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

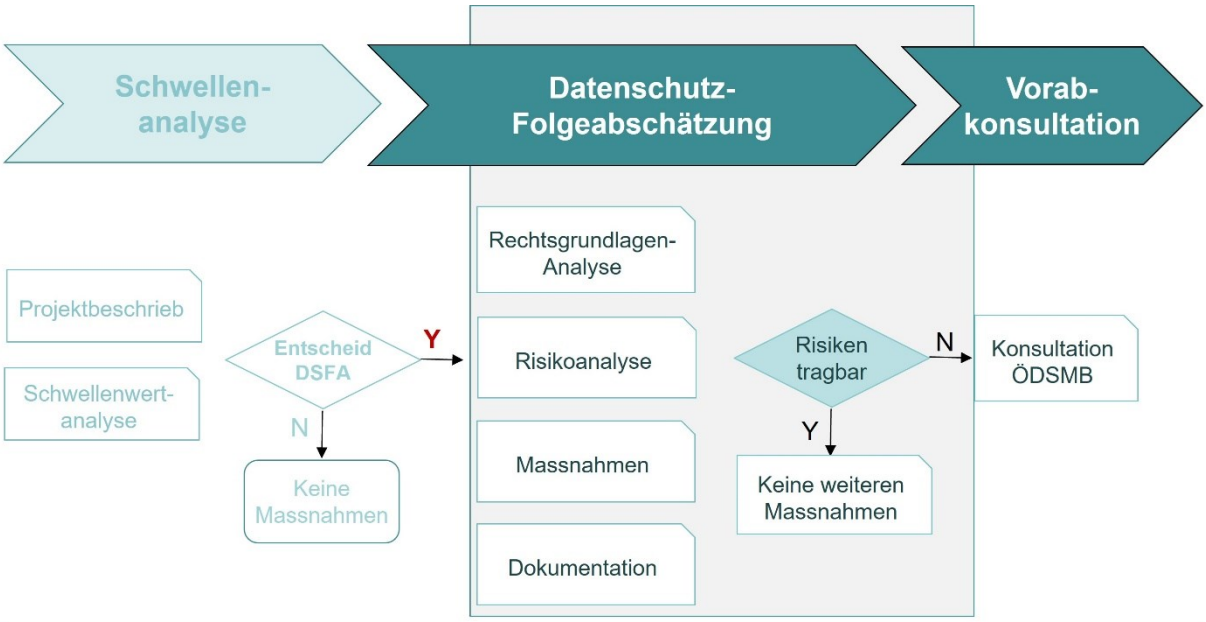
2024-PrD-301

V2.2 vom 9. Januar 2025

1 Datenschutz-Folgenabschätzung (Teil II) – Risikobeurteilung aus Sicht des Datenschutzes

1.1 Entscheidungsprozedur

Die Schwellwertanalyse Ihrer Datenbearbeitung hat ergeben, dass die Risiken für den Datenschutz abgeklärt werden müssen. Das weitere Vorgehen ist hier schematisch dargestellt:



Die eigentliche DSFA basiert auf:

1. der Rechtsgrundlagenanalyse,
2. der Risikoanalyse,

3. dem Massnahmenkatalog,
4. und der Analysedokumentation.

Dieses Dokument dient als Wegleitung zu den obigen ersten drei Themen einer DSFA. Die Dokumentation ist vom jeweiligen Verantwortlichen zu erstellen.

1.2 Vorgehen

Der Formularteil in diesem Dokument ist in der Reihenfolge der Kapitel auszufüllen.

In Kap. 3 sind die Risiken in einer Situation einzuschätzen, in der keine Sicherheitsmassnahmen ergriffen werden. In der Praxis sind einige Massnahmen bereits implementiert. Daher sollte von einer hypothetischen Situation ausgegangen werden, in der keine Massnahmen ergriffen werden.

In Kap. 5 sind die Risiken in einem Kontext einzuschätzen, in dem alle Sicherheitsmassnahmen umgesetzt sind oder umgesetzt werden sollen.

Nur wenn die Bearbeitungstätigkeiten trotz Massnahmen hohe Risiken aufweisen, muss der Verantwortliche die Aufsichtsbehörde vorab konsultieren (Art. 42 Abs. 1 DSchG).

Eine Liste mit Beispielen möglicher Dokumente findet sich in Kap. 7 dieses Dokuments.

