Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Was muss in einem Bearbeitungsreglement eines Bundesorgans aufgeführt werden?

Das Bearbeitungsreglement soll für die notwendige Transparenz im Umfeld sowohl der Systementwicklung als auch der Datenbearbeitung sorgen. Die erste Version des Bearbeitungsreglements ist am Ende der Projektplanungsphasen (Ende Konzeptphase nach HERMES[1]) verfügbar. Das Reglement wird in der Folge auch während des Systembetriebs nachgeführt. Insbesondere Systemänderungen sowie die Durchführung von Kontrollen sind in der Betriebsphase zu dokumentieren. Das Bearbeitungsreglement ist in möglichst kurzer und verständlicher Form zu führen, so dass das System auch von "Nicht-Experten" verstanden bzw. beurteilt werden kann. Es gilt der Grundsatz "soviel wie nötig, und so wenig wie möglich". Für detailliertere Informationen ist auf andere Dokumente zu verweisen.

Das Bearbeitungsreglement (Art. 21 i.V.m. Art. 16 der Verordnung zum Bundesgesetz über den Datenschutz; VDSG, SR 235.11) beinhaltet mindestens die folgenden Punkte:

- **Inhaltsverzeichnis**
- **Abkürzungen**
- **Reglementsänderungen**

1. **Name und Adresse des verantwortlichen Bundesorgans** (Art. 16, Abs. 1, Bst a VDSG)

2. **Name und vollständige Bezeichnung der Datensammlung** (Art. 16, Abs. 1, Bst b VDSG)

3. **Rechtsgrundlage und Zweck der Datensammlung** (Art. 16, Abs. 1, Bst d VDSG)

4. **Ausgangslage**
   Kurz festhalten, warum man ein System gestalten will, den Zweck sowie den gewünschten Soll-Zustand umschreiben.

5. **Kategorien der bearbeiteten Personendaten** (Art. 16, Abs. 1, Bst e VDSG)

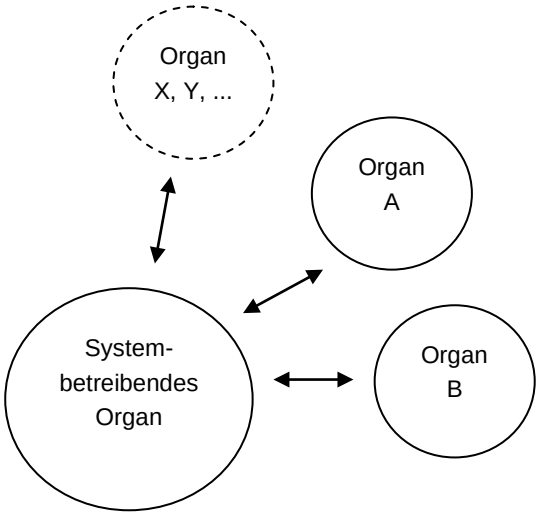
6. **Kategorien der Empfänger der Daten** (Art. 16, Abs. 1, Bst f VDSG)

7. **Kategorien der an der Datensammlung Beteiligten** (Dritte, die Daten in eine Datensammlung eingeben und verändern dürfen, Art. 16, Abs. 1, Bst g VDSG)

8. **Dokumentation, der vom System betroffenen Organisationseinheiten**
   (Systembetreibendes[2] Organ – Umsystem)

[1] HERMES ist ein Standard der Schweizerischen Bundesverwaltung für die Führung und Abwicklung von Projekten (Projektführungsmethode). In der Privatwirtschaft können auch andere Projektführungsmethoden verwendet werden.
[2] Es ist zu beachten, dass der Begriff "System" nicht EDV-technisch zu verstehen ist.

Feldeggweg 1, 3003 Bern
Tel. 058 462 43 95, Fax 058 465 99 96
www.edoeb.admin.ch



Schnittstellenbeschreibung

Von	Nach	Zweck	Datenart	Periodizität	Auslöser (Org.-Einheit)	Medium
SbO	Organ A		Freitext, sensitiv	monatlich		Papier
Organ A	SbO		...	...	...	...
Organ X	SbO	...	...	...	...	E-Mail

...

In der Schnittstellenbeschreibung sind folgende Angaben zur Datenweitergabe (Bekanntgabe) festzuhalten:

- von wem stammen die Daten?
- wer erhält die Daten?
- zu welchem Zweck werden die Daten weitergegeben?
- welche Daten werden weitergegeben?
- in welcher Periodizität werden die Daten weitergegeben?
- von wem wurde die Weitergabe initiiert?
- mit Hilfe welchen Mediums werden die Daten weitergegeben?

