[SGPD] DATA PROCESSING REGULATIONS V2

Plan-les-Ouates, August 21th 2018

SUMMARY

[SGPD] data processing regulations V2 1

1 GENERAL PROVISIONS 3

1.1 Applicable law 3

1.2 Premise of the data processing regulations 3

1.3 Data processing principles 3

1.4 Scope 4

1.5 DFi Employee and Agent Employee Duties 4

2 STRUCTURE OF DFI'S INFORMATION SYSTEM 5

2.1 Composition of DFi's Information System 5

2.2 Organisational chart 6

2.3 Resposabilities 7

2.4 Data processors 7

2.4.1 Operating segments 7

2.5 Interfaces 7

3 DATA PROCESSING / TYPES OF DAT 8

3.1 Data collected 8

3.2 Categories of data 8

3.3 Data communication 8

3.3.1 Data are regularly communicated for the purpose of 8

3.3.2 These data may be communicated in particular 9

4 Time limits on storing data, data removal 9

5 Documentation relating to the planning, building and operation of the Information System 9

6 Registration of files with the Swiss Data Protection Authority (PFPDT) (art. 16 of OLPD) 10

7 Process 10

8 CONTROL PROCEDURES AND TECHNICAL AND ORGANISATIONAL MEASURES 10

8.1. Access controls 10
8.2. Personal data media controls 10
8.3. User authentication 11
8.4. Transportation and transmission controls 11
8.5. Communication controls 11
8.6. Memory controls 11
8.7. User controls 11
8.8. Access controls 11
8.9. Entry controls 11
8.10. Software development 12
8.11. Supervision and responsibility 12
9 DESCRIPTION OF DATA FIELDS AND ORGANISATIONAL UNITS WITH ACCESS TO THEM 12
10 NATURE AND SCOPE OF USER ACCESS TO THE INFORMATION SYSTEM 12
10.1 Users 12
10.2 Managing access permissions 12
10.3 Management software access controls 13
10.4 Access to office documents 13
10.5 Access by employees working remotely (on-call) 13
10.6 Control of access to data available on extranet platforms 14
11 DATA SUBJECT RIGHTS 14
12 CONFIGURATION OF I.T. RESOURCES 14
13 FINAL PROVISIONS 15
13.1 Annexes 15
13.2 Regulation drafts and amendments 15
13.3 Entry into force 15
13.4 Publication 15
ANNEX 1 15
ANNEX 2 15
ANNEX 3 16

1 GENERAL PROVISIONS

1.1 Applicable law

- Federal Data Protection Act of 19 June 1992 (LPD)
- Decree of 14 June 1993 relating to the Federal Data Protection Act (OLPD)
- The Federal Act on the Surveillance of Postal Correspondence and Telecommunications (LSCPT)
- The Federal Decree on the Surveillance of Postal Correspondence and Telecommunications (OSCPT)
- GDPR – General Data Protection Regulation (UE 2016/679) which sets out the obligation of the Trust data regarding data protection and people's rights in respect of their personal data

1.2 Premise of the data processing regulations

According to articles 11 and 21 of the OLPD, the purpose of these data processing regulations is to provide transparent information on data processing carried out as part of the administrative management offered by DFi to its employees and customers.

1.3 Data processing principles

The purpose of gathering arises from the provisions of the employment contract and contracts with our customers.

In accordance with the consent given by the employee and customer, DFi is responsible for applying and enforcing the principles of the LPD. As such it is approved to process and arrange for the processing of personal data, including sensitive data and personality profiles needed by them in order to perform administrative tasks such as processing Human Resources and processing Commercial relations.

The processing of personal data is subject to the legal principles on data protection:

Lawfulness: processing must have a legal basis (law, decree, statutes, regulations, terms and conditions or equivalent) or be carried out with the consent of the data subjects.
Principle of good faith: Processing must be carried out in accordance with the principle of good faith. The collection of personal data must not be carried out without the knowledge of the data subject, nor against their will.
Proportionality: The processing must be appropriate, i.e. proportionate to the intended aim and must be restricted to what is necessary to meet the objective set.

Purpose: The personal data may only be processed for the purpose stated when collected and in the circumstances determined by law, statutes or the applicable regulations.
Recognisable collection: The collection of personal data and, in particular the purposes of processing, must be recognisable by the data subject; the purposes of processing must be stated at the time of collection; they may also be a result of circumstance.
Accuracy: Personal data must be complete and as current as circumstances allow. The data subject may request the rectification of inaccurate data.
Data security: Data must be protected by appropriate technical and organisational measures against loss and unauthorised processing.
The data subject's rights: The subjects of any data processed by DFi are entitled to be aware of these and, where relevant, to secure their correction or removal. Data shall only be removed insofar as this does not affect proper contract management.

