|  |  |
| --- | --- |
|  | If completed, at least: INTERNAL |

|  |
| --- |
|  |

Processing Regulations

< Project name / Asset name >

|  |
| --- |
|  |

|  |  |
| --- | --- |
| Classification | **INTERNAL** / CONFIDENTIAL / SECRET |
| Status | **in progress** / under review / approved for use |
| Project number | No |
| Project Lead (PL SR) | PL SR |
| Version | From Template V2.1 - P042-Hi04 - Processing Regulations |
| Date |  |
| Client | Client |
| Author(s) | Author |

Change control

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description, remarks | Name |
| 0.1 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Distribution list

|  |  |  |
| --- | --- | --- |
| Function | Name  | Department/Office |
| DPA |  |  |
| ITSOO |  |  |
|  |  |  |
|  |  |  |

Table of contents

[1 General 4](#_Toc152309913)

[1.1 Description 4](#_Toc152309914)

[1.2 Purpose of the processing regulations for federal bodies 4](#_Toc152309915)

[1.3 Tailoring 5](#_Toc152309916)

[1.4 Aids 5](#_Toc152309917)

[1.5 Approval 6](#_Toc152309918)

[2 Processing regulations of federal bodies 7](#_Toc152309919)

[2.1 General 7](#_Toc152309920)

[2.1.1 Legal basis 7](#_Toc152309921)

[2.1.2 Purpose of the data processing 8](#_Toc152309922)

[2.1.3 Categories of data subjects and categories of personal data processed 8](#_Toc152309923)

[2.2 Internal organisation 8](#_Toc152309924)

[2.2.1 Responsible federal body 8](#_Toc152309925)

[2.2.2 Processor 9](#_Toc152309926)

[2.2.3 Users and data access 9](#_Toc152309927)

[2.2.3.1 User group 9](#_Toc152309928)

[2.2.3.2 Access authorisation 10](#_Toc152309929)

[2.2.3.3 Roles 10](#_Toc152309930)

[2.2.3.4 Access authorisation process 10](#_Toc152309931)

[2.3 Data processing and control procedures 10](#_Toc152309932)

[2.3.1 Processing personal data 11](#_Toc152309933)

[2.3.1.1 Business processes 11](#_Toc152309934)

[2.3.1.2 Data disclosure and interfaces 11](#_Toc152309935)

[2.3.1.3 Verification of the recorded personal data 12](#_Toc152309936)

[2.3.1.4 Processes / Data processing procedures 12](#_Toc152309937)

[2.3.2 Retention period, archiving and deletion 12](#_Toc152309938)

[2.3.2.1 Retention period 12](#_Toc152309939)

[2.3.2.2 Archiving 12](#_Toc152309940)

[2.3.2.3 Deletion 12](#_Toc152309941)

[2.3.3 Rights of the data subjects 12](#_Toc152309942)

[2.4 Measures to ensure data security 13](#_Toc152309943)

[3 Annex 14](#_Toc152309944)

[3.1 Record of processing activities 14](#_Toc152309945)

[3.2 Data protection impact assessment 15](#_Toc152309946)

[3.3 Authorisation concept / Authorisation matrix 15](#_Toc152309947)

[3.4 List of documents 17](#_Toc152309948)

[3.5 Abbreviations 18](#_Toc152309949)

[3.6 Terms 19](#_Toc152309950)

# General

## Description

Description of the automated processing of the ICT project.

## Purpose of the processing regulations for federal bodies

The basis for the processing regulations – in relation to ICT projects in the Federal Administration – is the ISDP concept.

The **federal body responsible and its Processor** (see Art. 6 DPO) shall draw up processing regulations for automated processing operations if they:

* process sensitive personal data;
* carry out profiling;
* process personal data in accordance with Article 34 paragraph 2 letter c FADP[[1]](#footnote-1);
* make personal data accessible to cantons, foreign authorities, international organisations or private persons;
* link data collections with each other; or
* operate an information system or manage data collections with other federal bodies.