Die Schnittstellenbeschreibung umschreibt das oben aufgeführte “Bubble-Chart“.

8.1 Organigramm des systembetreibenden Organs (SbO)

Aufführen des Organigramms und der Bereiche (inkl. Anzahl Mitarbeitende), die mit dem System arbeiten.

8.2 Verantwortlichkeiten

Festhalten, wer für Anwendung, Netzwerk, Datenbank, Betriebssystem, usw. verantwortlich ist.

8.3 Weitere wichtige Anwendungen beim SbO mit Schnittstellen zu dem im vorliegenden Reglement aufgeführten System

Die Anwendungen sind aufzuführen.

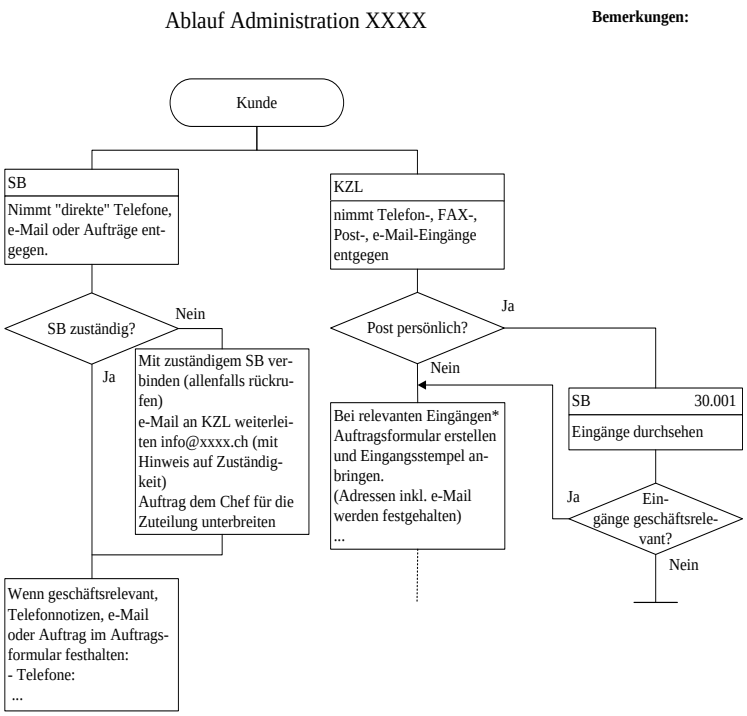
9. Auflisten der Unterlagen über die Planung, Realisierung und den Betrieb der Datensammlung

Planung: Vorstudie, Konzept, ...
Realisierung: Aufgrund eines Pflichtenheftes, Anwendungshandbuch
Betrieb: Benutzerhandbuch, Systemhandbuch, ...

10. Anmeldung der Datensammlung beim EDÖB (Art. 16 VDSG)
Für die anmeldepflichtigen Bundesorgane (vgl. Art. 11a des Bundesgesetzes über den Datenschutz; DSG, SR 235.1) ist die ordentliche Anmeldung als Anhang dem Reglement beizulegen. Die Anmeldung oder Nachführung wird für die Bundesverwaltung in den drei Nationalsprachen verlangt. Bundesorgane melden ihre Datensammlungen im Regelfall über Intranet an. Weitere Hinweise zur Anmeldung finden sich auf der Homepage des EDÖB: *www.derbeauftragte.ch*, unter: *Datenschutz > Datensammlung anmelden*.

11. Abläufe (Prozesse)
Die Abläufe sind zu dokumentieren. Je sensitiver das System ist, umso detaillierter muss die Beschreibung sein. Es gilt aber auch der Grundsatz “so tief wie notwendig“ (Transparenz).

Beispiel der Dokumentation eines Ablaufs:



12. Das für den Datenschutz und die Datensicherheit verantwortliche Organ (Art. 21, Abs. 2, Bst a VDSG)

13. Die Herkunft der Daten (Art. 21, Abs. 2, Bst b VDSG)
sollte aus der Schnittstellenbeschreibung ersichtlich sein.

14. Die Zwecke, für welche die Daten regelmässig bekannt gegeben werden (Art. 21, Abs. 2, Bst c VDSG)
sollten aus der Schnittstellenbeschreibung ersichtlich sein.

