|  |  |
| --- | --- |
|  | Wenn ausgefüllt mindestens: INTERN |

|  |
| --- |
|  |

Bearbeitungsreglement

< Projektname / Schutzobjektname >

|  |
| --- |
|  |

|  |  |
| --- | --- |
| Klassifizierung | **INTERN** / VERTRAULICH / GEHEIM |
| Status | **in Arbeit** / in Prüfung / genehmigt zur Nutzung |
| Projektnummer | Nr. |
| Projektleiter (PL LB) | PL LB |
| Version | Aus Template V2.1 - P042-Hi04 - Bearbeitungsreglement |
| Datum |  |
| Auftraggeber | Auftraggeber |
| Autor/Autoren | Autor |

Änderungskontrolle

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Beschreibung, Bemerkung | Name |
| 0.1 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Verteiler

|  |  |  |
| --- | --- | --- |
| Funktion | Name  | Departement / Amt |
| DSB |  |  |
| ISBO |  |  |
|  |  |  |
|  |  |  |

Inhaltsverzeichnis

1 Generelles 4

1.1 Beschreibung 4

1.2 Zweck des Bearbeitungsreglement von Bundesorganen 4

1.3 Tailoring 5

1.4 Hilfsmittel 5

1.5 Genehmigung 6

2 Bearbeitungsreglement von Bundesorganen 7

2.1 Allgemeines 7

2.1.1 Gesetzliche Grundlagen 7

2.1.2 Zweck der Datenbearbeitung 8

2.1.3 Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten 8

2.2 Interne Organisation 8

2.2.1 Verantwortliches Bundesorgan 8

2.2.2 Auftragsbearbeiter 9

2.2.3 Benutzer und Datenzugriff 9

2.2.3.1 Benutzerkreis 9

2.2.3.2 Zugriffsberechtigungen 10

2.2.3.3 Rollen 10

2.2.3.4 Prozess Zugriffsberechtigung 10

2.3 Datenbearbeitungs- und Kontrollverfahren 11

2.3.1 Bearbeitung der Personendaten 11

2.3.1.1 Geschäftsprozesse 11

2.3.1.2 Datenbekanntgabe und Schnittstellen 11

2.3.1.3 Kontrolle der erfassten Personendaten 12

2.3.1.4 Prozesse / Datenverarbeitungsverfahren 12

2.3.2 Aufbewahrungsdauer, Archivierung und Löschung 12

2.3.2.1 Aufbewahrungsdauer 12

2.3.2.2 Archivierung 12

2.3.2.3 Löschung 12

2.3.3 Rechte der betroffenen Personen 13

2.4 Massnahmen zur Gewährleistung der Datensicherheit 13

3 Anhang 14

3.1 Verzeichnis der Bearbeitungstätigkeiten 14

3.2 Datenschutz-Folgenabschätzung 15

3.3 Berechtigungskonzept / Berechtigungsmatrix 15

3.4 Dokumentenverzeichnis 17

3.5 Abkürzungen 18

3.6 Begriffe 19

# Generelles

## Beschreibung

Beschreibung der automatisierten Bearbeitung des IKT-Vorhabens.

## Zweck des Bearbeitungsreglement von Bundesorganen

Grundlage des Bearbeitungsreglements - im Rahmen von IKT-Vorhaben der Bundesverwaltung - ist das ISDS-Konzept.

Das **verantwortliche Bundesorgan und sein Auftragsbearbeiter** (siehe Art. 6 DSV) erstellen ein Bearbeitungsreglement für automatisierte Bearbeitungen, wenn sie:

* besonders schützenswerte Personendaten bearbeiten;
* ein Profiling durchführen;
* nach Artikel 34 Absatz 2 Buchstabe c DSG[[1]](#footnote-1) Personendaten bearbeiten;
* Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen Personendaten zugänglich machen;
* Datenbestände miteinander verknüpfen; oder
* mit anderen Bundesorganen zusammen ein Informationssystem betreiben oder Datenbestände bewirtschaften.