The **FDPIC** must draw up processing regulations for all automated processing operations (Art. 40 DPO).

The regulations must in particular contain information on

* the internal organisation structure,
* the data processing and control procedures, and
* the measures to ensure data security.

They contain a listing of all documents concerning the planning, realisation and operation of the data collection. The list of processing activities (pursuant to Art. 12 FADP), a data protection impact assessment (DPIA, pursuant to Art. 22 FADP) and any ISDP concept must be attached to the processing regulations as an annex.

The processing regulations are intended to guarantee the required transparency in relation to system development and adaptation and the automated electronic processing of personal data.

The first version of the processing regulations will be available on completion of the Concept phase in HERMES.

The federal body responsible and its Processor must regularly update the regulations and make them available to the data protection officer.

## Tailoring

The processing regulations must be kept as short and comprehensible as possible so that the description of the automated data collection can also be understood or assessed by non-experts (principle).

However, the more extensive or sensitive the intended processing of personal data is, the more detailed the processing regulations must be. The most important aspects from the point of view of data protection and information security – if not already included in the directory of processing activities, in the DPIA and in the ISDP concept – must be described in the processing regulations. For more detailed information, please refer to further documents.

It is important not to copy the contents of existing documents, but to refer to them with precise information and to attach these documents. The Rules of Procedure should not be an exercise in copying and reproducing.

The blue text serves as an aid to completing the document.

## Aids

The following aids may be used to draw up the processing regulations:

**Aids:**

* [Guidelines on security procedures and associated aids at federal level from the Federal Cyber Security Delegate, NCSC](https://intranet.ncsc.admin.ch/ncscintra/de/home/vorgaben-hilfsmittel/sicherheitsverfahren.html)
* [Main legislative instruments, FOJ](https://www.bj.admin.ch/bj/de/home/staat/legistik/hauptinstrumente.html)
* [Total revision of the Data Protection Act (DPA) - Overview of the most important changes related to drafting legal provisions on data processing by federal bodies, FOJ](https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/dsg-uebersicht-aenderungen.pdf.download.pdf/dsg-uebersicht-aenderungen-d.pdf)
* [Guide to Legislation on Data Protection, FOJ](https://www.bj.admin.ch/dam/bj/de/data/staat/legistik/hauptinstrumente/leitfaden-datenschutz.pdf.download.pdf/leitfaden-datenschutz-d.pdf)
* Technical and organisational measures (TOM) (in the FDPIC's Infocenter Data Protection)

## Approval

The signatures confirming approval must be added before the start of operations.

With his/her signature, the data protection officer confirms that he/she has examined the processing regulations. In particular, he/she has checked that the document is completed in full and that all required measures are documented. He/she has critically examined the information to see if it is consistent and correct in the context of the processing of the data.

The Controller approves the processing regulations with his/her signature.

|  |  |
| --- | --- |
| Date / Name / Signature **Data Protection Officer**: | …………………………………………………...…... |
| Date / Name / Signature **Controller**:  | …………………………………………………...…... |
|  |  |

Further signatures may be added.

The signatures may also be added in electronic form (in a PDF).

# Processing regulations of federal bodies

## General

### Legal basis

This section sets out the legal provisions on which the processing of personal data in the data file is based in accordance with the DPA:

**Art. 34 FADP** Legal basis

1 Federal bodies may only process personal data if there is a statutory basis for doing so.

2 A statutory basis in a formal law is required in the following cases:

a. The matter involves the processing of sensitive personal data.

b. The matter involves profiling.

c. The purpose or manner of the data processing may lead to a serious violation of the data subject's fundamental rights.

3 A statutory basis in a substantive law is sufficient as the basis for processing personal data under paragraph 2 letters a and b provided the following requirements are satisfied:

a. Processing is essential for a task required by a formal law.

b. The purpose of processing poses no particular risks to the data subject's fundamental rights.

