CANTON DU VALAIS
KANTON WALLIS

Préposé cantonal à la protection des données et à la transparence
Kantonaler Datenschutz- und Öffentlichkeitsbeauftragter
Lauris Loat

Durchführung einer Datenschutz-Folgenabschätzung (DSFA)

Diese Vorlage kann als Grundlage für den Aufbau einer Datenschutz-Folgenabschätzung (nachfolgend: „DSFA“) verwendet werden. Sie wird vom kantonalen Datenschutz- und Öffentlichkeitsbeauftragten ausschliesslich zu Informationszwecken zur Verfügung gestellt.

I. Projektbeschreibung

Allgemeine Informationen

Projektname	**[Name]**	
Bewertung erfolgt durch:	Verantwortliche Person:	**[Name]**
	Externer Berater:	**[Name]**
Dokumentversion	Version XX, [Datum]	

Vorhaben – was ist geplant?

[Beschreibung des Projekts / der Änderung]

Durchführung – wie wird das Projekt / die Änderung durchgeführt?

[Beschreibung der Funktionsweise des Projekts / der Änderung]

Ziel – warum wird das Projekt / die Änderung durchgeführt?

[Beschreibung der Beweggründe für das Projekt / die Änderung]

Zweck - was ist der Zweck der Datenbearbeitung?

[zum Beispiel: Sicherheitsanalyse, Audit, Berichte, Personalverwaltung, usw.]

Avenue de l’Industrie 8, CH-1870 Monthey
Tel +41 (0)27 607 18 70 e-mail: prepose@admin.vs.ch

Auswirkungen auf den Datenschutz – welche potenziellen Auswirkungen hat das Projekt / die Änderung auf die Rechte der betroffenen Personen?

[Welche Auswirkungen wird dieses Projekt / diese Änderung auf die Rechte der betroffenen Personen haben? Beschreiben Sie kurz diese Auswirkungen.]

Beteiligte - wer ist am Projekt / an der Änderung beteiligt?

[Listen Sie die Beteiligten auf, einschliesslich interner Teilnehmer sowie externer Organisationen (öffentlich/privat/ Dritte), die von diesem Projekt / dieser Änderung betroffen sein werden (z.B. durch die Teilnahme an der Entwicklung/Umsetzung oder indem sie durch den Ablauf/Betrieb beeinflusst werden).]

Erforderlichkeit einer DSFA?

[bitte ausfüllen]

Frühere DSFA oder andere Bewertungen, die im Zusammenhang mit dem Schutz von Personendaten im Rahmen dieses Projekts / dieser Änderung bereits durchgeführt wurden?

[Bitte geben Sie die Einzelheiten zu jeder früheren Bewertung an, die sich direkt oder indirekt auf den Datenschutz (inkl. Sicherheit) bezieht und die im Rahmen dieses Projekts durchgeführt wurde. Wenn es sich um eine Änderung eines bestehenden Systems handelt, kann eine Bewertung im Rahmen des Anfangsprojekts durchgeführt worden sein].

II. Rechtsgrundlagenanalyse

Rechtsgrundlagen

Auf welchen Rechtsgrundlagen basiert die Datenbearbeitung?

..

Datenlebenszyklus

Beschreibung des Datenlebenszyklus:

- Erhebung von Personendaten: Angabe der Quellen und Erhebungsformen

..

- Nutzung: Angabe des Benutzerkreises und der Verwendungsart

..

- Speicherung: Angabe der Speicherung und der Speicherorte

..

- Aufbewahrung: Angabe der gesetzlichen Vorgaben für die Aufbewahrung der Daten

..

- Archivierung: Angabe der Rechtsgrundlage für / gegen die Archivierung

..

- Löschung: Angabe der gesetzlichen Vorgaben für die Datenlöschung

..

Verhältnismässigkeit

Beschreibung der Verhältnismässigkeit in Bezug auf den Verwendungszweck unter Berücksichtigung der Grundsätze der Datensparsamkeit und Datenvermeidung.

..