Der **EDÖB** muss für sämtliche automatisierte Bearbeitungen ein Bearbeitungsreglement erstellen (Art. 40 DSV).

Das Reglement muss insbesondere Angaben

* zur internen Organisation,
* zum Datenbearbeitungs- und Kontrollverfahren sowie
* zu den Massnahmen zur Gewährleistung der Datensicherheit

enthalten.

Es enthält die Auflistung aller Unterlagen über die Planung, die Realisierung und den Betrieb der Datensammlung. Das Verzeichnis der Bearbeitungstätigkeiten (gemäss Art. 12 DSG), eine erstellte Datenschutz-Folgenabschätzung (DSFA, gemäss Art. 22 DSG) und ein allfälliges ISDS-Konzept sind dem Bearbeitungsreglement als Anhang beizufügen.

Das Bearbeitungsreglement soll für die notwendige Transparenz im Rahmen der Systementwicklung, -adaption wie auch der elektronischen Bearbeitung von Personendaten im Rahmen einer automatisierten Bearbeitung sorgen.

Die erste Version des Bearbeitungsreglements ist zum Ende der HERMES Phase Konzept verfügbar.

Das verantwortliche Bundesorgan und sein Auftragsbearbeiter müssen das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater zur Verfügung stellen.

## Tailoring

Das Bearbeitungsreglement ist in möglichst kurzer und verständlicher Form zu führen, so dass die Beschreibung der automatisierten Datensammlung auch von Nicht-Experten verstanden bzw. beurteilt werden kann (Grundsatz).

Je umfangreicher oder sensitiver die vorgesehene Bearbeitung von Personendaten jedoch ist, umso ausführlicher ist auch das Bearbeitungsreglement zu erstellen. Die wichtigsten Aspekte aus Sicht Datenschutz und Informationssicherheit - sofern nicht bereits im Verzeichnis der Bearbeitungstätigkeiten, in der DSFA und im ISDS-Konzept enthalten - müssen im Bearbeitungsreglement beschrieben sein. Für detailliertere Informationen ist auf weiterführende Dokumente zu verweisen.

Wichtig ist, dass Inhalte von bestehenden Dokumenten nicht kopiert werden, sondern auf diese mit präzisen Angaben verwiesen wird und diese Dokumente beigelegt werden. Das Bearbeitungsreglement soll keine Abschreib- und Kopierübung sein.

Der blaue Text dient als Hilfe zum Ausfüllen des Dokumentes.

## Hilfsmittel

Für die Erarbeitung des Bearbeitungsreglements dienen folgende Hilfsmittel:

**Hilfsmittel:**

* [Vorgaben zu Sicherheitsverfahren und dazugehörige Hilfsmittel auf Stufe Bund des Delegierten des Bundes für Cybersicherheit, NCSC](https://intranet.ncsc.admin.ch/ncscintra/de/home/vorgaben-hilfsmittel/sicherheitsverfahren.html)
* [Legistische Hauptinstrumente, BJ](https://www.bj.admin.ch/bj/de/home/staat/legistik/hauptinstrumente.html)
* [Totalrevision des Datenschutzgesetzes (DSG) - Übersicht zu den wichtigsten Änderungen für die Erarbeitung der Rechtsgrundlagen betreffend Datenbearbeitungen durch Bundesorgane, BJ](https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/dsg-uebersicht-aenderungen.pdf.download.pdf/dsg-uebersicht-aenderungen-d.pdf)
* [Gesetzgebungsleitfaden Datenschutz, BJ](https://www.bj.admin.ch/dam/bj/de/data/staat/legistik/hauptinstrumente/leitfaden-datenschutz.pdf.download.pdf/leitfaden-datenschutz-d.pdf)
* Technische und organisatorische Massnahmen (TOM) (in der Infothek Datenschutz des EDÖB)

## Genehmigung

Die Unterschriften zur Genehmigung müssen vor der Betriebsaufnahme geleistet werden.

