Merkblatt Datenschutz-Folgenabschätzung (DSFA)

1. Wann wird eine DSFA erstellt

Eine DSFA ist erforderlich, wenn die beschriebene Datenbearbeitung ein hohes Risiko für die Persönlichkeit (wenn besonders schützenswerte Personendaten bearbeitet oder wenn systematisch umfangreiche öffentliche Bereiche überwacht werden) oder die Grundrechte der betroffenen Personen darstellt bzw. mit sich bringen kann (vgl. Art. 22 Abs. 1 – 3 DSG). Entscheidend ist namentlich, ob eine besonders umfangreiche Bearbeitung besonders schützenswerter Daten erfolgt und ob neue Technologien verwendet werden.

Die DSFA enthält mindestens eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte.

2. Projekt/Datenbearbeitung

Zunächst wird die geplante Bearbeitung beschrieben (Art. 22 Abs. 3 DSG). Es sind bestehende oder geplante Rechtsgrundlagen für die Bearbeitung darzulegen. Analysiert wird, ob und welche Rechtsgrundlagen bestehen, geschaffen oder angepasst werden müssen. Gegebenenfalls werden bestehende Rechtsgrundlagen mit den geplanten Rechtsgrundlagen verglichen (Ist-/Soll-Vergleich).

3. Beschreibung der beabsichtigten Bearbeitung von Personendaten

Dieses Kapitel beinhaltet die Art, den Umfang und den Zweck der Bearbeitung der Personendaten sowie die Umstände, unter denen sie stattfindet (Art. 22 Abs. 2 DSG). Der Zweck gibt Antwort auf die Frage, warum die Personendaten beschafft und bearbeitet werden. Die Art der Datenbearbeitung beschreibt welche Bearbeitung(en) erfolgen soll(en): Beschaffung, Speicherung, Aufbewahrung, Verwendung, Veränderung, Bekanntgabe, Archivierung, Löschung oder Vernichtung von Daten.

Bei der Datenkategorie ist insbesondere anzugeben, ob und inwieweit die Bearbeitung Personendaten bzw. besonders schützenswerte Personendaten betrifft. Dabei muss auch angegeben werden, in welcher Form die Daten vorliegen (z.B. Schrift, Ton, Bild). Auch die Kategorien der betroffenen Personen (z.B. Angestellte, Versicherte) sind zu umschreiben.

Aus den Angaben über den Umfang der Bearbeitung wird ersichtlich, ob eine grosse Menge von Daten bearbeitet werden, ob eine grosse Anzahl von Personen betroffen sind und ob die Bearbeitung in zeitlicher oder in räumlicher Hinsicht umfangreich ist. In zeitlicher Hinsicht muss insbesondere angegeben werden, wie lange die Personendaten bearbeitet und aufbewahrt werden.

4. Risikoanalyse und vorgesehene Massnahmen

Identifizierung und Bewertung der Risiken für die Grundrechte der betroffenen Person
Risiken sind nicht angestrebte, mögliche negative Folgen, die Auswirkungen auf die Grundrechte der betroffenen Person haben oder haben können.

Beispiele für Risiken (nicht abschliessend): Verlust von Daten, fehlerhafte Daten, übermässige Erhebung von Daten, Einsicht durch Unbefugte, unzulässige Verknüpfung von Daten oder Profilbildung,

übermässige lange Aufbewahrung von Daten, Übermittlung von Daten in Drittstaaten, die Verfügungsfreiheit der betroffenen Person über ihre Daten wird stark eingeschränkt, es wird eine grosse Menge an Daten bearbeitet, eine hohe Anzahl Personen hat Zugriffsmöglichkeit auf die Daten.

Zunächst werden mögliche Risiken einer geplanten Bearbeitung von Personendaten identifiziert.

Es gibt unterschiedliche Arten von Risiken. Informationssicherheitsrisiken stehen im Zusammenhang mit der Datensicherheit. Beispiele: Verletzung der Integrität von Personendaten z.B. durch Manipulation oder Fehler im System, Verletzung der Vertraulichkeit z.B. durch Schwachstellen im System, missbräuchliche Verwendung der Informationen oder ein Angriff auf das System, Verletzung der Verfügbarkeit z.B. durch Ausfall der Systeme, Verlust der Informationen oder Ransomware, fehlende Nachvollziehbarkeit, d.h. die Bearbeitung der Personendaten kann nicht nachvollzogen werden, z.B. durch Fälschung oder Verlust der Protokolle.