4 In derogation from paragraphs 1–3, federal bodies may process personal data if any one of the following requirements is satisfied:

a. The Federal Council has authorised the processing because it considers that the data subject's rights are not at risk.

b. The data subject has consented to the processing in the specific case or has made their personal data generally accessible and has not explicitly prohibited any processing.

c. The processing is necessary in order to protect the life or physical integrity of the data subject or of a third party, and it is not possible to obtain the consent of the data subject within a reasonable time.

If the processing of personal data is transferred to a Processor by contract (e.g. outsourcing contract) or by legislation, the following requirements must be met according to Art. 9 para. 1 FADP:

* the data is only processed as the person responsible (the office, the organisational unit) itself would be allowed to do;
* no legal or contractual confidentiality obligation prohibits the transfer.

In particular, the Controller (or the federal body responsible) must ensure that the Processor guarantees data security (Art. 9 para. 2 FADP).

**Art. 36, para. 5 FADP** provides:

Federal bodies may make personal data generally accessible by means of automated information and communications services if there is a legal basis for publishing the data or if they disclose data based on paragraph 3. If there is no longer a public interest in making the data generally accessible, the data concerned shall be deleted from the automated information and communications service.

### Purpose of the data processing

(Basis: FADP Art. 6 para. 3 in conjunction with FADP Art. 1 para. 2 let. b, FADP Art. 6 para. 4 – 5, Art. 7 para. 3, Art. 12 para. 2)

The purpose, nature, scope and circumstances of the processing must be described.

At the start, a brief explanation must be given of why it is intended to design a system, what its purpose is and what the desired target state is.

### Categories of data subjects and categories of personal data processed

(Basis: FADP Art. 6 para. 6, 7, Art. 12 para. 2, Art. 19, DPO Art. 1 para. 2 let. a, Art. 13)

The following questions must be answered regarding the content of the processed data:

* What type of personal data is being processed (personal data, sensitive personal data, personality profiles, other)?
* What type, categories (or ‘groups’), number of individuals and volume of personal data are being processed?
* How were the personal data obtained

## Internal organisation

(Basis: FADP Art. 9, 10, 12, 13, 33; DPO Art. 7, 8, 17, 23, 25)

### Responsible federal body

Provide an organisation chart for the federal body responsible for data processing and the divisions (incl. number of employees) that work with the data. In particular, the Controller, the application owner, the data protection officer and the IT security officer for the administrative unit (ITSOO) must be listed by name.

Indicate the control procedures and who is responsible for data protection if a federal body processes personal data with other federal bodies, cantonal bodies or private persons.

If not already listed in the ISDP concept and this is attached, also record who is responsible for the application, network, database, operating system, etc. in which the data is contained or on which it is running.

Details of:

Responsible federal body:

User DataReg:

Application owner:

Data Protection Officer:

ITSOO:

Application controller:

Network controller:

Database controller:

Operating system controller:

### Processor

The Processor and the contact persons must be listed.

Details of:

Processor:

Contact person for the Provider /Processor:

### Users and data access

#### User group

The categories (or ‘groups’) of all organisational units or bodies entitled to have access (federal bodies, cantonal bodies, third parties) must be listed and a brief description must be given of the statutory tasks for which they require access to the data collection.

If applicable, refer to the communication matrix from the ISDP concept.

Below is an example of a possible representation.

Outline

Subsystems

| **Name** | **Description** | **Use** |
| --- | --- | --- |
| eIAM | Central identity and access management system for the Federal Administration.  | Used for user authentication and coarse-grained authorisation (role assignment). |
|  |  |  |
|  |  |  |

**eIAM / Keycloak**

eIAM is the central Identity & Access Management System of the Federal Administration. It is the responsibility of the Federal Chancellery, but operated by the FOITT (see <https://www.eiam.admin.ch/> ).

#### Access authorisation

The type and scope of access for the users of the data collection and the data fields must be listed or briefly described. If an authorisation matrix (or authorisation concept) already exists, it must be included in the annex to the processing regulations.