Mit seiner Unterschrift bestätigt der Datenschutzberater das Bearbeitungsreglement geprüft zu haben. Sie oder er haben insbesondere geprüft ob das Dokument vollständig ausgefüllt ist und alle geforderten Massnahmen dokumentiert sind. Sie oder er hat die Angaben kritisch hinterfragt, ob sie konsistent sind und im Kontext der Bearbeitung der Daten stimmen.

Der Verantwortliche genehmigt mit seiner Unterschrift das Bearbeitungsreglement.

|  |  |
| --- | --- |
| Datum / Name / Unterschrift **Datenschutzberater**: | …………………………………………………...…... |
| Datum / Name / Unterschrift **Verantwortlicher**:  | …………………………………………………...…... |
|  |  |

Weitere Unterschriften können hinzugefügt werden.

Die Unterschriften können auch in elektronischer Form (in einem PDF) angebracht werden.

# Bearbeitungsreglement von Bundesorganen

## Allgemeines

### Gesetzliche Grundlagen

Dieser Abschnitt hält die gesetzlichen Grundlagen fest, auf die sich die Bearbeitung der Personendaten in der Datensammlung gemäss DSG stützt:

**Art. 34 DSG** Rechtsgrundlagen

1 Bundesorgane dürfen Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht.

2 Eine Grundlage in einem Gesetz im formellen Sinn ist in folgenden Fällen erforderlich:

a. Es handelt sich um die Bearbeitung von besonders schützenswerten Personendaten.

b. Es handelt sich um ein Profiling.

c. Der Bearbeitungszweck oder die Art und Weise der Datenbearbeitung können zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person führen.

3 Für die Bearbeitung von Personendaten nach Absatz 2 Buchstaben a und b ist eine Grundlage in einem Gesetz im materiellen Sinn ausreichend, wenn die folgenden Voraussetzungen erfüllt sind:

a. Die Bearbeitung ist für eine in einem Gesetz im formellen Sinn festgelegte Aufgabe unentbehrlich.

b. Der Bearbeitungszweck birgt für die Grundrechte der betroffenen Person keine besonderen Risiken.

4 In Abweichung von den Absätzen 1–3 dürfen Bundesorgane Personendaten bearbeiten, wenn eine der folgenden Voraussetzungen erfüllt ist:

a. Der Bundesrat hat die Bearbeitung bewilligt, weil er die Rechte der betroffenen Person für nicht gefährdet hält.

b. Die betroffene Person hat im Einzelfall in die Bearbeitung eingewilligt oder hat ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt.

c. Die Bearbeitung ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen.

Wird die Bearbeitung von Personendaten durch Vertrag (z.B. Outsourcing-Vertrag) oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen, so müssen nach Art. 9 Abs. 1 DSG folgende Voraussetzungen erfüllt sein:

* die Daten werden nur so bearbeitet, wie der Verantwortliche (das Amt, die Organisationseinheit) selbst es tun dürfte;
* keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

Der Verantwortliche (bzw. das verantwortliche Bundesorgan) muss sich insbesondere vergewissern, dass der Auftragsbearbeiter die Datensicherheit gewährleistet (Art. 9 Abs. 2 DSG).

**Art. 36, Abs. 5 DSG** sehen vor:

Bundesorgane dürfen Personendaten mittels automatisierter Informations- und Kommunikationsdienste allgemein zugänglich machen, wenn eine Rechtsgrundlage die Veröffentlichung dieser Daten vorsieht oder wenn sie gestützt auf Absatz 3 Informationen der Öffentlichkeit zugänglich machen. Besteht das öffentliche Interesse an der Zugänglichmachung nicht mehr, so sind die betreffenden Daten wieder aus dem automatisierten Informations- und Kommunikationsdienst zu entfernen.

### Zweck der Datenbearbeitung

(Grundlagen: DSG Art. 6 Abs. 3 i.V.m DSV Art. 1 Abs. 2 lit. b, DSG Art. 6 Abs. 4 – 5, Art. 7 Abs. 3, Art. 12 Abs. 2)

Zweck, Art, Umfang und Umstände der Bearbeitung sind zu umschreiben.