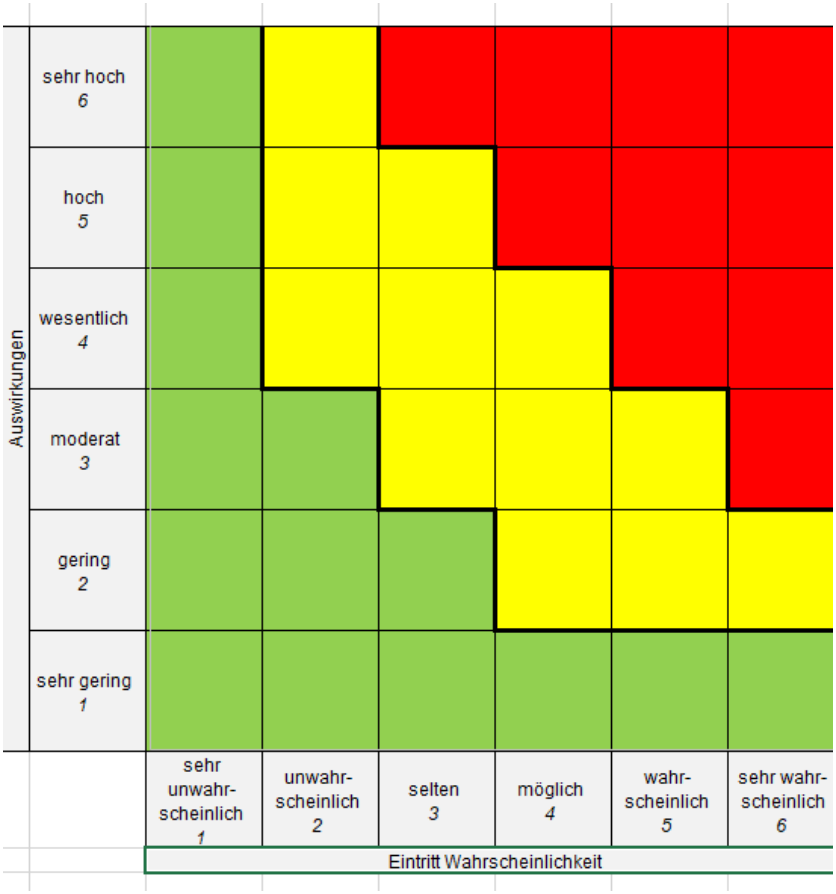
Datenschutzrisiken beziehen sich auf die einzelnen Datenbearbeitungsvorgänge. Sie gehen über die Datensicherheit hinaus. Beispiele: unrechtmässige Beschaffung und Bearbeitung von Personendaten, Verwendung von Personendaten zu nicht vorgesehenen Zwecken, Bearbeitung von inkorrekten Daten, unbefugter Zugriff auf Personendaten, übermässig lange Aufbewahrung von Personendaten, Verweigerung der Rechte der betroffenen Personen.

Eintrittswahrscheinlichkeit

Wurden die möglichen Risiken identifiziert, so wird für jedes Risiko zusätzlich die Eintrittswahrscheinlichkeit des Risikos und deren Auswirkung auf die Grundrechte der betroffenen Person.

Die Risikobewertung erfolgt mit Hilfe der 6 x 6-Risikomatrix, die auch im Rahmen der detaillierten Risikoanalyse zum ISDS-Konzept zur Anwendung gelangt[1]. Die Risiken, die in der Risikomatrix als gelb oder rot erscheinen, sind als hohes Risiko zu erachten. Für diese Risiken müssen Massnahmen vorgesehen werden. Die Massnahmen haben zum Ziel, die Risiken zu reduzieren.

[1] Die Vorlage für die detaillierte Risikoanalyse zum ISDS-Konzept ist unter folgender Webseite abrufbar: https://www.ncsc.admin.ch/ > Dokumentation > Informatiksicherheitsvorgaben Bund > Sicherheitsverfahren >Erhöhter Schutz.