#### Roles

Which roles exist for access authorisation (e.g. case officer, administrator) and which scope of access does the individual role contain (query, edit, print, no access, other)?

Below is an example of a possible representation.

| **Name** | **Description** |
| --- | --- |
| Case officer |  |
| Application controller |  |
| Administrator |  |
| … |  |

#### Access authorisation process

The arrangements (process and responsibilities) for granting and revoking access authorisation must be described here. The following questions must be answered:

* Who is responsible for granting and revoking access authorisation?
* Who regularly checks the access authorisations granted and updates them?
* What is the scope of access authorisation?
* What is the process for granting and revoking access authorisation?
* What are the steps in the process?
* Is it centrally controlled?

## Data processing and control procedures

(Basis: DPA Art. 6, 7, 8, 9, 10, 12, 13, 16, 19, 21, 22, 24, 25, 28, 33, 36, 37, 41, 42; DPO Art. 1, 2, 3, 4, 6, 9, 10, 11, 12, 13, 15, 16, 17, 18, 20, 22, 26, 29, 30)

Topics are

Destruction as soon as no longer necessary for the purpose of processing.

Measures to correct personal data.

Consent to the processing of personal data.

Data protection using technology and data protection-friendly default settings.

Data security measures.

Dealing with processors.

Involving data protection officers.

Keeping a list of processing activities.

Using certifications.

Requirements for lawfully disclosing personal data abroad.

Duty to provide information when collecting personal data.

Duty to inform about automated individual decisions.

Data protection impact assessment.

Reporting data security breaches.

Arrangements for granting the right to information.

Right to the handover or transfer of data.

Control of and responsibility for the joint processing of personal data.

Disclosure of personal data.

Objecting to the disclosure of personal data by a federal body.

Other rights and procedures that a person has or can take against a federal body.

Disclosure of official documents containing personal data

### Processing personal data

#### Business processes

Here, the most important business processes of data collection from the point of view of data protection are to be documented and/or graphically represented.

#### Data disclosure and interfaces

Graphical overview of the interfaces to other assets such as systems, applications, etc. is to be provided here. Reference can also be made to the ISDP concept, should a corresponding overview already exist there.

The interface description should contain the following information on data transfer (disclosure):

* who does the personal data originate from?
* who receives the personal data?
* why are the personal data being disclosed?
* what categories (or ‘groups’) of personal data are disclosed?
* how regularly are the personal data passed on?
* who initiated the transfer?
* which medium is used to pass on the personal data?

The purposes for which the personal data are regularly disclosed should be apparent from the interface description.

#### Verification of the recorded personal data

Who checks the accuracy of the personal data? Is there a process in place? Are these data regularly reviewed and corrected?

#### Processes / Data processing procedures

The processes for correcting, blocking, anonymising, saving, retaining, archiving and destroying data must be defined and described.

### Retention period, archiving and deletion

#### Retention period

The following questions must be addressed:

* How long may or must the collected personal data or each category (‘groups’) of personal data be kept?
* Where are the data stored and who is responsible for their storage?
* When will the data be deleted or should they be transferred to the Federal Archives?

#### Archiving

The organisational and technical arrangements (file formats, interfaces) for offering or transferring personal data to the Federal Archives must be specified here.

#### Deletion

When are personal data in the data collection that are no longer required deleted? This wording is to be coordinated accordingly with the ITSOO and the application controller.

### Rights of the data subjects

In particular, it must be specified who the data subject should contact (contact person/addressee) and how the internal process is to be carried out.

The means and procedures for exercising the rights to information, data portability, rectification, destruction of data and stopping their disclosure, as well as the right to have the data marked as disputed, must be created. Instruments for stopping disclosure to third parties must exist and must function.

The duty of federal bodies to provide information when collecting personal data must be taken into account and regulated accordingly.

## Measures to ensure data security

(Basis: DPA Art. 7, 8, 10, 12, 13, 22, 24, 33; DPO Art. 1, 2, 3, 4, 6, 15, 25, 26, 27)

The technical and organisational measures that ensure adequate data protection and are not already included in the ISDP concept should be listed here.