Bei der Ausgangslage soll man kurz festhalten, warum man ein System gestalten will, den Zweck (Zwecke) sowie den gewünschten Soll-Zustand umschreiben.

### Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten

(Grundlagen: DSG Art. 6 Abs. 6, 7, Art. 12 Abs. 2, Art. 19, DSV Art. 1 Abs. 2 lit. a, Art. 13)

Zum Inhalt der bearbeiteten Daten sind folgende Fragen zu beantworten:

* Welche Art von Personendaten werden bearbeitet (Personendaten, besonders schützenswerte Personendaten, Persönlichkeitsprofile, andere)?
* Welche Art, Kategorien (bzw. „Gruppen“) und Anzahl von Personen und Personendaten werden bearbeitet?
* Wie wurden die Personendaten beschafft

## Interne Organisation

(Grundlagen: DSG Art. 9, 10, 12, 13, 33; DSV Art. 7, 8, 17, 23, 25)

### Verantwortliches Bundesorgan

Aufführen des Organigramms des für die Datenbearbeitung verantwortlichen Bundesorgans und der Bereiche (inkl. Anzahl Mitarbeitende), die mit den Daten arbeiten. Insbesondere sind Verantwortlicher, Anwendungsverantwortlicher, Datenschutzberater und ISBO namentlich aufzulisten.

Angabe der Kontrollverfahren und die Verantwortung für den Datenschutz, wenn ein Bundesorgan Personendaten zusammen mit anderen Bundesorganen, mit kantonalen Organen oder mit privaten Personen bearbeitet.

Sofern nicht bereits im ISDS-Konzept aufgeführt und dieses beigelegt ist, ist auch festzuhalten, wer für die Anwendung, Netzwerk, Datenbank, Betriebssystem, usw., in welcher die Daten enthalten sind bzw. auf welcher diese laufen, verantwortlich ist.

Angaben über:

Verantwortliches Bundesorgan:

Nutzende DataReg:

Anwendungsverantwortliche Person:

Datenschutzberatende Person:

ISBO:

Verantwortlicher Anwendung:

Verantwortlicher Netzwerk:

Verantwortlicher Datenbank:

Verantwortlicher Betriebssystem:

### Auftragsbearbeiter

Der zuständige Auftragsbearbeiter und die verantwortlichen Ansprechpersonen sind aufzuführen.

Angaben über:

Auftragsbearbeiter:

Ansprechperson LE/Auftragsbearbeiter:

### Benutzer und Datenzugriff

#### Benutzerkreis

Die Kategorien (bzw. „Gruppen“) aller zugriffsberechtigten Organisationseinheiten bzw. Stellen (Organe des Bundes, Kantonale Organe, Dritte) sind aufzuführen und es ist kurz zu umschreiben, für welche gesetzlichen Aufgaben sie einen Zugriff auf die Datensammlung benötigen.

Allenfalls hier einen Verweis auf die Kommunikationsmatrix aus dem ISDS-Konzept machen.

Nachstehend ein **Beispiel** einer möglichen Darstellung.

Skizze

Umsysteme

| **Name** | **Beschreibung** | **Verwendung** |
| --- | --- | --- |
| eIAM | Zentrales Identity und Access Management System von der Bundesverwaltung.  | Wird für die Benutzer-Authentisierung und die Grob-Autorisierung (Rollenzuweisung) verwendet. |
|  |  |  |
|  |  |  |

**eIAM / Keycloak**

eIAM ist das zentrale Identity & Access Management System der Bundesverwaltung. Verantwortet durch die Bundeskanzlei und Betrieben durch das BIT (siehe <https://www.eiam.admin.ch/> ).

