# Datenschutzfolgeabschätzung DSFA

## Ausgangslage

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

## DSFA-Prozedur



Wie in der Prozedur ersichtlich ist, braucht es dazu:

Rechtsgrundlagenanalyse

Risikoanalyse

Massnahmenkatalog

Dokumentation

Nutzen sie dazu die Vorlagen in den nachfolgenden Kapiteln.

# Rechtsgrundlagenanalyse

## Rechtsgrundlagen

Auf welchen Rechtsgrundlagen basiert die Datenbearbeitung?

|  |
| --- |
| .. |

## 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

|  |
| --- |
| .. |

## Verhältnismässigkeit

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

|  |
| --- |
| .. |

# Risikobeurteilung aus Sicht des Datenschutzes

## Einschätzung der Hauptrisiken (ohne Massnahmen)

|  |  |  |
| --- | --- | --- |
| Unerlaubte Zugriffe auf Personendaten (Vertraulichkeit) | **Eintretens-wahrscheinlichkeit** | **Auswirkungen:** |
| gering | mittel | hoch |
| hoch | [ ]  | [ ]  | [ ]  |
| mittel | [ ]  | [ ]  | [ ]  |
| gering | [ ]  | [ ]  | [ ]  |
|   |  |   |   |   |
| Unerlaubte Manipulation der Personendaten (Integrität) | **Eintretens-wahrscheinlichkeit** | **Auswirkungen:** |
| gering | mittel | hoch |
| hoch | [ ]  | [ ]  | [ ]  |
| mittel | [ ]  | [ ]  | [ ]  |
| gering | [ ]  | [ ]  | [ ]  |
|   |  |   |   |   |
| Verlust der Daten / kein Zugriff auf Daten (Verfügbarkeit) | **Eintretens-wahrscheinlichkeit** | **Auswirkungen:** |
| gering | mittel | hoch |
| 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. der Verschlüsselung, Anonymisierung/Pseudonymisierung, Passwortweitergabe, Malware etc.) | **Eintretens-wahrscheinlichkeit** | **Auswirkungen:** |
| gering | mittel | hoch |
| hoch | [ ]  | [ ]  | [ ]  |
| mittel | [ ]  | [ ]  | [ ]  |
| gering | [ ]  | [ ]  | [ ]  |
|   |  |   |   |   |
| Ungenügende oder fehlende Vorgaben für die Benutzenden. Fehlende Sensibilisierung / Schulung / Kontrolle | **Eintretens-wahrscheinlichkeit** | **Auswirkungen:** |
| gering | mittel | hoch |
| 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 | [ ]  | [ ]  | [x]  |
|  |
| Weiteres Risiko | **Eintretens-wahrscheinlichkeit** | **Auswirkungen:** |
| gering | mittel | hoch |
| hoch | [ ]  | [ ]  | [ ]  |
| mittel | [ ]  | [ ]  | [ ]  |
| gering | [ ]  | [ ]  | [x]  |

# Massnahmen zur Risikominimierung

Welche der folgenden Massnahmen[[1]](#footnote-1) sind zur Reduktion der Risiken vorgesehen und werden vor der Betriebsaufnahme umgesetzt?

## Allgemeine Massnahmen für den Grundschutz

|  |  |  |
| --- | --- | --- |
| Es existiert eine ISMS (Information Security Management System). Die Datenbearbeitung wird darin eingebunden. | **Nein**[ ]  | **Ja**[ ]  |
| Eine Sicherheitsorganisation ist etabliert; 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 Applikation wird auf einer zertifizierten Umgebung betrieben (Bsp: ISO 27001/2) |[ ] [ ]

## Applikationsspezifische Massnahmen

|  |  |  |
| --- | --- | --- |
| Die Daten sind klassifiziert (Art. 9 des Reglements über die Personendaten; DSR) und die Dateneigentümer bestimmt | [ ]  | [ ]  |
| Das Berechtigungskonzept ist erstellt und die Grundsätze des «need-to-know»-Ansatzes sind berücksichtigt. |[ ] [ ]
| Alle Empfänger 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: |[ ] [ ]

# Risikoeinschätzung nach Umsetzung der Massnahmen

## Einschätzung der Hauptrisiken (mit Massnahmen)

|  |  |  |
| --- | --- | --- |
| Unerlaubte Zugriffe auf Personendaten (Vertraulichkeit) | **Eintretens-wahrscheinlichkeit** | **Auswirkungen:** |
| gering | mittel | hoch |
| hoch | [ ]  | [ ]  | [ ]  |
| mittel | [ ]  | [ ]  | [ ]  |
| gering | [ ]  | [ ]  | [ ]  |
|   |  |   |   |   |
| Unerlaubte Manipulation der Personendaten (Integrität) | **Eintretens-wahrscheinlichkeit** | **Auswirkungen:** |
| gering | mittel | hoch |
| hoch | [ ]  | [ ]  | [ ]  |
| mittel | [ ]  | [ ]  | [ ]  |
| gering | [ ]  | [ ]  | [ ]  |
|   |  |   |   |   |
| Verlust der Daten / kein Zugriff auf Daten (Verfügbarkeit) | **Eintretens-wahrscheinlichkeit** | **Auswirkungen:** |
| gering | mittel | hoch |
| 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. der Verschlüsselung, Anonymisierung/Pseudonymisierung, Passwortweitergabe, Malware etc.) | **Eintretens-wahrscheinlichkeit** | **Auswirkungen:** |
| gering | mittel | hoch |
| hoch | [ ]  | [ ]  | [ ]  |
| mittel | [ ]  | [ ]  | [ ]  |
| gering | [ ]  | [ ]  | [ ]  |
|   |  |   |   |   |
| Ungenügende oder fehlende Vorgaben für die Benutzenden. Fehlende Sensibilisierung / Schulung / Kontrolle | **Eintretens-wahrscheinlichkeit** | **Auswirkungen:** |
| gering | mittel | hoch |
| 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 | [ ]  | [ ]  | [ ]  |

## Verbleibende Restrisiken

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

|  |
| --- |
| .. |
| .. |
|  |
|  |
|  |

# 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[ ]  | JA[ ]  |

Datum: Signatur:

# 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
1. Angelehnt an die Norm ISO 27002 [↑](#footnote-ref-1)