Outline

# Annex

## Record of processing activities

Controllers and processors must each keep a record of their processing activities (Article 12 FADP).

The Controller’s record must contain as a minimum:

* the identity of the Controller;
* the purpose of processing;
* a description of the categories of data subjects and the categories of personal data processed;
* the categories of recipients;
* if possible, the retention period for the personal data or the criteria for determining this period;
* if possible, a general description of the measures to ensure data security in accordance with Article 8 FADP;
* if the data are disclosed abroad, indication of the state concerned and the guarantees pursuant to Article 16 paragraph 2 FADP.

The Processor’s record must contain information on the identity of the Processor and of the Controller, on the categories of processing carried out on behalf of the Controller, and at least

* if possible, a general description of the measures to ensure data security in accordance with Article 8 FADP;
* if the data are disclosed abroad, details of the state concerned and the guarantees pursuant to Article 16 paragraph 2 FADP.

All federal bodies must submit their record to the FDPIC (Art. 12 para. 4 FADP) and must do so, as with the first version of the processing regulations, at the end of the Concept phase (Art. 31 para. 2 DPO).

The federal bodies are obliged to update this information on an ongoing basis and to submit their updated record to the FDPIC. The record is submitted via the FDPIC's web application ‘[DataReg](http://www.edoeb.admin.ch/dienstleistungen/00587/00966/index.html?lang=de)’.

A copy of the confirmation that the record has been submitted to the FDPIC must be kept with the processing regulations.

## Data protection impact assessment

In certain circumstances, the Controller must prepare a data protection impact assessment (Article 22 DPA).

The data protection impact assessment contains a description of the planned processing, an evaluation of the risks to the personality or fundamental rights of the data subject and a description of the measures to be taken to protect personality and fundamental rights.

If such a document exists, a copy of it shall be kept with the processing regulations.

## Authorisation concept / Authorisation matrix

The authorisation concept or the authorisation matrix is to be attached as an annex to the processing regulations.

Below is a simplified **example** of an authorisation matrix.

|  |  |  |  |
| --- | --- | --- | --- |
| Data field names | Confederation | Canton | Third party |
|  | OU I | OU II | OU III | … | … | … | Cant. Office | … | … | … | … | … | … | … |
|  |
| I. Master data |
| Surname(s) | A | A | B | … | … | … | A | … | … | … | … | … | … | … |
| First name(s) | A | A | B | … | … | … | A | … | … | … | … | … | … | … |
| Date of birth |  | A | A | … | … | … | A | … | … | … | … | … | … | … |
| Nationality |  | A | A | … | … | … | B | … | … | … | … | … | … | … |
| … | … | … | … | … | … | … | … | … | … | … | … | … | … | … |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| II. Dossier information |
| Dossier keeper | B | B | B | … | … | … | A | … | … | … | … | … | … | … |
| Dossier status | B | B | B | … | … | … |  | … | … | … | … | … | … | … |
| Reference number | A | B | B | … | … | … | B | … | … | … | … | … | … | … |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| III. Title X |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Access levels**

A = Query

B = Processing

empty = no access

other

**Organisational units**

OU I: e.g. legal service of the relevant OU

OU II: e.g. case officer of the OU concerned

OU III: e.g. administrator of the OU concerned

…

Cant. Office: e.g. cantonal police authorities

…

## List of documents

Includes a list of all acts, ordinances, directives, regulations, technical specifications, etc. relevant to the data collection in question. The list must be supplemented (extended) by the department's and/or office's own documents.