Bei den Auswirkungen kann es sich um physische Auswirkungen (z.B. eine fehlerhafte medizinische Behandlung aufgrund fehlerhafter Daten), materielle Auswirkungen (z.B. Verlust der Arbeitsstelle, Missbrauch der Kreditkarte, Erhebung ungerechtfertigter Gebühren) oder immaterielle Auswirkungen (Diskriminierungen, u.a. Rassismus, Sexismus, gesellschaftliche Nachteile, Stigmatisierung wegen Krankheit) handeln. Die Auswirkungen auf die Grundrechte der betroffenen Person oder der Schweregrad der Risiken können in sechs Stufen eingeteilt werden: sehr gering, gering, moderat, wesentlich, hoch oder sehr hoch. Die Stufen können wie folgt umschrieben werden.

sehr gering: keine Auswirkung auf die Grundrechte; keine merklichen moralischen oder sozialen Verletzungen; kein adäquat kausaler finanzieller Schaden. z.B. geringfüge Überschreitung der zulässigen Aufbewahrungsdauer von Personendaten; unerwünschte Telefonanrufe oder Nachrichten ohne direkte oder indirekte Folgen.

gering: vernachlässigbare Auswirkung auf die Grundrechte; kaum merkliche moralische oder soziale Verletzungen; evtl. adäquat kausaler minimaler finanzieller Schaden. z.B. Notwendigkeit, das eigene Internetkonto, die E-Mail-Adresse oder die Telefonnummer zu ändern.

moderat: geringfügige langfristige oder schwerwiegende kurzfristige Auswirkung auf die Grundrechte; geringe psychische, moralische oder soziale Verletzungen; evtl. adäquat kausal finanzieller Schaden. z.B. intransparente, unzulässige Beeinflussung des Kaufverhaltens.

wesentlich/hoch: schwerwiegende langfristige Auswirkung auf die Grundrechte; mittelschwere physische, psychische, moralische oder soziale Verletzungen; substanzieller adäquat kausal finanzieller Schaden. z.B. Verweigerung/Auflösung eines Vertragsverhältnisses; Reputationsschäden.

sehr hoch: fatale Auswirkung auf die Grundrechte; schwerwiegende physische, psychische, moralische oder soziale Verletzungen; existenzgefährdender adäquat kausal finanzieller Schaden, z.B. folgenschwere falsche medizinische Behandlung aufgrund unrichtiger Patienteninformationen oder

Patientenidentifikation; Risiko der grenzüberschreitenden Verfolgung aufgrund von persönlichen in den Herkunftsstaat gelangenden Daten von Asylsuchenden, mit Auswirkungen auf die betroffene Person oder ihre Familie (körperliche Unversehrtheit, Leben usw.).

Die Eintrittswahrscheinlichkeit ist eine Schätzung der Wahrscheinlichkeit für das Eintreten eines bestimmten Ereignisses in einem bestimmten Zeitraum in der Zukunft. Sie ist auch in sechs Stufen einzuteilen: sehr unwahrscheinlich, unwahrscheinlich, selten, möglich, wahrscheinlich, sehr wahrscheinlich. Bei der Beurteilung der Wahrscheinlichkeit kann die Legende, die im Rahmen der detaillierten Risikoanalyse zum ISDS-Konzept zur Anwendung gelangt, herangezogen werden. Demnach ist die Wahrscheinlichkeit nach dem nachfolgenden Massstab zu bemessen:

sehr unwahrscheinlich	über 10 Jahren
unwahrscheinlich	alle 5-10 Jahre
selten	alle 3-5 Jahre
möglich	alle 2-3 Jahre
wahrscheinlich	alle 1-2 Jahre
sehr wahrscheinlich	mehrmals pro Jahr

Vorgesehene Massnahmen

Mögliche Massnahmen zum Schutz der betroffenen Personen können sowohl organisatorische als auch technische Massnahmen sein.

Beispiele für organisatorische Massnahmen (nicht abschliessend): die Implementierung von Schulungen, Weisungen, Benutzeranleitungen, Berechtigungskonzepte, Geheimhaltungspflichten, ISMS, Prozesse für Auskunftsrechte, Prozesse für Löschgesuche sowie Compliance-Checks.

Beispiele für technische Massnahmen (nicht abschliessend): Zugriffskontrollen, Zugangskontrollen, zeitlich begrenzte Zugriffe, Verschlüsselungen, Anonymisierungen und Datenminimierungen.

5. Konsultation Datenschutzberater / EDÖB

Ergibt sich aus der DSFA, dass die Datenbearbeitung trotz der umgesetzten oder vorgesehenen Massnahmen ein hohes Risiko für die betroffenen Personen zur Folge hat, so muss der Datenschutzberater und schliesslich der EDÖB konsultiert werden (vgl. Art. 10 und Art. 23 DSG).