III. Risikobeurteilung aus Sicht des Datenschutzes

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
Datenverlust / kein Zugriff auf Daten (Verfügbarkeit)	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐

	Eintretens-wahrscheinlichkeit	Auswirkungen:		
Unerlaubte Bekanntgabe/Weitergabe der Personendaten im In- und/oder Ausland		gering	mittel	hoch
	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐

	Eintretens-wahrscheinlichkeit	Auswirkungen:		
Kompromittierung von Schutzmassnahmen (Bsp. Verschlüsselung, Anonymisierung/Pseudonymisierung, Passwortweitergabe, Malware usw.)		gering	mittel	hoch
	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐

	Eintretens-wahrscheinlichkeit	Auswirkungen:		
Weitere Risiken		gering	mittel	hoch
	hoch	☒	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐

IV. Massnahmen zur Risikominimierung

Welche der folgenden Massnahmen[1] eignen sich am besten zur Risikominimierung und werden vor der Betriebsaufnahme umgesetzt?

	Nein	Ja
Es existiert ein ISMS (Information Security Management System). Die Datenbearbeitung wird darin eingebunden.	☐	☐
Eine Sicherheitsorganisation ist eingerichtet ; Verantwortung, Aufgaben und Kompetenzen für den Datenschutz sind definiert und zugewiesen.	☐	☐
Die Sensibilisierung der Benutzer im Umgang mit Personendaten ist in der Organisation vorhanden (Einführung, Schulung).	☐	☐
Die Daten sind klassifiziert und die Dateneigentümer bestimmt.	☐	☐
Das Berechtigungskonzept ist erstellt und die Grundsätze des «need-to-know»-Ansatzes sind berücksichtigt.	☐	☐
Alle interne/externe Empfänger von Personendaten 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).	☐	☐

[1] Basierend auf der Norm ISO 27002

Die nötigen kryptografischen Massnahmen (Verschlüsselung) für den Schutz von Personendaten sind akkurat eingesetzt.	☐	☐
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 gespeichert (Backup & Restore).	☐	☐
Ein angemessener Schutz gegen Malware ist vorhanden.	☐	☐
Die Datenzugriffe werden protokolliert und überprüft.	☐	☐
Die Sicherheitsupdates werden nach getesteten Verfahren zeitnah installiert.	☐	☐
Die Netzwerkssicherheit ist gewährleistet.	☐	☐
Die Kommunikationskanäle sind definiert und entsprechen den Datenschutzanforderungen.	☐	☐
Die Lieferanten sind verpflichtet, die Datenschutzanforderungen einzuhalten (Verträge, SLA).	☐	☐
Die Sicherheitsmassnahmen werden periodisch überprüft und angepasst.	☐	☐
Weitere Massnahmen:	☐	☐

V. Risikoeinschätzung nach Umsetzung der Massnahmen

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
Datenverlust / kein Zugriff auf Daten (Verfügbarkeit)	hoch	☐	☐	☐

	mittel	☐	☐	☐
	gering	☐	☐	☐
Unerlaubte Bekanntgabe/Weitergabe der Personendaten im In- und/oder Ausland	**Eintretens-wahrscheinlichkeit**	**Auswirkungen:**		
		gering	mittel	hoch
	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
Kompromittierung von Schutzmassnahmen (Bsp. Verschlüsselung, Anonymisierung/Pseudonymisierung, Passwortweitergabe, Malware usw.)	**Eintretens-wahrscheinlichkeit**	**Auswirkungen:**		
		gering	mittel	hoch
	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐
Weitere Risiken	**Eintretens-wahrscheinlichkeit**	**Auswirkungen:**		
		gering	mittel	hoch
	hoch	☐	☐	☐
	mittel	☐	☐	☐
	gering	☐	☐	☐

Restrisiken

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

..
..

VI. Entscheid Vorabkonsultation

Sollten Restrisiken im vorherigen Kapitel aufgeführt sein, ist eine Vorabkonsultation des Walliser Datenschutz- und Öffentlichkeitsbeauftragten erforderlich.

Ein Vorabkonsultation ist erforderlich	NEIN ☐	JA ☐

Datum: Namen des Unterzeichners: Unterschrift:

Nachweise und Dokumentation

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

[Beispiele

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