#### Zugriffsberechtigungen

Art und Umfang des Zugriffs der Benutzer der Datensammlung sowie die Datenfelder sind aufzuführen bzw. kurz zu umschreiben. Falls bereits eine Berechtigungsmatrix (bzw. Berechtigungskonzept) existiert, ist diese in den Anhang des Bearbeitungsreglements aufzunehmen.

#### Rollen

Welche Rollen von Zugriffsberechtigungen gibt es (z.B. Sachbearbeiter, Administrator) und welchen Zugriffsumfang beinhaltet die einzelne Rolle (Abfragen, Bearbeiten, Drucken, kein Zugriff, andere)?

Nachstehend ein **Beispiel** einer möglichen Darstellung.

| **Name** | **Beschreibung** |
| --- | --- |
| Sachbearbeiter |  |
| Anwendungsverantwortlicher |  |
| Administrator |  |
| … |  |

#### Prozess Zugriffsberechtigung

Hier sind die Modalitäten (Prozess und Verantwortlichkeiten) für die Erteilung und Entzug der Zugriffsberechtigungen zu beschreiben. Folgende Fragen sind zu beantworten:

* Wer ist verantwortlich für die Erteilung und den Entzug der Zugriffsberechtigung?
* Wer überprüft regelmässig die erteilten Zugriffsberechtigungen und aktualisiert diese?
* Umfang der Zugriffsberechtigung?
* Prozess für die Erteilung und den Entzug der Zugriffsberechtigungen vorhanden?
* Ablauf des Prozesses?
* Zentral gesteuert?

## Datenbearbeitungs- und Kontrollverfahren

(Grundlagen: DSG Art. 6 - 10, 12, 13, 16, 19, 21, 22, 24, 25, 28, 33, 36, 37, 41, 42; DSV Art. 1 - 4, 6, 9 - 13, 15 - 18, 20, 22, 26, 29, 30)

Themen sind

Vernichtung sobald zum Zweck der Bearbeitung nicht mehr erforderlich.

Massnahmen zur Berichtigung der Personendaten.

Einwilligung zur Bearbeitung von Personendaten.

Datenschutz durch Technik und datenschutzfreundlicher Voreinstellungen.

Datensicherheitsmassnahmen.

Umgang mit Auftragsbearbeiter.

Einbezug Datenschutzberatende.

Verzeichnis Bearbeitungstätigkeiten führen.

Verwendung von Zertifizierungen.

Voraussetzungen für legale Bekanntgabe von Personendaten ins Ausland.

Informationspflicht bei der Beschaffung von Personendaten.

Informationspflicht bei automatisierten Einzelentscheidungen.

Datenschutz-Folgenabschätzung.

Meldung von Verletzungen der Datensicherheit.

Ausgestaltung Auskunftsrecht.

Recht auf Datenherausgabe oder -übertragung.

Kontrolle und Verantwortung bei gemeinsamer Bearbeitung von Personendaten.

Bekanntgabe von Personendaten.

Widerspruch gegen die Bekanntgaben von Personendaten durch ein Bundesorgan.

Weitere Ansprüche und Verfahren einer Person an ein Bundesorgan.

Bekanntgabe von amtlichen Dokumenten mit Personendaten

### Bearbeitung der Personendaten

#### Geschäftsprozesse

Hier sind die aus Sicht Datenschutz wichtigsten Geschäftsprozesse der Datensammlung zu dokumentieren und/oder grafisch darzustellen.

#### Datenbekanntgabe und Schnittstellen

Grafische Übersicht der Schnittstellen zu anderen Schutzobjekten wie Systemen, Applikationen, Anwendungen, usw. sind hier abzubilden. Es kann auch auf das ISDS-Konzept verwiesen werden, sollte dort eine entsprechende Übersicht bereits bestehen.

Die Schnittstellenbeschreibung sollte folgende Angaben zur Datenweitergabe (Bekanntgabe) enthalten:

* von wem stammen die Personendaten?
* wer erhält die Personendaten?
* zu welchem Zweck werden die Personendaten weitergegeben?
* welche Kategorien (bzw. „Gruppen“) von Personendaten werden weitergegeben?
* in welcher Periodizität werden die Personendaten weitergegeben?
* von wem wurde die Weitergabe initiiert?
* mit Hilfe welchen Mediums werden die Personendaten weitergegeben?