|  |  |
| --- | --- |
| Type of document | Title |
| Acts | Legal basis for the asset (to be completed by the author) |
|  | [Federal Act of 25 September 2020 on Data Protection (Data Protection Act; FADP; SR 235.1)](https://www.fedlex.admin.ch/eli/cc/2022/491/de) |
|  | [Federal Act of 17 December 2004 on Freedom of Information in the Administration (Freedom of Information Act, FoIA; SR 152.3)](http://www.admin.ch/ch/d/sr/c152_3.html) |
|  | [Federal Act of 26 June 1998 on Archiving (Archiving Act, ArchA; SR 152.1)](http://www.admin.ch/ch/d/sr/c152_1.html) |
| Ordinances | [Ordinance of 25 November 2020 on the Coordination of the Digital Transformation (DTIO; SR 172.010.58)](https://www.fedlex.admin.ch/eli/cc/2020/988/de) |
|  | [Ordinance of 31 August 2022 on Data Protection (Data Protection Ordinance, DSV; SR 235.11)](https://www.fedlex.admin.ch/eli/cc/2022/568/de) |
|  | [Ordinance of 4 July 2007 on the Protection of Federal Information (Information Protection Ordinance, IPO; SR 510.411)](https://www.fedlex.admin.ch/eli/cc/2007/414/de) |
|  | [Ordinance of 22 November 2017 on the Protection of Personal Data relating to Federal Personnel (FPDO; SR 172.220.111.4)](https://www.fedlex.admin.ch/eli/cc/2017/793/de) |
|  | [Ordinance of 27 May 2020 on Protection against Cyber Risks in the Federal Administration](https://www.fedlex.admin.ch/eli/cc/2020/416/de) (Cyber Risks Ordinance, CyRO) |
| Strategies | [SN002 - National Strategy for the Protection of Switzerland against Cyber Risks (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) |
|  |  |
| Own Documents | Authorisation concept |
|  | Data flow diagram |
|  | IT architecture structure |
|  | … |

## Abbreviations

|  |  |
| --- | --- |
| Abbreviation | Meaning |
| Art. | Article |
| DPA | Data protection Advisor |
| DPO | Ordinance on Data Protection (SR 235.11) |
| FADP | Federal Data Protection Act (SR 235.1) |
| FDPIC | Federal Data Protection and Information Commissioner |
| FOJ | Federal Office of Justice |
| ICT | Information and communication technology |
| ITSOO | Information Security Officer of the Organisational Unit |
| ISDP concept | Information security and data protection concept |
| let. | letter |
| NCSC | National Cyber Security Centre |
| OU | Organisational unit |
| para. | paragraph |
| PL | Project leader |
| PL SR | Project leader Service recipients |
| … | … |

## Terms

|  |  |
| --- | --- |
| Term | Definition |
| Processing | Any handling of personal data, irrespective of the means and procedures used, in particular the collection, storage, keeping, use, modification, disclosure, archiving, deletion or destruction of data (see Art. 5 let. d FADP). |
| Disclosure | Transmitting personal data or making such data accessible (Art. 5 let. e FADP). |
| Sensitive personal data | Data relating to religious, philosophical, political or trade union-related views or activities; health, the private sphere or affiliation to a race or ethnicity; genetic data; social assistance measures; and administrative and criminal proceedings or sanctions (Art. 5 let. c FADP). |
| Breach of data security | A breach of security that leads to the accidental or unlawful loss, deletion, destruction or modification or unauthorised disclosure or access to personal data (Art. 5 let. h FADP). |
| Controller | Private person who or federal body which, alone or jointly with others, determines the purpose and the means of processing personal data (Art. 5 let. j FADP). |
| Processor | Private person or federal body that processes personal data on behalf of the Controller (Art. 5 let. k FADP). |
| Personal data, data subject | Any information relating to an identified or identifiable natural person (Art. 5 let. a and b FADP). |
| Profiling | Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (Art. 5 let. f FADP). |
| High risk profiling | Profiling that poses a high risk to the data subject's personality or fundamental rights by matching data that allow an assessment to be made of essential aspects of the personality of a natural person (Art. 5 let. g FADP). |
| … | … |

1. **Art. 34** Legal basis:
2 A statutory basis in a formal law is required in the following cases:
c. The purpose or manner of the data processing **may lead to a serious violation of the data subject's fundamental rights**. [↑](#footnote-ref-1)