



Fachstelle Datenschutz

Merkblatt¹ Datenschutz-Folgenabschätzung

A Was ist eine Datenschutz-Folgenabschätzung (DSFA)²

Eine DSFA ist ein Verfahren, anhand dessen die Bearbeitung von Personendaten beschrieben, ihre Notwendigkeit und Verhältnismässigkeit bewertet und die Risiken für die Grundrechte der betroffenen Person durch eine entsprechende Risikoabschätzung und die Ermittlung von Gegenmassnahmen besser kontrolliert werden soll. Kurz: Mittels einer DSFA sollen Risiken identifiziert und bewertet werden, die durch den Einsatz von neuen Verfahren, Technologien und Systemen im Rahmen der Datenbearbeitung entstehen.

B Wer erstellt die DSFA?

Die DSFA ist vom öffentlichen Organ bzw. von derjenigen Stelle innerhalb der Verwaltung durchzuführen, welche über das Projekt entscheidet und welche die Verantwortung für die Datenbearbeitung trägt.

C In welchen Fällen ist eine DSFA erforderlich?

Wenn eine Bearbeitung von Personendaten ein *hohes Risiko* für die Grundrechte der betroffenen Person mit sich bringen kann.

Das hohe Risiko ergibt sich insbesondere aus

- der Art
- dem Umfang
- den Umständen
- dem Zweck

der Bearbeitung und besonders dann, wenn neue Technologien³ verwendet werden.

D Welche Bearbeitungsvorgänge stellen ein hohes Risiko dar und es ist in jedem Fall eine DSFA erforderlich?

Bearbeitungsvorgänge	Beispiel / nähere Umschreibung
Umfangreiche Datenbearbeitung folgender Kategorien von Personendaten: <ul style="list-style-type: none"> – Religiöse, weltanschauliche sowie politische Ansichten und Tätigkeiten – Gesundheit, Intimsphäre und ethnische Zugehörigkeit – Genetische Daten – Biometrische Daten, die eine natürliche Person eindeutig identifizieren – Leistungen und Massnahmen der sozialen Hilfe – Strafrechtliche sowie disziplinarische Verfahren und Sanktionen 	Mitgliedschaften in Organisationen und Vereinen, Informationen über Krankheiten, Behinderungen, spezifische Erbmerkmale und daraus folgende Krankheitsdispositionen, Finger- oder Handabdrücke, charakteristische Gang- oder Sprechart, Vollzug der Arbeitslosenversicherung, administrative Führerausweistzüge

¹ Dieses Merkblatt stützt sich u.a. auf die Liste der Verarbeitungstätigkeiten der Europäischen Datenschutzkonferenz, den Heidelberger Kommentar zur Datenschutz-Grundverordnung, Hrsg. Schwartmann/Jaspers/Thüsing/Kugelmann (nachfolgend Heidelberger Kommentar) und das Merkblatt vom 19.08.2018 der Beauftragten für Öffentlichkeit und Datenschutz des Kantons Aargau.

² Art. 8a Datenschutzgesetz, sGS 142.1, DSG.

³ Bei einer neuen Technologie sind die persönlichen und sozialen Folgen des Einsatzes noch nicht vollständig untersucht und weisen viele Unbekannte auf. Heutige Beispiele sind Autonomik, Big Data, Cloud Computing, Smart Cars, Smart Cities oder Datenbearbeitung innerhalb von IoT-Systemen, Heidelberger Kommentar, S. 786.



Zusammenstellung von Personendaten, welche die Beurteilung der Persönlichkeit einer natürlichen Person erlaubt	Tracking-Verfahren, Sicherheitsüberprüfungen, Führungszeugnisse
Automatisierte, systematische und umfassende Bewertung persönlicher Aspekte (Profiling)	Es werden grössere Datenmengen zusammengeführt und automatisiert ausgewertet, wodurch etwa besondere Vorlieben und Interessen oder Aufenthaltsorte einzelner Personen ermittelt werden können.

E Welche Bearbeitungsvorgänge können ein hohes Risiko darstellen?