Die Zwecke, für welche die Personendaten regelmässig bekannt gegeben werden sollten aus der Schnittstellenbeschreibung ersichtlich sein.

#### Kontrolle der erfassten Personendaten

Wer kontrolliert die Richtigkeit der Personendaten? Ist ein entsprechender Prozess vorhanden? Existiert eine regelmässige Prüfung und Korrektur dieser Daten?

#### Prozesse / Datenverarbeitungsverfahren

Die Prozesse für Berichtigung, Sperrung, Anonymisierung, Speicherung, Aufbewahrung, Archivierung und Vernichtung der Daten sind zu definieren und zu beschreiben.

### Aufbewahrungsdauer, Archivierung und Löschung

#### Aufbewahrungsdauer

Folgende Fragen sind zu klären:

* Wie lange dürfen bzw. müssen die erfassten Personendaten bzw. Kategorien („Gruppen“) von Personendaten aufbewahrt werden?
* Ort und Verantwortlichkeiten der Aufbewahrung der Personendaten?
* Zu welchem Zeitpunkt werden diese gelöscht oder sollen sie ans Bundesarchiv abgeliefert werden?

#### Archivierung

Die organisatorischen und technischen Modalitäten (Dateiformate, Schnittstellen) zum Anbieten bzw. der Abgabe der Personendaten ans Bundesarchiv sind hier festzuhalten.

#### Löschung

Zu welchem Zeitpunkt werden nicht mehr benötigte Personendaten in der Datensammlung gelöscht? Diese Formulierung ist mit dem ISBO und dem Anwendungsverantwortlichen entsprechend abzustimmen.

### Rechte der betroffenen Personen

Es ist insbesondere festzuhalten, an wen sich die betroffene Person wenden soll (Ansprechperson/Adressat), und wie das interne Verfahren (Prozess) abläuft.

Die Instrumente und Verfahren für die Ausübung des Auskunftsrechts, Datenherausgabe oder -übertragungsrechts, Berichtigungs-, Vernichtungs- und Sperrungsrechts sowie das Recht auf die Anbringung eines Bestreitungsvermerks müssen geschaffen werden. Instrumente für die Sperrung der Bekanntgabe an Dritte müssen bestehen und umgesetzt werden können.

Die Informationspflicht beim Beschaffen von Personendaten durch Bundesorgane ist entsprechend zu berücksichtigen und zu regeln.

## Massnahmen zur Gewährleistung der Datensicherheit

(Grundlagen: DSG Art. 7, 8, 10, 12, 13, 22, 24, 33; DSV Art. 1 - 4, 6, 15, 25 - 27)

Hier sind diejenigen technischen und organisatorischen Massnahmen aufzuführen, welche einen angemessenen Datenschutz gewährleisten und nicht bereits im ISDS-Konzept enthalten sind.

Skizze

# Anhang

## Verzeichnis der Bearbeitungstätigkeiten

Die Verantwortlichen und Auftragsbearbeiter führen je ein Verzeichnis ihrer Bearbeitungstätigkeiten (Artikel 12 DSG).

Das Verzeichnis des Verantwortlichen enthält mindestens:

* die Identität des Verantwortlichen;
* den Bearbeitungszweck;
* eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;
* die Kategorien der Empfängerinnen und Empfänger;
* wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;
* wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 8 DSG;
* falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien nach Artikel 16 Absatz 2 DSG.

Das Verzeichnis des Auftragsbearbeiters enthält Angaben zur Identität des Auftragsbearbeiters und des Verantwortlichen, zu den Kategorien von Bearbeitungen, die im Auftrag des Verantwortlichen durchgeführt werden, sowie mindestens

* wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 8 DSG;
* falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien nach Artikel 16 Absatz 2 DSG.

