**Datenschutz-Folgenabschätzung**

**für Online-Gesuche**

|  |  |
| --- | --- |
| Projektbezeichnung: |  |
| Autor: |  |
| Datum: |  |

# Rechtsgrundlagenanalyse und Beschreibung der Bearbeitung von Personendaten

## **Rechtsgrundlagen**

Rechtsgrundlagen für Datenbearbeitung durch das gesuchstellende Organ

| **Datenbearbeitung** | **Rechtsgrundlagen** | **Gegeben?** |
| --- | --- | --- |
| *Beschreibung der Datenbearbeitungen der Gesuchstellerin/des Gesuchstellers (Darstellung des Sachverhalts; Beispiele: «Führen des Verzeichnisses der Mitglieder der Kirchgemeinde»; «Veranlagung und Erhebung von Steuern der Zugerinnen und Zuger»; «Auszahlung von landwirtschaftlichen Direktzahlungen und Beiträgen»; etc.)* | *Paragraf/Artikel des Gesetzes, der – die beschriebene Daten­bearbeitung erlaubt oder – die Aufgabe regelt, welche die beschriebene Daten-bearbeitung erfordert* | *j/n* |
|  |  |  |

## **Beschreibung des Datenbezugs/der Datenbekanntgabe via Online-Zugriff**

| **Vom Zugriff betroffene Personendaten** | **Herkunft** | **Zweck/e, für welche/n der Datenbezug erfolgen soll** | **Verhältnismässigkeit** |
| --- | --- | --- | --- |
| *Hier kann auf Teil 1 Ziff. 4 des Gesuchsformulars bzw. allenfalls auf eines der Zusatzblätter zum Gesuchsformular verwiesen werden.* *Beispiele:**Wohnadresse**Todesdatum**Niederlassung/Aufenthalt* | *Verantwortliches Organ, Datenbestand.* | *Beispiele:* *«Überprüfen und aktualisieren der Wohnadresse von Beitragsberechtigten»**«Vermeiden von postalischen Zustellungen an verstorbene Personen»**«Überprüfen der Beitragsberechtigung aufgrund des aktuellen Meldestatus (Niederlassung/Aufenthalt)»*  | *Begründung von Umfang, Art und Dauer des Datenbezugs/der Datenbekanntgabe.**Beschreibung des Zeitpunkts der Aufhebung des Datenbezugs/der Datenbekanntgabe von einzelnen betroffenen Personen.* *Darlegung der Geeignetheit und Erforderlichkeit des Datenbezugs/der Datenbekanntgabe.*  |
|  |  |  |  |

**Protokollierung des Online-Zugriffs**

Bei Online-Zugriffen in Form von Einzelabfragen über eine Benutzeroberfläche auf das kantonale Personenregister (sog. «GUI-Abfrage») muss dieser Block nicht ausgefüllt werden. Die Logfiles werden von der Fachanwendung, auf die zugegriffen wird, erstellt, die Protokollierung ist bekannt.

| **Protokollierungs-mechansimus und Logdaten** | **Aufbewahrungsdauer und Zugriffsrechte** *(Angabe)*  | **Löschungsmechanismus nach Ablauf der Aufbewahrungsdauer** |
| --- | --- | --- |
| *Beschreiben der Protokollierung und der Logdaten* | *Tage, Monate oder Jahre oder, falls dies nicht möglich, Kriterien für die Festlegung dieser Dauer.* *Zugriffsberechtigungen auf Logdaten.* | *Beschreiben des Löschvorgangs.* |
|  |  |  |

# Geplante Umsetzung

Bitte beschreiben Sie die einzelnen Themen direkt in dieser Vorlage. Es kann jederzeit auf Drittdokumente verwiesen werden (bitte konkrete Textstellen angeben), sofern diese die notwendigen Informationen enthalten.

| **Thema** | **Projektangaben** |
| --- | --- |
| Prozessbeschreibung | *Prozessbeschreibung oder Flussdiagramm* |
| Datenflussdiagramm | *Ein Datenflussdiagramm zeigt die Datenbearbeitung/den Datenbezug übersichtlich auf, insbesondere unter grafischer Darstellung der betroffenen Anwendungen und Datenbestände, deren Beziehungen bzw. Schnittstellen untereinander sowie der Nutzerzugriffe.**Ein einfaches Beispiel:* |
| Technische Umsetzung | *Kurze Beschreibung der wesentlichen Umsetzungsfaktoren, wie** *eingesetzte Anwendungen, Systeme und Technologien (sowohl bezüglich Fachanwendungen zur Datenbearbeitung als auch der Schnittstelle bzw. der eingesetzten Kommunikationsmittel)*
* *ob diese intern oder extern betrieben werden*
* *Schnittstellen zu weiteren Systemen*
* *ob und wie eine Datenübermittlung bzw. ein Datenzugriff über Drittnetzwerke (z.B. über das Internet) oder via Ausland erfolgt*
* *etc.*