1.4 Scope

This agreement applies to data processed by DFi in managing its Human Resources and Commercial Relations.

1.5 DFi Employee and Agent Employee Duties

DFi employees means individuals bound by either a permanent or temporary employment contract with DFi. DFi agent employees means individuals bound by an employment contract with an agent of DFi.

NON-DISCLOSURE REQUIREMENT

Individuals processing the data of employees and customers managed by DFi as part of an employment contract or a DFi service agreement are required not to disclose any information obtained in exercising their duties, in particular in relation to sensitive Human Resources data.

The non-disclosure requirement shall continue to apply following the termination of the employment contract or the contract with the agent or the specific contract. This requirement is included in the contractual documents relating to the commitment or the contract with the agent or the specific contract.

This requirement forms an integral part of DFi's employment contracts, the regulations of staff responsible for determining the employee's duties as well as terms and conditions with third parties (Suppliers), non-disclosure agreements and DFi's General Terms and Conditions of Sale.

2 STRUCTURE OF DFI'S INFORMATION SYSTEM

2.1 Composition of DFi's Information System

1. Technical management system

2. Human Resources management system

3. Business management system (performance charts)

4. Financial management system

   - Accounting and office overhead expenses sub-system
   - Customer financial management sub-system
   - Dispute management sub-system

5. Messages and communications management system

   - Electronic exchange management system
   - Email management sub-system
   - Telephone and fax management sub-system

6. Document management system

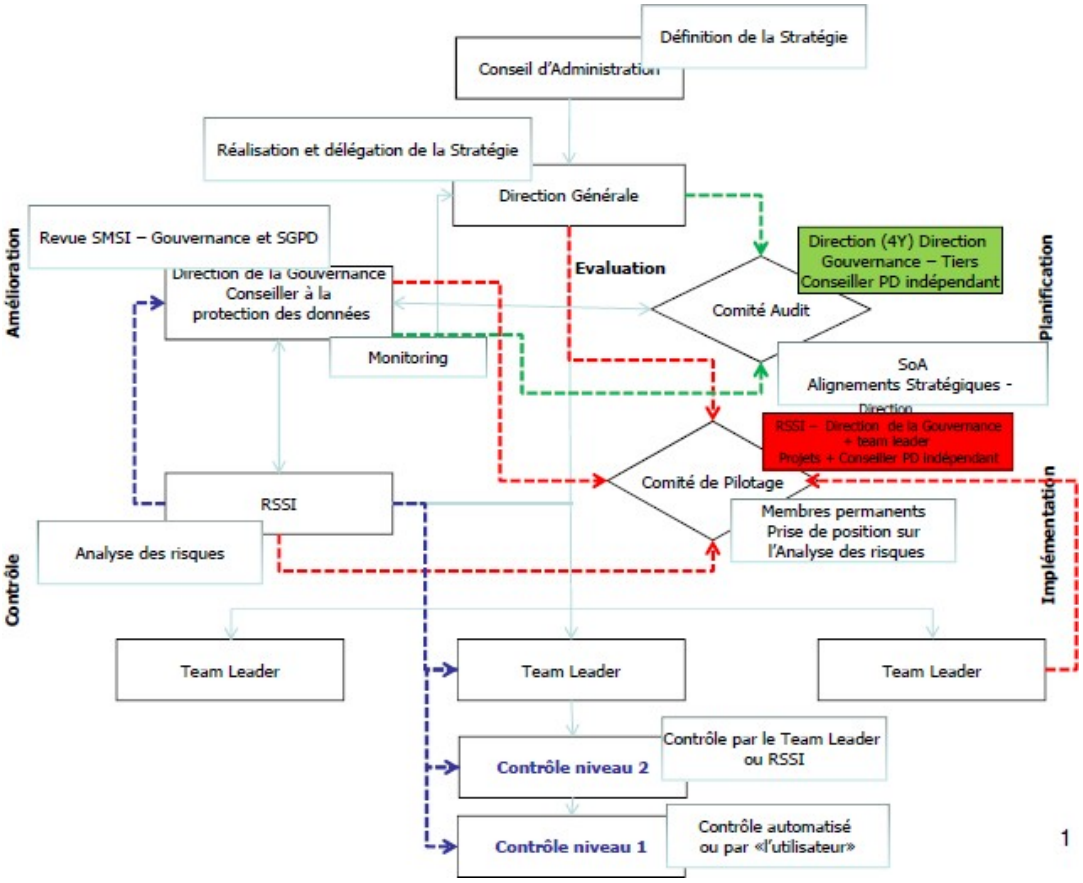
   - Document indexing sub-system
   - Document archiving sub-system (hard copies)

7. Intranet/extranet management system

8. I.T. processing management system

   - I.T. development sub-system
   - Telecommunication network management for DFi services sub-system
   - Security management sub-system

2.2 Organisational chart



2.3 Resposabilities

DFi management is responsible for data protection and security. On issues relating to data protection law, it takes advice from the in-house counsel and independent counsel specialising in data protection.