Die Meldung der Verzeichnisse ist für alle Bundesorgane zwingend (Art. 12 Abs. 4 DSG) und erfolgt ebenfalls, wie die erste Version des Bearbeitungsreglements, zum Ende der Phase Konzept (Artikel 31 Absatz 2 DSV).

Die Bundesorgane sind verpflichtet, diese Angaben laufend zu aktualisieren und ihre Verzeihnisse dem EDÖB zu melden. Die entsprechende Meldung erfolgt über die Web-Anwendung „[DataReg](http://www.edoeb.admin.ch/dienstleistungen/00587/00966/index.html?lang=de)“ des EDÖB.

Eine Kopie der Meldung der Verzeichnisse beim EDÖB ist dem Bearbeitungsreglement beizulegen.

## Datenschutz-Folgenabschätzung

Der Verantwortliche muss unter bestimmten Bedingungen eine Datenschutz-Folgenabschätzung (Artikel 22 DSG) erstellen.

Die Datenschutz-Folgenabschätzung enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte.

Beim Vorliegen einer solchen ist eine Kopie derselben dem Bearbeitungsreglement beizulegen.

## Berechtigungskonzept / Berechtigungsmatrix

Das Berechtigungskonzept bzw. die Berechtigungsmatrix ist als Anhang dem Bearbeitungsreglement beizufügen.

Nachstehend ein vereinfachtes **Beispiel** einer Berechtigungsmatrix.

|  |  |  |  |
| --- | --- | --- | --- |
| Datenfeldnamen | Bund | Kanton | Dritte |
|  | VE I | VE II | VE III | … | … | … | Kant. Amt | … | … | … | … | … | … | … |
|  |
| I. Stammdaten |
| Name(n) | A | A | B | … | … | … | A | … | … | … | … | … | … | … |
| Vorname(n) | A | A | B | … | … | … | A | … | … | … | … | … | … | … |
| Geburtsdatum |  | A | A | … | … | … | A | … | … | … | … | … | … | … |
| Staatsangehörigkeit |  | A | A | … | … | … | B | … | … | … | … | … | … | … |
| … | … | … | … | … | … | … | … | … | … | … | … | … | … | … |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| II. Dossierinformationen |
| Dossierinhaber | B | B | B | … | … | … | A | … | … | … | … | … | … | … |
| Dossierstatus | B | B | B | … | … | … |  | … | … | … | … | … | … | … |
| Referenznummer | A | B | B | … | … | … | B | … | … | … | … | … | … | … |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| III. Titel X |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Zugriffsstufen**

A = Abfragen

B = Bearbeiten

leer = kein Zugriff

andere

**Organisationseinheiten**

VE I: z.B. Rechtsdienst der betreffenden VE

VE II: z.B. Sachbearbeiter/-in der betreffenden VE

VE III: z.B. Administrator der betreffenden VE

…

Kant. Amt: z.B. kantonale Polizeibehörden

…

## Dokumentenverzeichnis

Beinhaltet die Auflistung aller für die betreffende Datensammlung relevanten Gesetze, Verordnungen, Weisungen, Regelungen, technischen Spezifikationen, usw. Die Auflistung ist durch die departements- und/oder amtseigenen Dokumente zu ergänzen (erweitern).

