ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence, de la protection des données et de la médiation ATPrDM
Kantonale Behörde für Öffentlichkeit, Datenschutz und Mediation ÖDSMB

Chorherrengasse 2, 1700 Freiburg

T +41 26 322 50 08
www.fr.ch/oedsmb

2024-PrD-301

V2.2 vom 9. Januar 2025

1 Datenschutz-Folgenabschätzung (Teil I) – Vorabprüfung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person

1.1 Grundlagen der Datenschutz-Folgenabschätzung

Führt eine neue Bearbeitung von Daten voraussichtlich zu einem erhöhten Risiko für die Grundrechte der betroffenen Person, so muss der Verantwortliche vorgängig eine Datenschutz-Folgenabschätzung durchführen (DSFA ; Art. 41 Abs. 1 DSchG).

Eine DSFA ist übrigens nur dann erforderlich, wenn das Projekt auf die Bearbeitung von Personendaten im Sinne von Artikel 4 Absatz 1 Buchstabe a DSchG abzielt. So besteht für Tätigkeiten, bei denen öffentliche oder anonyme Daten bearbeitet werden, keine Pflicht zur Durchführung einer DSFA.

Wichtige Begriffe

Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Nicht als Personendaten gelten der Staatshaushalt, meteorologische Messungen oder Daten, die nicht mit einer bestimmbaren Person in Verbindung gebracht werden oder gebracht werden können.

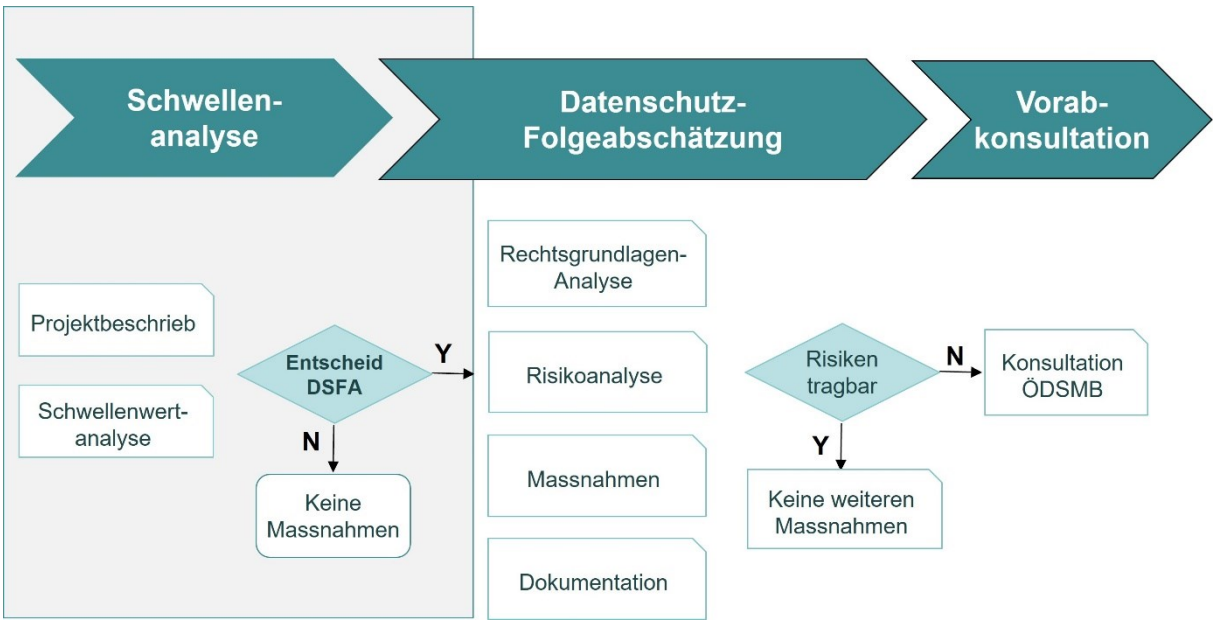
1.2 Zweck des Dokuments

Um festzustellen, ob die geplante Datenbearbeitung ein hohes Risiko darstellt oder nicht, enthält dieses Dokument ein Risikomessungsschema. Die Verwendung dieses Dokuments ist fakultativ. Der Verantwortliche kann seine DSFA anderweitig dokumentieren, unter anderem mit dem ISDS-Konzept.

