Handlungspflicht bei der Bearbeitung von persönlichen Daten

Datenschutz-Folgenabschätzung im Personalumfeld

Mit der Revision des Datenschutzgesetzes gibt es für Verantwortliche auch eine neue Pflicht: die Erstellung einer Datenschutz-Folgenabschätzung (DSFA), «wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann».[1] Mit der Revision wurde der risikobasierte Ansatz gestärkt, und die DSFA ist eines der Instrumente dazu.[2] Wir zeigen, wie in einem solchen Fall vorzugehen ist.

Von Ursula Uttinger

Im Gegensatz zu Geheimhaltungsvereinbarungen, Datenschutzerklärungen und Auftragsdatenvereinbarungen ist die DSFA bis jetzt weniger im Fokus. Dies mag damit zusammenhängen, dass eine solche erst für neue Bearbeitungen seit dem 1. September 2023 anzuwenden ist.

Idealerweise ist eine DSFA Bestandteil des Projektmanagements: Wird ein neues Projekt lanciert, sollte in einem ersten Schritt geprüft werden, ob Personendaten bearbeitet werden. Wird diese Frage mit «ja» beantwortet, folgt als Nächstes eine Schwellenwertanalyse, die dazu dient, herauszufinden, ob eine Datenbearbeitung ein hohes Risiko für Betroffene mit sich bringen kann. Der Begriff «hohes Risiko» ist auszulegen und wird im Gesetz nicht weiter definiert. Die Praxis und allfällige Gerichtsentscheide – wobei mit Letzteren nicht sehr schnell, falls überhaupt zu rechnen ist – werden dies klären müssen.[3]

In welchem Fall bringt eine Datenbearbeitung ein hohes Risiko für Betroffene?

Auslegungshilfen findet man im Gesetz: Als hohes Risiko gelten die Verwendung neuer Technologien, Art, Umfang und Zweck der Bearbeitung, insbesondere, wenn umfangreich besonders schützenswerte Personendaten bearbeitet und systematisch umfangreiche öffentliche Bereiche überwacht werden (DSG 22 II). Konkret: Entscheidet sich ein Unternehmen, ein neues HR-Tool zu installieren, handelt es sich mit Sicherheit um Personendaten; nun ist zu klären, ob eine DSFA durchzuführen ist. Was unter besonders schützenswerten Daten zu verstehen ist, wird in Art. 5 lit. c DSG definiert:

1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten
2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie
3. genetische Daten
4. biometrische Daten, die eine natürliche Person eindeutig identifizieren
5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen
6. Daten über Massnahmen der sozialen Hilfe

Zumindest bei quellensteuerpflichtigen Personen ist die Religion im Personaldossier zu finden; indirekt dürfte es durch die archivierten Absenzmeldungen auch Anhaltspunkte zu Gesundheitsdaten geben, denn Arbeitsunfähigkeitszeugnisse werden ebenfalls regelmässig abgelegt. Je nach Branche und Funktion kann ein Strafregisterauszug Teil der Personaldaten sein. Ob es nun in grossem Umfang ist, hängt auch von der Grösse des Unternehmens ab. Bei einem KMU mit 20 Mitarbeitenden kann kaum von «grossem Umfang» gesprochen werden. Je grösser das Unternehmen, desto eher sollte eine DSFA durchgeführt werden.

Werden nicht umfangreich besonders schützenswerte Personendaten bearbeitet, kann man als Hilfsmittel für den Entscheid, ob eine DSFA durchzuführen ist, die sogenannte Schwellenwertanalyse der Artikel-29-Datenschutzgruppe[4] nutzen. Dabei handelt es sich um ein Dokument, das für die DSFA nach Art. 35 der europäischen DSGVO[5] erstellt wurde, deren Gesetzestext sich aber nicht fundamental vom schweizerischen Pendant unterscheidet.

Kriterien der Schwellenwertanalyse

Gemäss dieser Schwellenwertanalyse ist eine DSFA durchzuführen, wenn von neun Kriterien zwei erfüllt sind. Dabei handelt es sich um nachfolgende Kriterien:

1. Bewertung oder Einstufung und damit Erstellung eines Profilings
2. Automatisierte Entscheidfindung mit Rechtswirkung oder ähnlicher Bedeutung
3. Systematische Überwachung von Personen
4. Bearbeitung von vertraulichen oder höchst sensiblen Daten

5. Datenverarbeitung in grossem Umfang
6. Abgleich oder Zusammenführung von Datensätzen
7. Daten über schutzbedürftige Personen
8. Innovative Nutzung oder Anwendung neuer Technologien
9. Verarbeitung, die betroffene Personen an der Ausübung eines Rechts oder Nutzung einer Dienstleistung hindert

Ist eine DSFA durchzuführen, muss man sich überlegen, welche Risiken mit einer Bearbeitung für die Betroffenen damit einhergehen. Im Musterformular des Schweizerischen Gewerbeverbands (SGV)[6] ist diese Schwellenwertanalyse bereits enthalten.