|  |  |
| --- | --- |
| Dokumententyp | Titel |
| Gesetze | Gesetzliche Grundlage des Schutzobjektes (vom Verfasser zu ergänzen) |
|  | [Bundesgesetz vom 25. September 2020 über den Datenschutz (Datenschutzgesetz; DSG; SR 235.1)](https://www.fedlex.admin.ch/eli/cc/2022/491/de) |
|  | [Bundesgesetz vom 17. Dezember 2004 über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ; SR 152.3)](http://www.admin.ch/ch/d/sr/c152_3.html) |
|  | [Bundesgesetz vom 26. Juni 1998 über die Archivierung (Archivierungsgesetz, BGA; SR 152.1)](http://www.admin.ch/ch/d/sr/c152_1.html) |
| Verordnungen | [Verordnung vom 25. November 2020 über die Koordination der digitalen Transformation (Verordnung über die digitale Transformation; VDTI; SR 172.010.58)](https://www.fedlex.admin.ch/eli/cc/2020/988/de) |
|  | [Verordnung vom 31. August 2022 über den Datenschutz (Datenschutzverordnung; DSV; SR 235.11)](https://www.fedlex.admin.ch/eli/cc/2022/568/de) |
|  | [Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV; SR 510.411)](https://www.fedlex.admin.ch/eli/cc/2007/414/de) |
|  | [Verordnung vom 22. November 2017 über den Schutz von Personendaten des Bundespersonals (BPDV; SR 172.220.111.4)](https://www.fedlex.admin.ch/eli/cc/2017/793/de) |
|  | [Verordnung vom 27. Mai 2020 über den Schutz vor Cyberrisiken in der Bundesverwaltung](https://www.fedlex.admin.ch/eli/cc/2020/416/de) |
| Strategien | [SN002 - Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022 - 18.4.2018](https://intranet.ncsc.admin.ch/dam/ncscintra/de/dokumente/grundlagen/ncs/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_DE.pdf.download.pdf/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_DE.pdf) |
|  |  |
| Eigene Dokumente | Berechtigungskonzept |
|  | Darstellung des Datenflusses / Datenflussdiagramm |
|  | IT-Architekturaufbau |
|  | … |

## Abkürzungen

|  |  |
| --- | --- |
| Abkürzung | Bedeutung |
| Abs. | Absatz |
| Art. | Artikel |
| BJ | Bundesamt für Justiz |
| Bst. | Buchstabe |
| DSB | Datenschutzberater/-innen |
| DSG | Bundesgesetz über den Datenschutz (SR 235.1) |
| DSV | Verordnung über den Datenschutz (SR 235.11) |
| EDÖB | Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter |
| IKT | Informations- und Kommunikationstechnik |
| ISBO | Informatiksicherheitsbeauftragte/r der Organisationseinheit |
| ISDS-Konzept | Informationssicherheits- und Datenschutzkonzept |
| LB | Leistungsbezüger |
| LE | Leistungserbringer |
| NCSC | Nationales Zentrum für Cybersicherheit |
| PL | Projektleiter/-in |
| VE | Verwaltungseinheit |
| … | … |

## Begriffe

|  |  |
| --- | --- |
| Begriff | Bedeutung |
| Bearbeiten | Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten (siehe Art. 5 Bst. d DSG). |
| Bekanntgeben | Das Übermitteln oder Zugänglichmachen von Personendaten (Art. 5 Bst. e DSG). |
| Besonders schützenswerte Personendaten | Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; über die Gesundheit, die Intimsphäre oder Zugehörigkeit zu einer Rassen oder Ethnie; über die Gene; über Massnahmen der sozialen Hilfe; und über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen (Art. 5 Bst. c DSG). |
| Verletzung der Datensicherheit: | Eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden (Art. 5 Bst. h DSG). |
| Verantwortlicher | Private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet (Art. 5 Bst. j DSG). |
| Auftragsbearbeiter | private Person oder Bundesorgan, die oder das im Auf-trag des Verantwortlichen Personendaten bearbeitet (Art. 5 Bst. k DSG). |
| Personendaten, betroffene Person | Alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. (Art. 5 Bst. a und b DSG). |
| Profiling | Jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen (Art. 5 Bst. f DSG). |
| Profiling mit hohem Risiko | Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt (Art. 5 Bst. g DSG). |
| … | … |

1. **Art. 34** Rechtsgrundlagen:
2 Eine Grundlage in einem Gesetz im formellen Sinn ist in folgenden Fällen erforderlich:
c. Der Bearbeitungszweck oder die Art und Weise der Datenbearbeitung **können zu einem schwerwiegenden Eingriff in die Grundrechte** der betroffenen Person führen. [↑](#footnote-ref-1)