Diese Vorlage ist auszufüllen, sobald das ISDS-Konzept erstellt worden ist. Sie ergänzt das ISDS-Konzept und kann sich auf dieses beziehen.

1.3 Entscheidungsprozedur

Das nachstehende Schema fasst die verschiedenen Etappen einer DSFA zusammen. Stellt sich heraus, dass ein erhöhtes Risiko besteht, so muss der Verantwortliche die Aufsichtsbehörde vorab konsultieren (Art. 42 Abs. 1 DSchG).



In einem ersten Schritt einer DSFA, der sogenannten «Schwellenanalyse» sollte vorab ein **Beschrieb des Datenbearbeitungsprojekts** erstellt werden. In Kap. 2 dieses Dokuments ist eine entsprechende Vorlage zu finden.

Sobald der Projektbeschrieb vorliegt, kann der Verantwortliche die **eigentliche Schwellenwertanalyse** durchführen. Nach Abschluss dieser Analyse wird das Risiko für die Grundrechte der betroffenen Personen als hoch oder niedrig eingestuft.

Bei einem hohen Risiko ist für die geplante Datenbearbeitung eine DSFA erforderlich.

2 Organisation und Beschrieb der Datenbearbeitung

In diesem Kapitel wird auf den Projektbeschrieb im Allgemeinen eingegangen. Es bezieht sich auf alle Bearbeitungstätigkeiten, einschliesslich aller IT-Projekte, die eine Bearbeitung von Personendaten beinhalten.

2.1 Organisation

Auftraggeber der Datenbearbeitung	
Verantwortlicher der Datenbearbeitung	
Datenschutzverantwortlicher	

Wichtige Begriffe

- *Auftraggeber der Datenbearbeitung* ist die Stelle, die für die Ergebnisse des Vorhabens und die Erreichung der Ziele unter Einhaltung der festgelegten Kosten und Fristen verantwortlich ist. Er ist für die Leitung des Datenbearbeitungsvorhabens verantwortlich und führt es zu einem erfolgreichen Abschluss. Es ist jeweils nur eine Stelle anzugeben.
- *Verantwortlicher der Datenbearbeitung* ist die Stellen, die über den Zweck und die Mittel der Bearbeitung von Personendaten entscheidet (Art. 4 Abs. 1 Bst. h DSchG). Konkret ist dies das öffentliche Organ, das über die Bearbeitung der Personendaten, den Zweck der Bearbeitung und die Mittel für die Bearbeitung entscheidet. Es kann mehrere für eine gemeinsame

Datenbearbeitung Verantwortliche geben (Art. 36 Abs. 2 DSchG). Gegebenenfalls muss die Verantwortung jedes beteiligten öffentlichen Organs präzisiert und dokumentiert werden (welches öffentliche Organ ist für die Richtigkeit der Daten verantwortlich, welches Organ ist für die technische Umsetzung der Softwarelösung verantwortlich usw.). Es sind eine oder mehrere Stellen anzugeben.

- *Datenschutzverantwortlicher* ist die natürliche Person, die für Datenschutzfragen zuständig ist und für den Verantwortlichen der Datenbearbeitung arbeitet. Sie ist die Ansprechperson beim Verantwortlichen der Datenbearbeitung. Es sind eine oder mehrere natürliche Personen anzugeben.