The table contains a breakdown of roles and responsibilities:

Role	Responsibility
General data protection, SGPD and training	Counsel specialising in data protection and Data Management and Protection System manager and Information Systems Security manager
Requests to access and view files	Management, Human Resources
Technical security of data	Information Systems Security Manager
Access profiles	Human resources, Director of Governance and Information Systems Security Manger
Destruction of electronic data	Management and Information Systems Security Manager

2.4 Data processors

2.4.1 Operating segments

Employees working in the segments below have access to DFi's Information System in order to manage Human Resources and for Commercial relations:

1. Human Resources Segment
2. Commercial relations segment
3. Accounting and Finance
4. Management Team

2.5 Interfaces

Several interfaces are used to process employee data.
Several interfaces are used to communicate directly with employees and customers. Interfaces exist for use by our customers to access their customer accounts online.
In principle, the data are transmitted electronically or in hard copy through a strong system of authentication, encryption and advanced data transmission technologies, data protection and security is guaranteed.

3 DATA PROCESSING / TYPES OF DAT

3.1 Data collected

EMPLOYEES

Data are mainly from employees themselves, individuals authorised by employees (former employer, AVS federal old-age, survivors and disability insurance officials, criminal record checks) public offices etc.

CUSTOMERS

Data are mainly from the customers themselves and data in the public domain (internet or federal pubic records).

3.2 Categories of data

Annex 1 lists categories of employee data included in the inventory of files in DFi's Information System. Annex 2 lists categories of customer data included in the inventory of files in DFi's Information System.

3.3 Data communication

Data can be communicated if authorised by the employee or customer by contractual consent, if there is a legal basis or if the communication is in the public interest.

3.3.1 Data are regularly communicated for the purpose of

EMPLOYEES

Drawing up compulsory insurance contracts
Paying salaries
Producing internal and federal statistics
Checking data accuracy

CUSTOMERS

Drawing up DFi service agreements
Issuing invoices for DFi services
Producing internal and federal statistics
Checking data accuracy

3.3.2 These data may be communicated in particular

IN THE CASE OF EMPLOYEES TO

- DFi human resources
- Authorities (pension and disability schemes, unemployment benefits etc.)
- Insurers
- Courts
- In specific cases, and upon written request setting out the grounds, to the relevant social welfare authorities, civil courts, penal courts and criminal prosecution authorities, the prosecution service an the Federal Intelligence Service (SRC).

IN THE CASE OF CUSTOMERS TO

- All DFi employees
- Authorities (OfCom, VAT etc.)
- Courts
- In specific cases, and upon written request setting out the grounds, to the relevant social welfare authorities, civil courts, penal courts and criminal prosecution authorities, the prosecution service an the Federal Intelligence Service (SRC).

4 TIME LIMITS ON STORING DATA, DATA REMOVAL

The length of time data may be stored is based on Swiss law in this area. Beyond the legal time limit for data storage, the data in DFi's Information System must be destroyed.

5 DOCUMENTATION RELATING TO THE PLANNING, BUILDING AND OPERATION OF THE INFORMATION SYSTEM

Files containing documentation relating to the planning, building and operation of DFi's Information Systems and subsystems are stored by the Governance Division.

6 REGISTRATION OF FILES WITH THE SWISS DATA PROTECTION AUTHORITY (PFPDT) (ART. 16 OF OLPD)

The in-house counsel on data protection keeps an inventory of data files to be made available to the PFPDT.

7 PROCESS

The collection, processing and transmission of data from DFi's Information System are based on processes. These are documented and internal to DFi.