Die Aufsichtsbehörde teilt ihre etwaigen Einwände und Empfehlungen zu der geplanten Bearbeitung innerhalb einer Frist von zwei Monaten mit. In Ausnahmefällen kann diese Frist um einen Monat verlängert werden, wenn es sich um eine komplexe Datenbearbeitung handelt.

2 Rechtsgrundlagenanalyse

2.1 Rechtsgrundlagen

Auf welchen Rechtsgrundlagen basiert die Datenbearbeitung?

…

2.2 Datenlebenszyklus

Beschreiben Sie den Datenlebenszyklus.

- **Datenerhebung**: Benennen Sie die Quellen und Erhebungsformen

  …

- **Nutzung**: Benennen Sie den Benutzerkreis (auch Abrufverfahren) und die Art der Datennutzung (Beschaffen, Einsichtnahme, Kopieren, Ändern, Bearbeiten im Auftrag usw.)

  …

- **Speicherung**: Benennen Sie die Speicherung (Trägermedien, technische Mittel, Auftragserteilung an Dritte usw.) und die Speicherorte

  …

- **Aufbewahrung**: Benennen Sie die gesetzlichen Vorgaben für die Aufbewahrung (insbesondere Aufbewahrungsdauer)

  …

- **Archivierung**: Benennen Sie die rechtliche Grundlage für/gegen eine Archivierung

  …

- **Löschung**: Benennen Sie die gesetzlichen Vorgaben für die Datenlöschung (Verfahren für die Datenlöschung, Anonymisierung usw.)

  …

2.3 Verhältnismässigkeit

Beschreiben Sie die Verhältnismässigkeit in Bezug auf den Verwendungszweck unter der Prämisse der Datensparsamkeit und Datenvermeidung. Es dürfen nur die Daten erhoben und verwendet werden, die für den jeweiligen Bearbeitungszweck erforderlich sind. Aus dem Grundsatz der Verhältnismässigkeit leitet sich ab, dass der Zweck der Datenbearbeitung so weit wie möglich ohne die Erhebung neuer Daten erreicht werden muss und nur die Daten bearbeitet werden dürfen, die für den verfolgten Zweck absolut notwendig sind.

…

3 Risikobeurteilung aus Sicht des Datenschutzes (siehe Anhang 1)

3.1 Einschätzung der Hauptrisiken (ohne Massnahmen)

	Eintretens-wahrscheinlichkeit	**Auswirkungen:**		
		gering	mittel	hoch
Unerlaubte Zugriffe auf Personendaten (Vertraulichkeit)	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
	Eintretens-wahrscheinlichkeit	**Auswirkungen:**		
		gering	mittel	hoch
Unerlaubte Manipulation der Personendaten (Integrität)	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
	Eintretens-wahrscheinlichkeit	**Auswirkungen:**		
		gering	mittel	hoch
Verlust der Daten / kein Zugriff auf Daten (Verfügbarkeit)	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
	Eintretens-wahrscheinlichkeit	**Auswirkungen:**		
		gering	mittel	hoch
Unerlaubte Bekanntgabe/Weitergabe der Personendaten im In- und/oder Ausland	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
	Eintretens-wahrscheinlichkeit	**Auswirkungen:**		
		gering	mittel	hoch
Kompromittierung von Schutzmassnahmen (Bsp. der Verschlüsselung, Anonymisierung, Pseudonymisierung, Passwortweitergabe, Malware etc.)	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
	Eintretens-wahrscheinlichkeit	**Auswirkungen:**		
		gering	mittel	hoch
Ungenügende oder fehlende Vorgaben für die Benutzenden. Fehlende Sensibilisierung, Schulung und Kontrolle	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐

Fehlende/ungenügende vertragliche Vereinbarungen mit Dienstleistern	**Eintretens-wahrscheinlichkeit**	**Auswirkungen:**		
		gering	mittel	hoch
	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
Weiteres Risiko	**Eintretens-wahrscheinlichkeit**	**Auswirkungen:**		
		gering	mittel	hoch
	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
Weiteres Risiko	**Eintretens-wahrscheinlichkeit**	**Auswirkungen:**		
		gering	mittel	hoch
	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐

4 Massnahmen zur Risikominimierung

Der Verantwortliche für die Datenverarbeitung muss Maßnahmen ergreifen, die geeignet sind, Risiken mit mittlerer oder hoher Auswirkung zu reduzieren. Diese Maßnahmen müssen vor Beginn der vorgesehenen Datenverarbeitung umgesetzt werden.

