



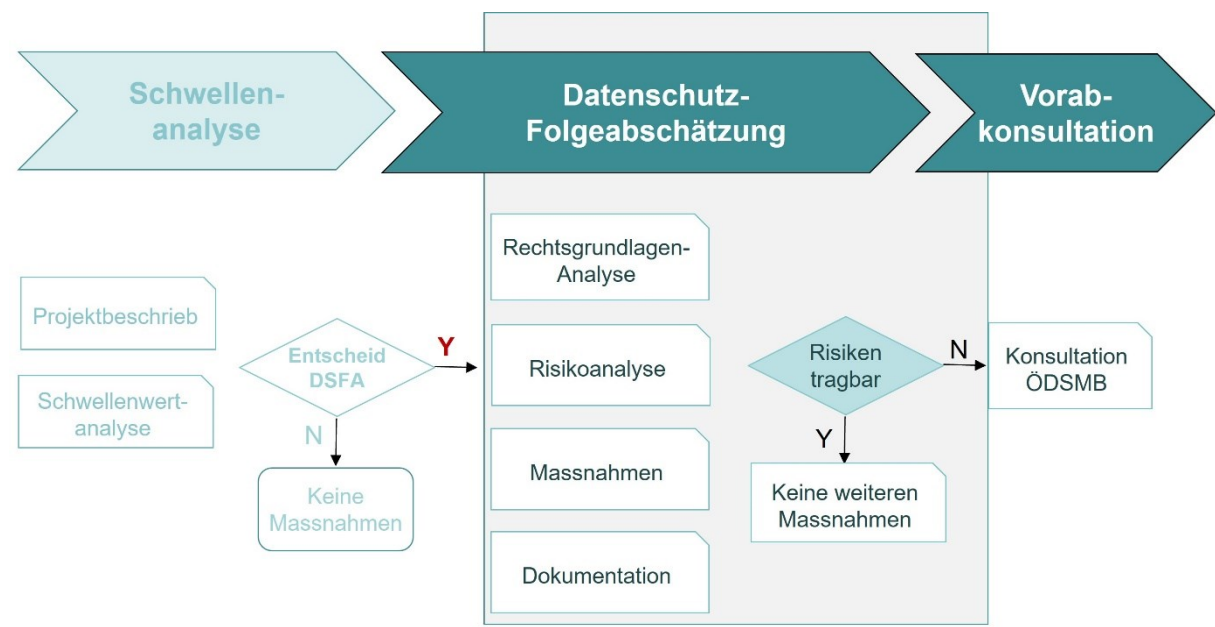
V2 du 26 janvier 2024

1 Datenschutzfolgeabschätzung DSFA

1.1 Ausgangslage

Die Schwellwertanalyse ihrer Datenbearbeitung hat ergeben, dass eine Datenschutzfolgeabschätzung notwendig ist. Das weitere Vorgehen ist hier schematisch dargestellt:

1.2 DSFA-Prozedur



Wie in der Prozedur ersichtlich ist, braucht es dazu:

- Rechtsgrundlagenanalyse
- Risikoanalyse
- Massnahmenkatalog
- Dokumentation

Nutzen sie dazu die Vorlagen in den nachfolgenden Kapiteln.

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 und die Art der Nutzung

- Speicherung: Benennen sie die Speicherung und die Speicherorte

- Aufbewahrung: Benennen sie die gesetzlichen Vorgaben für die Aufbewahrung

- Archivierung: Benennen sie die rechtliche Grundlage für/gegen eine Archivierung

- Löschung: Benennen sie die gesetzlichen Vorgaben für die Datenlöschung

2.3 Verhältnismässigkeit

Beschreiben sie die Verhältnismässigkeit in Bezug auf den Verwendungszweck unter die Prämisse der Datensparsamkeit und Datenvermeidung.

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 / 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 checked="" 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 checked="" type="checkbox"/>

4 Massnahmen zur Risikominimierung

Welche der folgenden Massnahmen¹ sind zur Reduktion der Risiken vorgesehen und werden vor der Betriebsaufnahme umgesetzt?

4.1 Allgemeine Massnahmen für den Grundschutz

	Nein	Ja
Es existiert eine 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 Benutzer im Umgang mit Personendaten ist in der Organisation vorhanden (Einführung, Schulung).	<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

Die Daten sind klassifiziert (Art. 9 des Reglements über die Personendaten; DSR) und die Dateneigentümer bestimmt	<input type="checkbox"/>	<input type="checkbox"/>
Das Berechtigungskonzept ist erstellt und die Grundsätze des «need-to-know»-Ansatzes sind berücksichtigt.	<input type="checkbox"/>	<input type="checkbox"/>
Alle Empfänger 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"/>

¹ Angelehnt an die Norm ISO 27002

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:	<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 / 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	□	□	□
	mittel	□	□	□
	gering	□	□	□
Weiteres Risiko	Eintretens- wahrscheinlichkeit	Auswirkungen:		
		gering	mittel	hoch
	hoch	□	□	□
	mittel	□	□	□
	gering	□	□	□
Weiteres Risiko	Eintretens- wahrscheinlichkeit	Auswirkungen:		
		gering	mittel	hoch
	hoch	□	□	□
	mittel	□	□	□
	gering	□	□	□

5.2 Verbleibende Restrisiken

Risiken aufführen, die in der Bewertung nach der Umsetzung der Massnahmen noch «gelb» oder «rot» sind:

..
..

6 Entscheid Vorabkonsultation

Sollten in Kap. 5.2. Risiken aufgeführt sein, ist eine Vorabkonsultation bei der kantonalen Behörde für Öffentlichkeit, Datenschutz und Mediation des Kanton Freiburg notwendig.

Es braucht eine Vorabkonsultation	NEIN <input type="checkbox"/>	JA <input type="checkbox"/>
-----------------------------------	----------------------------------	--------------------------------

Datum:

Signatur:

7 Nachweise und Dokumentationen

Hier sind die Nachweise und Dokumentationen aufzuführen, welche die organisatorischen, rechtlichen und technischen Massnahmen beschreiben, die einen datenschutzkonformen Betrieb sicherstellen:

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