

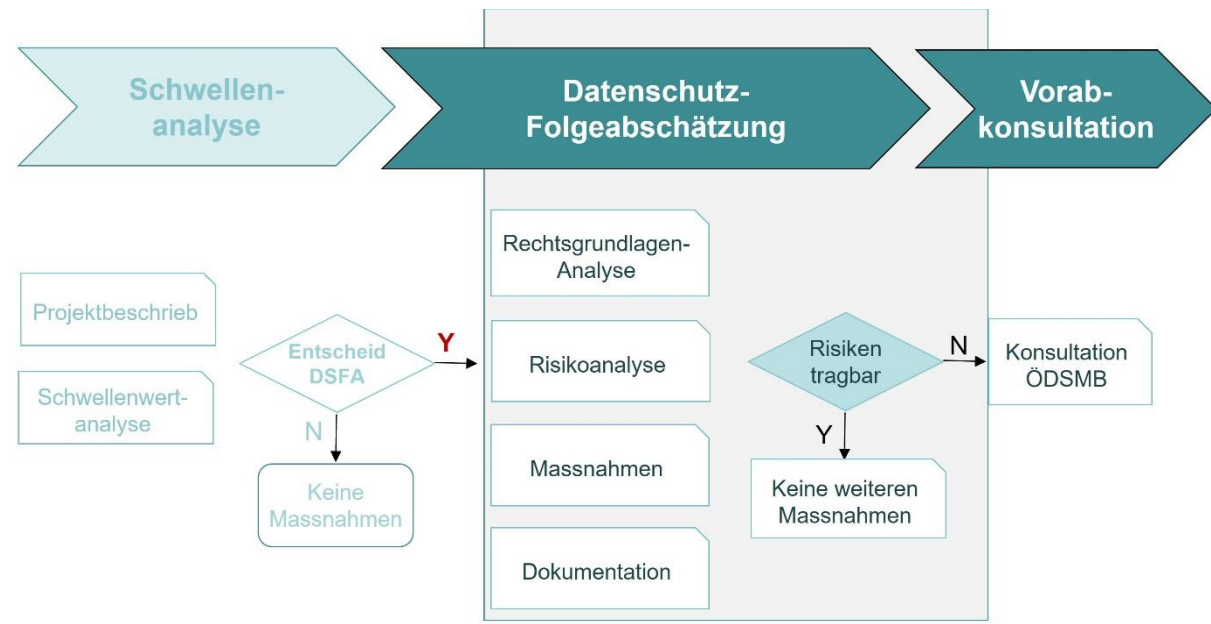


V2.1 vom du 27. August 2024

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 (Teil I der Datenschutz-Folgenabschätzung). Es muss also die eigentliche Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden. Das weitere Vorgehen ist hier schematisch dargestellt:



Die eigentliche DSFA basiert auf der Rechtsgrundlagenanalyse, der Risikoanalyse, dem Massnahmenkatalog und der Analysedokumentation.

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

1.2 Vorgehen

Der Formulareteil 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

3.1 Einschätzung der Hauptrisiken (ohne Massnahmen)

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

Fehlende/ungenügende vertragliche Vereinbarungen mit Dienstleistern	Eintretens- wahrscheinlichkeit	Auswirkungen:		
		gering	mittel	hoch
	hoch	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	mittel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	gering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Weiteres Risiko	Eintretens- wahrscheinlichkeit	Auswirkungen:		
		gering	mittel	hoch
	hoch	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	mittel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	gering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Weiteres Risiko	Eintretens- wahrscheinlichkeit	Auswirkungen:		
		gering	mittel	hoch
	hoch	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	mittel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	gering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.	<input type="checkbox"/>	<input type="checkbox"/>
Eine Sicherheitsorganisation ist etabliert; Verantwortung, Aufgaben und Kompetenzen für den Datenschutz sind definiert und zugewiesen.	<input type="checkbox"/>	<input type="checkbox"/>
Die Sensibilisierung der BenutzerInnen im Umgang mit Personendaten ist in der Organisation vorhanden (Einführung, Schulung).	<input type="checkbox"/>	<input type="checkbox"/>
Die Daten sind klassifiziert (Art. 9 des Reglements über die Personendaten; DSR) und die Dateneigentümer bestimmt.	<input type="checkbox"/>	<input type="checkbox"/>
Die Applikation wird auf einer zertifizierten Umgebung betrieben (Bsp: ISO 27001/2)	<input type="checkbox"/>	<input type="checkbox"/>

4.2 Applikationsspezifische Massnahmen

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

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

5 Risikoeinschätzung nach Umsetzung der Massnahmen

5.1 Einschätzung der Hauptrisiken (mit Massnahmen)

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

Fehlende/ungenügende vertragliche Vereinbarungen mit Dienstleistern	Eintretens- wahrscheinlichkeit	Auswirkungen:		
		gering	mittel	hoch
	hoch	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	mittel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	gering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<hr/>				
Weiteres Risiko (<i>bitte angeben</i>) :	Eintretens- wahrscheinlichkeit	Auswirkungen:		
		gering	mittel	hoch
	hoch	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	mittel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	gering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<hr/>				
Weiteres Risiko (<i>bitte angeben</i>) :	Eintretens- wahrscheinlichkeit	Auswirkungen:		
		gering	mittel	hoch
	hoch	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	mittel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	gering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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 Aufsichtsbehörde

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 (den ersten und zweiten Teil) übermitteln.

Eine Konsultation der Aufsichtsbehörde ist erforderlich.	NEIN <input type="checkbox"/>	JA <input type="checkbox"/>
----------------------------------------------------------	----------------------------------	--------------------------------

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