*Ist die Erstellung eines ISDS-Konzepts erforderlich (siehe Ziff. 4), bitte dort konkret ausführen.* |
| IT-Grundschutz? | IT-Grundschutz sichergestellt und dokumentiert?[ ]  Ja [ ]  Nein |
| Auftragsdaten-bearbeitung | *Übersicht über Auftragsdatenbearbeiter, insbesondere IT-Dienstleister, mit Art der Datenbearbeitung, Standort und technischer Anbindung. Nachweis der Einhaltung der kantonalen Datenschutzbestimmungen durch den Auftragsdatenbearbeiter und allenfalls dessen Subunternehmer beilegen (Vertrag, Vereinbarung, Geheimhaltungserklärungen etc.)* |
| Berechtigungs-konzept | *Berechtigung der zugreifenden Personen: Wie wird sichergestellt, dass die Rechte gemäss Ziff. 7 des Gesuchsformulars umgesetzt werden.**Allfällig technischer User: Mit welchen Rechten wird ein solcher User auf der Stufe Schnittstelle ausgestattet?* |

# Risikoanalyse und Bewertung der Massnahmen

***Die vorabgefüllten Risiken und Massnahmen in der nachfolgenden Tabelle sind im Sinne einer Checkliste als Beispiele zu verstehen.***

**Zu den einzelnen Spalten (in der nachfolgenden Tabelle)**:

1. **Risikoanalyse**: Welche Risiken sind mit der geplanten oder geänderten Bearbeitung von Personendaten verbunden?
*Die Risiken sind ohne die Berücksichtigung von möglichen geplanten Massnahmen aufzuführen (inhärentes Risiko).*
2. **Risikobewertung:** Wie sind die identifizierten Risiken in Bezug auf das Schadensausmass und die Eintretenswahrscheinlichkeit zu bewerten?
*Bei der Risikobewertung wird ebenfalls die Annahme getroffen, dass keine risikomindernden Massnahmen getroffen worden sind. Übertragen in die Risikoanalyse der DSFA wird «nur» der Wert des Schnittpunktes zwischen Schadensausmass und Eintretenswahrscheinlichkeit gemäss Matrix (farblich dargestellt bzw. mit tief/mittel/hoch bezeichnet).*
3. **Massnahmen:** Welche Massnahmen zur Bewältigung des identifizierten Risikos werden getroffen?
4. **Bewertung Restrisiko:** Welches Risiko bleibt nach Berücksichtigung der vorgesehenen Massnahme (Spalte C) bestehen?



BEISPIELE für Risiken und Massnahmen

Im Sinn von Beispielen sind einige der möglichen Risiken und Massnahmen erwähnt. Bitte ergänzen/anpassen.