In einem nächsten Schritt sind die konkreten Risiken zu bewerten. Hier ist das Formular der Luzerner Datenschutzstelle[7] hilfreich, in dem bereits diverse Risiken erfasst sind. Es wird unterschieden in allgemeine Risiken wie unberechtigter Zugriff, unerwünschte Veränderung der Personendaten, Verlust von Personendaten sowie prozessspezifische Risiken wie Verlust der Vertraulichkeit. Dann kommt aber der eigentliche Knackpunkt: Man sollte sich überlegen, welche Risiken man sonst noch hat. Hier gilt es einerseits kreativ zu sein, und gleichzeitig sollten die Risiken andererseits auch tatsächlich bestehen. Um dies zu erreichen, empfiehlt es sich, diese Risikoanalyse in einem Team zu erstellen. Denn Risikomanagement ist keine exakte Wissenschaft, vielmehr ist dabei die Erfahrung und persönliche Empfindung relevant.[8]

Die beiden Achsen, Eintretenswahrscheinlichkeit und Auswirkungen, sind klar zu definieren, damit ein gemeinsames Verständnis besteht und die Bewertung nachvollzogen werden kann. Die Bezeichnung «hoch» alleine wird unterschiedlich verstanden und interpretiert. Dabei muss in einem ersten Schritt die Bewertung ohne Massnahmen erfolgen, danach sind Massnahmen zu definieren und ist die Bewertung erneut vorzunehmen. Bleibt das Risiko weiterhin hoch, ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) zu konsultieren und vorgängig eine Stellungnahme einzuholen – Art. 23 DSG. Dies bedeutet nicht, dass ein geplantes Projekt nicht möglich ist, sofern die geplante Datenbearbeitung datenschutzkonform ist; allenfalls schlägt der EDÖB Massnahmen zur Eindämmung der festgestellten Risiken vor.[9] Ein hohes Risiko nach Massnahmen dürfte nur äusserst selten vorkommen. Das Ergebnis der DSFA ist zwei Jahre bis nach Beendigung der Datenbearbeitung aufzubewahren (DSV 14[10]).

Von der Erstellung einer DSFA ist ein Unternehmen befreit, wenn der private Verantwortliche gesetzlich zur Bearbeitung verpflichtet ist (DSG 22 IV); auf eine Vorabkonsultation kann verzichtet werden, wenn das private Unternehmen eine Datenschutzberaterin/einen Datenschutzberater ernannt hat und diese/dieser in die DSFA involviert war und sich damit auseinandergesetzt hat.

Fazit

Werden im HR-Umfeld neue Projekte lanciert, dürften Personendaten betroffen sein. In einer frühen Projektphase sollte mittels Schwellenwertanalyse geprüft werden, ob eine DSFA notwendig ist. Muss eine DSFA durchgeführt werden, hilft es, diese im Team zu erstellen. Bereits für die Schwellenwertanalyse wie auch für die DSFA gibt es viele Hilfsmittel; allenfalls lohnt es sich, von diesen das Beste für sich zusammenzutragen. Grundsätzlich ist das Formular des SGV auf das Wesentliche beschränkt, bezüglich möglicher Risiken ist das Formular der Datenschutzstelle Luzern aber hilfreicher. Doch alle Vorlagen und Muster entbinden nicht vom Hinterfragen und Prüfen. Am besten stellt man sich in die Schuhe der betroffenen Personen, um mögliche Risiken zu erkennen. Hohe Risiken dürften nur in den seltensten Fällen bestehen. Falls dies dennoch zutreffen sollte, sind mit der nötigen Ernsthaftigkeit das Projekt und Massnahmen zur Verbesserung des Datenschutzes und der Datensicherheit zu prüfen. Denn eine Datenschutz-/Datensicherheitsverletzung ist möglichst zu verhindern.

Fussnoten

1 Art. 22 DSG (SR 235.1 Bundesgesetz über den Datenschutz).
2 www.edoeb.admin.ch/edoeb/de/home/datenschutz/grundlagen/dsfa.html (22.9.23).
3 EDÖB – Merkblatt zur Datenschutz-Folgenabschätzung (DSFA) nach Art. 22 und 23 DSG, Stand August 2023, Ziff. 4.
4 Datenschutzgruppe nach Artikel 29, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 «wahrscheinlich ein hohes Risiko mit sich bringt» (wp 248 rev. 01).
5 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.
6 www.sgv-usam.ch/media/19650/20221222_dsg_muster_datenschutz_folgenabschaetzung_de.docx (22.9.23).
7 https://tinyurl.com/5x868dfs (25.9.23).
8 Ursula Uttinger/Thomas Geiser, Das neue Datenschutzrecht, Rz 3.40, Basel, 2023
9 BBl 2017, 7062 f.
10 Verordnung über den Datenschutz (DSV) SR 235.11.

Ursula Uttinger ist ausgebildete Juristin mit verschiedenen Nachdiplomstudien und Weiterbildungen. Sie befasst sich seit über 25 Jahren mit dem Datenschutz, war in verschiedenen Unternehmen für den Datenschutz verantwortlich, hat aber auch mehrere Jahre ein Case-Management-Unternehmen geführt und diverse Führungsfunktionen auf GL-Stufe innegehabt. Heute ist sie Dozentin an der Hochschule Luzern und als selbstständige Beraterin für Datenschutz tätig.