Der vorliegende Leitfaden enthält im Folgenden eine beispielhafte Liste von Maßnahmen, die sich an der Norm ISO 27002 orientieren.

4.1 Allgemeine Massnahmen für den Grundschutz

	Nein	Ja
Es existiert ein ISMS (Information Security Management System). Die Datenbearbeitung wird darin eingebunden.	☐	☐
Eine Sicherheitsorganisation ist etabliert; Verantwortung, Aufgaben und Kompetenzen für den Datenschutz sind definiert und zugewiesen.	☐	☐
Die Sensibilisierung der BenutzerInnen im Umgang mit Personendaten ist in der Organisation vorhanden (Einführung, Schulung).	☐	☐
Die Daten sind klassifiziert (Art. 9 des Reglements über die Personendaten; DSR) und die Dateneigentümer bestimmt.	☐	☐
Die Applikation wird auf einer zertifizierten Umgebung betrieben (Bsp: ISO 27001)	☐	☐

4.2 Applikationsspezifische Massnahmen

Das Berechtigungskonzept ist erstellt und die Grundsätze des «need-to-know»-Ansatzes sind berücksichtigt.	☐	☐
Alle EmpfängerInnen von Personendaten extern/intern sind bestimmt und es ist sichergestellt, dass diese berechtigt sind, die Daten zu bearbeiten.	☐	☐
Die Integrität der Personendaten ist gewährleistet (keine absichtliche oder unbeabsichtigte Manipulation von Personendaten möglich).	☐	☐
Die nötigen kryptografischen Massnahmen (Verschlüsselung) für den Schutz von Personendaten sind akkurat eingesetzt.	☐	☐
Das Management der kryptografischen Schlüssel ist ausschl. beim verantwortlichen Organ		
Die Massnahmen für einen angemessenen physischen Schutz der Daten und Systeme sind getroffen und auf ihre Effektivität geprüft.	☐	☐
Die Betriebsprozesse für das Change- und Releasemanagement sind etabliert.	☐	☐
Die Daten werden regelmässig gesichert (Backup & Restore).	☐	☐
Es gibt einen angemessenen Schutz gegen Malware.	☐	☐
Die Datenzugriffe werden protokolliert und überprüft.	☐	☐
Die Sicherheitsupdates werden nach getesteten Verfahren zeitnah eingespielt.	☐	☐

Die Netzwerkssicherheit ist gewährleistet.	☐	☐
Die Kommunikationskanäle sind definiert und entsprechen den Datenschutzanforderungen.	☐	☐
Die Lieferanten sind auf die Einhaltung der Datenschutzanforderungen verpflichtet (Verträge, SLA).	☐	☐
Die Sicherheitsmassnahmen werden periodisch überprüft und angepasst.	☐	☐
Es gibt eine Betriebsanleitung/Betriebshandbuch für die Benutzer und/oder Benutzerschulung	☐	☐
Weitere Massnahmen *(bitte angeben)*:	☐	☐

5 Risikoeinschätzung nach Umsetzung der Massnahmen

5.1 Einschätzung der Hauptrisiken (mit Massnahmen)

	Eintretens-wahrscheinlichkeit	Auswirkungen:		
		gering	mittel	hoch
Unerlaubte Zugriffe auf Personendaten (Vertraulichkeit)	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
	Eintretens-wahrscheinlichkeit	Auswirkungen:		
		gering	mittel	hoch
Unerlaubte Manipulation der Personendaten (Integrität)	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
	Eintretens-wahrscheinlichkeit	Auswirkungen:		
		gering	mittel	hoch
Verlust der Daten / kein Zugriff auf Daten (Verfügbarkeit)	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
	Eintretens-wahrscheinlichkeit	Auswirkungen:		
		gering	mittel	hoch
Unerlaubte Bekanntgabe/Weitergabe der Personendaten im In- und/oder Ausland	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
	Eintretens-wahrscheinlichkeit	Auswirkungen:		
		gering	mittel	hoch
Kompromittierung von Schutzmassnahmen (Bsp. der Verschlüsselung, Anonymisierung, Pseudonymisierung, Passwortweitergabe, Malware etc.)	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
	Eintretens-wahrscheinlichkeit	Auswirkungen:		
		gering	mittel	hoch
Ungenügende oder fehlende Vorgaben für die Benutzenden. Fehlende Sensibilisierung, Schulung und Kontrolle	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐

Fehlende/ungenügende vertragliche Vereinbarungen mit Dienstleistern	**Eintretens-wahrscheinlichkeit**	**Auswirkungen:**		
		gering	mittel	hoch
	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
Weiteres Risiko *(bitte angeben)* : …… …… ……	**Eintretens-wahrscheinlichkeit**	**Auswirkungen:**		
		gering	mittel	hoch
	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
Weiteres Risiko *(bitte angeben)* : …… …… ……	**Eintretens-wahrscheinlichkeit**	**Auswirkungen:**		
		gering	mittel	hoch
	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐

5.2 Verbleibende Restrisiken

Geben Sie die verbleibenden mittleren (gelben) oder hohen (roten) Risiken an, die nach der Umsetzung der Maßnahmen bestehen.

..
..
..
..

6 Entscheid Vorabkonsultation der Ausichtsbehörde

Sollten noch Restrisiken bestehen (Kapitel 5.2), muss der Verantwortliche für die Datenverarbeitung die kantonale Behörde für Öffentlichkeit, Datenschutz und Mediation des Kantons Freiburg konsultieren (Art. 42 DSchG).

Gegebenenfalls wird er der Behörde alle relevanten Unterlagen (Kapitel 7) sowie die vorliegende DSFA übermitteln.

Eine Konsultation der Aufsichtsbehörde ist erforderlich.	NEIN ☐	JA ☐

Datum : Unterschrift :

7 Nachweise und Dokumentationen

Es ist erforderlich, der Aufsichtsbehörde sämtliche Unterlagen vorzulegen, die die organisatorischen, rechtlichen und technischen Maßnahmen beschreiben, die geeignet sind, einen datenschutzkonformen Betrieb zu gewährleisten.

Die erforderlichen Dokumente sind folgende:

- ISDS-Konzept
- Berechtigungskonzept
- Architekturplan
- Datenlebenszyklus inkl. Löschkonzept
- Personalreglement für den Umgang mit Personendaten
- Lieferantenverträge (Dienstleistungsverträge)
- Rechtliche Grundlagen der Datenbearbeitung
- Weitere Dokumente

Anhang 1 : Beispiel Risikobewertung

Ein Risiko wird aus dem Produkt von Eintretenswahrscheinlichkeit und Auswirkung berechnet. **Diese Bewertung kann je nach Art und Umfang der Datenbearbeitung sehr stark variieren. Deshalb ist es wichtig diese Bewertung auf die vorliegende Datenbearbeitung/das vorliegende Projekt jeweils zu überprüfen und gegebenenfalls anzupassen.**

Die Eintretenswahrscheinlichkeit des Auftretens kann in drei Stufen eingeteilt werden: hoch, mittel oder niedrig. Diese können je nach Situation unterschiedlich sein und müssen von Fall zu Fall präzisiert werden. Beispiel zur Bewertung der drei Stufen:

- gering: weniger als einmal alle 10 Jahre.
- Mittel: alle 2 bis 5 Jahre ;
- Hoch: mehrmals pro Jahr ;

Die Auswirkungen können in drei Stufen eingeteilt werden: gering, mittel oder hoch. Dies kann je nach Situation unterschiedlich sein und muss von Fall zu Fall präzisiert werden. Diese Stufen können wie folgt beschrieben werden:

- Gering: vernachlässigbare Auswirkungen auf die Sicherheit und den Datenschutz; kaum wahrnehmbare moralische oder soziale Beeinträchtigungen; mögliche minimale finanzielle Schäden;
- Mittel: Langfristig geringe oder kurzfristig schwerwiegende Auswirkungen auf die Sicherheit und den Datenschutz; geringe psychische, moralische oder soziale Beeinträchtigungen; mögliche finanzielle Schäden ;
- Hoch: Langfristig schwerwiegende Auswirkungen auf die Sicherheit und den Datenschutz; mittelschwerer physischer, psychischer, moralischer oder sozialer Schaden; erheblicher finanzieller Schaden.

Die in der Matrix grün markierten Risiken können als akzeptabel eingestuft werden, d. h. die Restrisiken sind zulässig, ohne dass Massnahmen ergriffen werden müssen. Risiken in Gelb oder Rot müssen als hoch eingestuft werden, und es sind Massnahmen erforderlich, um sie möglichst in den grünen Bereich zu bringen.

Risiko	Auswirkung		
Eintretenswahrscheinlichkeit	gering	mittel	Hoch
hoch			
mittel			
gering			