Bearbeitungsvorgänge	Beispiel / nähere Umschreibung
Verwendung neuer Technologien, Mechanismen und Verfahren	Umfangreiche Nutzung von Cloud-Diensten, Fingerabdrucksensoren, Gesichtserkennung
Zwei oder mehrere öffentliche Organe bearbeiten Personendaten in einem gemeinsamen elektronischen System	Kantonales Einwohnerregister
Ableichung, Zusammenführung und Verknüpfung von Datensätzen	Beispielsweise bei der Verwendung von Personendaten im statistischen Bereich
Auftragsdatenverarbeitung (Datenbearbeitung durch Dritte)	Bewerbermanagement
Übermittlung von Personendaten in Länder ohne gleichwertiges Datenschutzniveau	Siehe Staatenliste des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten ⁴
Daten besonders schutzbedürftiger Personen oder Personen in einem Abhängigkeitsverhältnis werden bearbeitet (Patientinnen und Patienten, Minderjährige, Arbeitnehmende)	eDossier, Patientendossier

Faustregel:

Sind zwei der Kriterien unter Bst. E erfüllt, ist i.d.R. eine DSFA erforderlich. Je mehr Kriterien eine Bearbeitung erfüllt, umso höher wird das Risiko für die Rechte und Freiheiten der betroffenen Person i.d.R. eingeschätzt.⁵

⁴ <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html> (siehe Staatenliste).

⁵ Heidelberger Kommentar, S. 799.



Ein weiteres Indiz für ein hohes Risiko liegt vor, wenn die Bearbeitung der Personendaten die anschliessend aufgezählten Folgen haben kann:

- Diskriminierung
- Identitätsdiebstahl oder –betrug
- finanzieller Verlust
- Rufschädigung
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Personendaten
- unbefugte Aufhebung der Pseudonymisierung
- andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile
- wenn betroffene Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden.⁶

F Inhalt der DSFA

1. Projektbeschreibung:

- Verantwortliche Stelle
- Daten bearbeitende Stellen
- Bezeichnung des Verfahrens
- Systematische Beschreibung der geplanten Bearbeitung (Aufzählung nicht abschliessend):
 - Zweck und Art der Datenbearbeitung
 - Umfang (beispielsweise Häufigkeit des Abrufs)
 - Umstände (Möglichkeit der Person, sich der Bearbeitung zu entziehen, automatisierte Bearbeitung, Transparenz für die betroffene Person gewährleistet)
 - Empfänger der Daten
 - Kreis der betroffenen Personen
 - Aufbewahrungsdauer der Daten
 - verwendete Technologie bzw. eingesetzte Technik (Daten und ihre Formate, Verschlüsselungsmethoden, verwendete IT-Systeme und deren Schnittstellen, Zugriffsberechtigungen sowie beteiligte Personen)
 - Klassifizierung der Personendaten
- 2. Sich daraus ergebende Risiken (physische, materielle und immaterielle Schäden) für die betroffenen Personen
- 3. Bewertung dieser Risiken
- 4. Abhilfemassnahmen:
 - Darstellung der geplanten Abhilfemassnahmen, inkl. Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt wird
 - Nachweis, dass das Datenschutzgesetz eingehalten wird
- 5. Bewertung der geplanten Abhilfemassnahmen
- 6. Bewertung des Restrisikos, Notwendigkeit und Verhältnismässigkeit der Inkaufnahme
- 7. Fazit

⁶ Heidelberger Kommentar, S. 790.



G Abschluss der DSFA

Ergibt die DSFA, dass trotz getroffener Massnahmen das *Risiko* für die Grundrechte der betroffenen Personen *hoch bleibt*, muss das Vorhaben der Fachstelle für Datenschutz zur Vorabkonsultation unterbreitet werden⁷. Siehe dazu das Merkblatt zur "Vorabkonsultation" <https://www.sg.ch/sicherheit/datenschutz/merkblaetter-und-arbeitshilfen.html>

Anmerkung: Es gibt Bearbeitungsvorgänge, die in jedem Fall zur Vorabkonsultation vorgelegt werden müssen, siehe auch dazu oben erwähntes Merkblatt zur "Vorabkonsultation".

Die Unterlagen zur DSFA müssen aufbewahrt werden, damit der Nachweis der Einhaltung der Datenschutzvorschriften erbracht werden kann.⁸

Die Fachstelle für Datenschutz steht Ihnen für Fragen gern zur Verfügung:
058 229 14 14 (Mo bis Mi und Fr)

⁷ Art. 8b DSG.

⁸ Art. 3 Abs. 3 DSG.