften eingehalten sind.

In einem letzten Schritt werden Massnahmen beschrieben, mit denen die Risiken reduziert werden können; dies dürfte vor allem durch technische und organisatorische Massnahmen erfolgen.

Ein Beispiel: Wird im Rahmen der Digitalisierung eine Bearbeitung von Daten in eine Cloud verschoben, könnten Zugriffe nur mittels Multi-Faktor-Authentifizierung möglich sein. Also nebst einem Passwort braucht es noch eine biometrische Authentifizierung oder einen Token, um zugreifen zu können. Die Daten sind in der Cloud verschlüsselt, und nur der Datenverantwortliche hat den Schlüssel etc.

Umsetzung einer DSFA

In einem zweiten Schritt haben die Teilnehmenden des Workshops sich in Gruppen aufgeteilt und einen konkreten Fall erarbeitet, wobei die einzelnen Gruppen unterschiedliche Vorlagen genutzt haben (einmal ein Tool von einer kantonalen Datenschutzbehörde, einmal ein Tool von einer Anwaltskanzlei). Dabei zeigte sich schnell, dass die Durchführung einer DSFA mehr Zeit in Anspruch nimmt als man gemeinhin annehmen könnte.

Erkenntnisse aus dem Workshop waren:

- Idealerweise füllt die verantwortliche Person, allenfalls die Projektleitung das Formular bereits aus;
- In einem zweiten Schritt wird dieses Formular in einer grösseren Gruppe diskutiert (keinesfalls einfach abgenickt). Folgende Funktionen sind idealerweise vertreten: Datenschutzberater, IT-Verantwortlicher, Person, in deren Interesse das Projekt/die Datenbearbeitung erfolgt, eventuell noch eine Person, von der man weiss, dass sie Sachen kritisch hinterfragt.

Fazit

Für die Teilnehmenden war insbesondere der Austausch vor Ort mit Personen aus der gleichen Branche sehr wertvoll, nebst dem praktischen Ausfüllen der Formulare. Es gibt nicht ein Formular, das gegenüber den anderen besser ist, vielmehr ist es auch eine Frage des Geschmackes, was man lieber ausfüllt.

Weiter wurde festgestellt, dass je nach Kanton die Behörden die Herausforderungen der Branche mehr oder weniger gut verstehen. Schwierig wird es immer dann, wenn eine Behörde ohne Verständnis für eine Branche Dokumente verlangt, um der Dokumente willen. Gerade in solchen Fällen ist es hilfreich, wenn sich Unternehmen aus dem gleichen Kanton koordinieren.

Die DSFA ist ein neuer Schritt, der im Projektmanagement aufzunehmen ist. Hat man eine DSFA erstellt, werden die nächsten einfacher sein – und bei ähnlichen Bearbeitungen kann auch eine DSFA ergänzt werden bzw. es können einzelne Punkte übernommen werden.

Die DSFA ist Teil der Datenschutz-Compliance. Nebst Datenschutz-Compliance sollte nie vergessen werden: Datenschutz ist auch ein Menschenrecht – und deshalb geht es bei der DSFA auch um die Grundrechte und den Schutz der Persönlichkeit.

SHPP

Da das Gesundheitswesen spezielle Fragestellungen hat, ist inzwischen ein Verein gegründet worden, ausgerichtet auf Datenschutz im Gesundheitsumfeld (vgl. *www.shpp.ch*). Datenschutz ist kein Wettbewerbsvorteil, ein gegenseitiger Austausch hilft allen.

Ursula Uttinger ist unter anderem Dozentin an der Hochschule Luzern und Leiterin Legal & Compliance am Spital Muri. Sie beschäftigt sich seit über 27 Jahren mit dem Thema Datenschutz in verschiedensten Funktionen.