15. **Die Kontrollverfahren und insbesondere die technischen und organisatorischen Massnahmen nach Art. 20 VDSG** (Art. 21, Abs. 2, Bst d VDSG sowie Art. 8-10 VDSG)
Es sind diejenigen Kontrollverfahren aufzuführen, die während der Planung, der Realisierung als auch in der Betriebsphase durchgeführt wurden bzw. werden.

Technische und organisatorische Massnahmen
Je nach Betrachtungsweise können sich die acht unten aufgeführten Zielsetzungen überschneiden. Bei den jeweiligen Zielsetzungen ist aufzuführen, mit welchen Vorkehrungen man diesen gerecht wird. Bitte beachten Sie in diesem Zusammenhang auch Punkt 19 (Konfiguration der Informatikmittel).
Zugangskontrolle: (Art. 9, Abs. 1, Bst a VDSG)
Unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren;
Datenträgerkontrolle: (Art. 9, Abs. 1, Bst b VDSG)
Unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen*;*
Transportkontrolle: (Art. 9, Abs. 1, Bst c VDSG)
Bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können*;*
Bekanntgabekontrolle: (Art. 9, Abs. 1, Bst d VDSG)
Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können*;*
Speicherkontrolle: (Art. 9, Abs. 1, Bst e VDSG)
Unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern;
Benutzerkontrolle: (Art. 9, Abs. 1, Bst f VDSG)
Die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern;
Zugriffskontrolle: (Art. 9, Abs. 1, Bst g VDSG)
Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen;
Eingabekontrolle (Protokollierung): (Art. 9, Abs. 1, Bst h VDSG)
In automatisierten Systemen muss nachträglich überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden. (Die Protokollierung hat allerdings nur dann zu erfolgen, wenn sie sinnvoll oder notwendig ist. Die Mitarbeiter sind über die Protokollierungen zu informieren.)

16. **Die Beschreibung der Datenfelder und der Organisationseinheiten, die darauf Zugriff haben** (Art. 21, Abs. 2, Bst e DSG)
In der Zugriffsmatrix ist festhalten, welche Rollen (Stellen) welche Daten mutieren, einsehen, ..., dürfen (Zugriffskontrolle).

17. **Art und Umfang des Zugriffs der Benutzer der Datensammlung** (Art. 21, Abs. 2, Bst f VDSG)
Es ist aufzuführen, wie die Daten abgefragt (selektiert) werden können und ob auf die gesamte Datenmenge zugegriffen werden darf (Zugriffskontrolle).

18. **Die Datenbearbeitungsverfahren, insbesondere die Verfahren bei der Berichtigung, Sperrung, Anonymisierung (Pseudonymisierung), Speicherung, Aufbewahrung, Archivierung oder Vernichtung der Daten** (Art. 21, Abs. 2, Bst g VDSG)
Der Grossteil der obigen Anforderungen sollte durch die Dokumentation der Abläufe abgedeckt worden sein. Verfahren, die aus den dokumentierten Prozessen nicht ersichtlich sind, sind an dieser Stelle aufzuführen.

    Die Instrumente und Verfahren für die Ausübung des Berichtigungs-, Vernichtungs- und Sperrungsrechts sowie das Recht auf Anbringung eines Bestreitungsvermerks sind zu schaffen (Art. 25 i.V.m. 20 DSG). Der betroffenen Person ist die Verweigerung oder Einschränkung ihrer Rechte in einer Verfügung mitzuteilen.

    Das Bearbeiten beginnt bei der Erhebung der Personendaten und endet bei deren Anonymisierung oder Löschung.

19. **Die Konfiguration der Informatikmittel** (Art. 21, Abs. 2, Bst h VDSG)
Anwendung
Netzwerk
Datenbank
Betriebssystem
Hardware
Die getroffenen Schutz- und Sicherheitsmassnahmen können, soweit sie informatikbezogen sind und man sie den obigen „Teilsystemen“ zuordnen kann, in diesem Bereich aufgeführt werden.

20. **Das Verfahren zur Ausübung des Auskunftsrechts** (Art. 21, Abs. 2, Bst i VDSG i.V.m. Art. 8 und 9 DSG und Art. 13 VDSG)
Es ist insbesondere festzuhalten, an wen sich die Person wenden soll, die Auskunft verlangt, und wie das interne Verfahren (inklusive Prozess bis zur Verfügung) abläuft.

Anhang 1 *Kopie der ordentlichen Anmeldung der Datensammlung*
Anhang 2 *Die drei wichtigsten Bildschirmmasken der Anwendung*

Stand: Mai 2014