| *#* | *A) Inhärentes Risiko* | *B) Bewertung (tief, mittel, hoch)* | *C) Massnahme* | *D) Restrisiko (tief, mittel, hoch)* |
| --- | --- | --- | --- | --- |
| *1. Datenminimierung/Datensparsamkeit* |
| *1.1* | *Datenbezug/-bekanntgabe betrifft Personen, die für die Gesuchstellerin/den Gesuchsteller nicht relevant sind.* |  | * *Einsatz von Mindest-Suchparametern zur Begrenzung der Suchresultate;*
* *Datenbezug/-bekanntgabe bedingt Vorhandensein einer betroffenen Person im Datenbestandder Gesuchstellerin/des Gesuchstellers;*
* *Einsatz von Filterkriterien (nur aktive, nur bestimmte Altersgruppe, nur Niedergelassene etc.).*
 |  |
| *1.2* | *Datenbezug/-bekanntgabe betrifft Personendaten, die nicht erforderlich sind* |  | * *Rollenbasierte Einschränkung der Zugriffsrechte auf erforderliche Personendaten (Attribute);*
* *Einsatz von automatisierten Bearbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme von Personendaten verhindern und die Einflussnahme begrenzen, bspw. Einsatz von Ampelsystemen;*
* *Einschränkung auf die notwendigen Ereignismeldungen.*
 |  |
| *1.3* | *Datenbezug/-bekanntgabe ist zeitlich unbeschränkt möglich bzw. nicht auf die erforder-liche Zeitdauer beschränkt*  |  | * *Festlegung und Umsetzung eines Konzepts für zeitlich beschränkten Bezug/zeitlich beschränkte Bekanntgabe von Daten der betroffenen Personen bzw. eines Löschkonzepts (bspw. nach Abschluss des Strafverfahrens oder des Schulaustritts ist ein Datenbezug nicht mehr möglich)*
 |  |
| *2. Vertraulichkeit* |
| *2.1* | *Unbefugte Personen (innerhalb und ausserhalb der gesuchstellenden Organisationseinheit) können sich Zugang zu Personendaten verschaffen, die Daten zur Kenntnis nehmen oder diese nutzen* |  | * *Erstellen eines Berechtigungs- und Rollenkonzepts nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die Gesuchstellerin/den Gesuchsteller;*
* *Implementierung eines sicheren Authentisierungsverfahrens;*
* *Festlegung und Kontrolle der Nutzung zugelassener Ressourcen bzw. sicherer Kommunikationsmittel;*
* *Verschlüsselung von transferierten und gespeicherten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen;*
* *Schutz vor äusseren Einflüssen (Spionage, Hacking);*
* *Meldung von Datenschutzverletzungen (§ 7c DSG).*
 |  |
| *2.2* | *Missbrauch der Online-Zugriffe durch zugriffsberechtigte Mitarbeitende* |  | * *Sorgfältige Instruktion der zugriffsberechtigten Mitarbeitenden und allfälliger Auftragsdatenbearbeiter;*
* *Protokollierung der Online-Zugriffe;*
* *Konzept für Kontrolle/Auswertung der Protokolldaten in Zusammenarbeit mit dem verantwortlichen Organ, Festlegung Follow-up-Prozess, Sanktionen (Aufhebung bzw. Sperrung des Online-Zugriffs).*
 |  |
| *5. Nichtverkettung* |
| *5.1* | *Daten (aus verschiedenen Quellen) können ohne Zweckbindung zusammengeführt werden* |  | * *Einschränkung von Bearbeitungs-, Nutzungs- und Übermittlungsrechten;*
* *Trennung nach Organisations-/Abteilungseinheiten.*
 |  |
| *6. Transparenz* |
| *6.1* | *Die Transparenz gegenüber betroffenen Personen ist nicht gewährleistet* |  | * *Information der betroffenen Personen über die Datenerhebung/ den Datenbezug bei Dritten via Online-Zugriff;*
* *Regelung der Zuständigkeiten für Auskunftsrechte der betroffenen Personen.*
 |  |

# Informationssicherheits- und Datenschutz-Konzept (ISDS)

Ein ISDS-Konzept (Vorlage zum Download [hier](https://www.zg.ch/behoerden/datenschutzstelle/services/bewilligungen-online-zugriffe)) ist unter bestimmten Voraussetzungen zusammen mit dieser DSFA einzureichen (bitte Zutreffendes ankreuzen).

|  |  |  |  |
| --- | --- | --- | --- |
| *#* | *Frage* |  |  |
| *1* | *Bestehen gemäss Risikoanalyse in Kapitel 3 dieses Dokuments hohe Restrisiken für die Grundrechte der betroffenen Personen?* | [ ]  *ja**ISDS-Konzept notwendig* | [ ]  *nein**Zu #2* |
| *2* | *Werden die Daten ausschliesslich innerhalb der geschützten kantonalen oder gemeindlichen Netzwerke bearbeitet?* | [ ]  *ja**Kein ISDS-Konzept* | [ ]  *nein**ISDS-Konzept notwendig* |

Es wird ein ISDS-Konzept

[ ]  miteingereicht.

[ ]  nicht miteingereicht.

# Genehmigung / Bestätigung

(bitte Zutreffendes ankreuzen)

Die/der Unterzeichnete genehmigt die Dokumente der Datenschutz-Folgenabschätzung. Sie/Er bestätigt, dass

[ ]  Datenbearbeitungen

[ ]  keine Datenbearbeitungen

vorliegen, die zu einem hohen Restrisiko für die Grundrechte der betroffenen Person führen können.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Ort, Datum |  | Vorname Name, Funktion der/des Unterschriftberechtigten für das gesuchstellende Organ  |