2.2 Beschrieb der Datenbearbeitung

Auftrag	
Zweck der Datenbearbeitung	
Liste der zu bearbeitenden Personendaten	
Kreis der Benutzer	
Eingesetzte Technologien	
Betrieb (on premise / Cloud)	
Auftragsbearbeitung und Auslagerung	

Wichtige Begriffe

- *Der Auftrag* besteht darin, das allgemeine Ziel des Vorhabens zu präzisieren. Beispiele: Anlegen eines Registers der Besitzer von Öltanks, die Wasser verunreinigen können, Implementierung einer Fakturierungslösung für alle Verwaltungseinheiten.
- *Der Zweck der Datenbearbeitung* definiert den Zweck der bearbeiteten Daten.
- *Die eingesetzte Technologie* bezeichnet die technische Umsetzung der Datenbearbeitung. Für eine Datenbearbeitungsaktivität können mehrere Technologien eingesetzt werden. Beispiele: Nutzung von Cloud-Diensten wie zum Beispiel Software as a Service (SaaS[1]), Nutzung von künstlicher Intelligenz, Mobile Computing über eine Smartphone-App usw.
- Beim *Betrieb* geht es um die Bestimmung des Nutzungsmodells für die Daten. Insbesondere ist anzugeben, ob die Daten intern oder über Drittanbieter bearbeitet werden. Beispiele: Hosting der Daten in eigenen Rechenzentren, auf in vom ITA eingerichteten Infrastrukturen (intern), ausgelagertes Hosting bei einem Dienstleister, Bereitstellung der Daten über die Cloud, usw.

[1] SaaS: Das SaaS-Modell basiert auf dem Prinzip, dass Software und IT-Infrastruktur von einem externen IT-Dienstleister betrieben und vom Kunden als Dienstleistung in Anspruch genommen werden.

3 Schwellenwertanalyse

		Nein	Ja
1	Werden besonders schützenswerte Personendaten in grossem Umfang bearbeitet?	☐	☐
2	Ist eine grosse Anzahl an Personen betroffen?	☐	☐
3	Werden die Personendaten von verschiedenen Organisationseinheiten genutzt/ergänzt/ausgewertet?	☐	☐
4	Findet die Datenbearbeitung ausserhalb der Schweiz in Staaten statt, die nicht der Datenschutz-Grundverordnung (DSGVO) unterliegen?	☐	☐
5	Werden die Daten in einer Cloud bearbeitet?	☐	☐
6	Werden die Daten oder Teile davon zu Profilingzwecken eingesetzt, resp. können in späteren Schritten der Datenbearbeitung dazu eingesetzt werden?	☐	☐
7	Werden neue Technologien, Mechanismen oder Prozeduren eingesetzt?	☐	☐
8	Werden umfangreiche öffentliche Bereiche systematisch überwacht?	☐	☐
9	Werden Personendaten in Drittstaaten *übermittelt*, wo die ausländische Gesetzgebung keinen angemessenen Schutz gewährleistet?	☐	☐
10	Kann eine grosse oder unbegrenzte Anzahl Personen auf die Daten zugreifen?	☐	☐
11	Bestehen Risiken bei der Datenbearbeitung, die eine datenschutzkonforme Bearbeitung verhindern könnten? (Entwicklung, Betrieb, Support etc.)	☐	☐

Wichtige Anmerkungen zu den obigen Fragen:

Frage 1	«*besonders schützenswerte Personendaten*»: bei den besonders schützenswerten Personendaten handelt es sich um die Daten nach Art. 4 Abs. 1 Bst. c DSchG. Beispiele: Gesundheitsdaten, Daten zu Massnahmen der Sozialhilfe oder zu religiösen Tätigkeiten. «*in grossem Umfang*» nimmt Bezug auf eine umfangreiche Bearbeitung. Es sind insbesondere folgende Kriterien zu berücksichtigen: die Anzahl der betroffenen Personen, das Volumen der bearbeiten Daten, die Dauer oder Dauerhaftigkeit der Bearbeitungstätigkeit oder auch die geographische Ausdehnung einer Bearbeitungstätigkeit. Eine Bearbeitung in grossem Umfang liegt auch vor, wenn Daten systematisch bearbeitet werden, z.B. die Personendaten einer ganzen Dienststelle, eines Spitals, die Gesamtheit der Sozialhilfebezüger oder wenn Daten aus verschiedenen Quellen zusammengeführt oder verknüpft werden
Frage 2	«*grosse Anzahl an Personen*» ist ein unbestimmter Begriff, der im Ermessen des Verantwortlichen der Datenbearbeitung liegt. Es kann sich um eine absolute Zahl von Personen handeln oder um eine relative Anzahl nach Massgabe des erfassten Personenkreises. Wie zum Beispiel die Schülerdaten einer Primarschule.

	Betroffene Personen sind Personen, deren Daten bearbeitet werden. Es handelt sich also nicht um die Personen, die zur Erfüllung ihrer Aufgaben auf die verarbeiteten Daten zugreifen können (vgl. Frage 10).
Frage 4	*Die DSGVO* (Verordnung EU 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) ist eine Verordnung der Europäischen Union. Sie gilt für die 27 Mitgliedstaaten der Europäischen Union.
Frage 5	Unter *Cloud* sind Datenbearbeitungen zu verstehen, die an einem anderen Ort durch von Dritten betriebene Server durchgeführt werden (Art. 4 Abs. 1 Bst. g DSchG).
Frage 6	*Profiling ist jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Personendaten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser Person zu analysieren oder vorherzusagen (Art. 4 Abs. 1 Bst. f DSchG).* *Mit anderen Worten geht es darum, aus den bearbeiteten Daten Informationen über Personen abzuleiten.*
Frage 7	«*neue Technologien, Mechanismen oder Prozeduren*»: Darunter fallen die Benutzung neuartiger, innovativer Technologien, neuartiger Bearbeitung oder wenn eine bereits genutzte Technologie signifikante Veränderungen erfährt. Erfasst werden ebenfalls neuartiges Material und neuartige Hard- und Software. Z.B. die Einführung eines Portals, Einsatz von Body-Cams, Einsatz von Bewertungsplattformen für die öffentliche Verwaltung, biometrische Verfahren, Einsatz von Algorithmen für automatisierte Entscheidfindung, Einsatz von künstlicher Intelligenz, automatisierte Auswertung von Video-Aufnahmen, Smart Health usw.
Frage 8	«*systematisch überwacht*»: Die Überwachung ist vereinbart, organisiert oder methodisch oder erfolgt im Rahmen einer Strategie oder eines allgemeinen Datenerfassungsplans. Darunter fallen nicht nur Videoüberwachungen, sondern etwa auch die automatische Erfassung von Fahrzeugkennzeichen in öffentlichen Parkhäusern oder Parkplätzen, die Überwachung in einem Spital, an Bushaltestellen usw.
Frage 10	«*grosse oder unbegrenzte Anzahl Personen*» ist ein unbestimmter Begriff, der im Ermessen des Verantwortlichen liegt. Es kann sich um eine absolute Zahl von Personen handeln oder um eine relative Zahl im Verhältnis zum erfassten Personenkreis. Dazu gehören auch Online-Zugriffe oder Abrufverfahren. Beispiel: alle Mitarbeiterinnen und Mitarbeiter des Staates.

4 Entscheid

Wenn Sie mindestens eine der Fragen in Kap. 3 mit «JA» beantwortet haben, ist eine Datenschutz-Folgenabschätzung obligatorisch.

Es braucht eine Datenschutz-Folgenabschätzung	NEIN ☐	JA ☐

Datum: Signatur:

Für die Durchführung der Datenschutz-Folgenabschätzung können Sie das Dokument «Datenschutz-Folgenabschätzung Teil II - Risikobeurteilung aus Sicht des Datenschutzes» verwenden.