8 CONTROL PROCEDURES AND TECHNICAL AND ORGANISATIONAL MEASURES

8.1. Access controls

All DFi premises in which sensitive personal data are processed are protected electronically and/or manually against access by unauthorised third parties.
Access to DFi premises is only granted to employees identified by biometric recognition. Visitors are asked to go to DFi reception to sign in and be given a visitor badge.
Access rights are granted according to the position and job title of the employee. They vary in scope. Moreover, access is managed on a site by site basis and may be granted on a temporary basis. Any access or attempted access is logged by the access management software.
CCTV and alarm systems are managed only in the Data Centres by the Data Centres.
Certain premises may be accessed with a badge given to the employee. Each badge is identified and a record of badges given to employee is kept.
Access to Data Centres is protected by a strong system of authentication, identify checks and CCTV. Anyone accessing these premises, along with the time, may be identified using access logs.

8.2. Personal data media controls

Only duly authorised individuals may access DFi's Information System and only authorised individuals may process data saved on electronic media.

8.3. User authentication

Access to the modules of DFi's Information System is only possible for those with the necessary means of authentication.

8.4. Transportation and transmission controls

Appropriate technical measures are in place to secure the transmission of data so that unauthorised individuals may not read, copy, amend or delete data during its transmission or the transportation of data media.

8.5. Communication controls

Data recipients who access personal data using data communication equipment are identified, particularly in the case of service providers who access Human Resources data, our customers' data and technical data from our telecommunication system.

8.6. Memory controls

Technical measures are in place to prevent unauthorised individuals from entering data in the memory or having access to memorised data, amending or deleting it.

8.7. User controls

Only terminals approved by DFi may be connected to DFi’s information network.

8.8. Access controls

Authorised individuals only have access to the data needed to perform their tasks. The nature and scope of user access to the database are described in these regulations.

8.9. Entry controls

In addition to controlling access to DFi's Information System, automated processing of data are logged to allow retrospective checking that the data was processed in accordance with the purposes for which it was collected or communicated. Logs are stored in a format that meets auditing requirements. They are accessible only by organisations or individuals responsible for checking the enforcement of provisions on data protection and used only for this purpose.

8.10. Software development

Development, test and production environments are all kept strictly separate.

8.11. Supervision and responsibility

Data controllers ensure that users act in accordance with instructions, these Processing regulations and annexes.

9 DESCRIPTION OF DATA FIELDS AND ORGANISATIONAL UNITS WITH ACCESS TO THEM

DFi Information System permissions are controlled using a system of access permissions.

10 NATURE AND SCOPE OF USER ACCESS TO THE INFORMATION SYSTEM

10.1 Users

The individuals authorised to access DFi's Information System are:
1. DFi employees.
2. DFi system administrators.

10.2 Managing access permissions

The purpose of Information System security is to ensure the confidentiality, integrity and availability of information. An important factor in security is the concept of access management which comprises two strands: physical access, allowing a user to access the various buildings and premises belonging to the company, and logical access, which allows him or her to log into the systems and software to access the information they need.

10.3 Management software access controls

Employee and customer data are managed on separate I.T. platforms.
Logical access is managed, on the one hand by the I.T. segment in the case of standard software and, on the other hand, by the business lines for certain specific software. An initial workflow allows each new employee to be authenticated. Further access can then be requested. A validation workflow allows managers to accept or reject the requests. Access management is based on the 'least privilege' principle, i.e. an employee will only have access to the information relevant to his or her tasks. Under this principle, initially any access is locked and permissions are only granted on request.

When an employee leaves the company, his or her permissions are removed and it is no longer possible for the employee to log into the logical systems, nor to access the premises.

10.4 Access to office documents

Data managed by the various DFi management software applications may be transferred to office files. These working documents are saved in an office directory specific to each DFi segment. The line management determines permissions to access this directory based on the employee's position. Permissions are managed (allocation, amendment, removal) by DFi's Head of Information System Security who assigns each employee to a group of users authorised to access the data saved in each directory. Access to documents saved in the office directories may be logged. Access to the audit logs generated will in this case be restricted to employees of the I.T. segment responsible for the security of the Information System.

10.5 Access by employees working remotely (on-call)

DFi has employees who may be on-call from home. This involves being available for DFi outside business hours to work on DFi's Information System in the event of anomalies. Access to software from home is governed by the same principles as those which apply to employees working on-site. Logging into DFi’s Information System is through a strong authentication method.

10.6 Control of access to data available on extranet platforms

A restricted amount of personal data are made accessible on DFi's extranet platforms. Access to these by authorised individuals is protected by a method of strong authentication.

11 DATA SUBJECT RIGHTS

Requests for access in accordance with article 8 of LPD must be sent in writing to DFi's Data protection department along with proof of identity (copy of official document, with photo) to the following address:

DFi Service SA
Service protection des données
Ch. Des Aulx 18
1228 Plan-les-Ouates

Using the following forms:

• on the website www.dfi.ch under contact for customer data

• in the internal tool of documentation for the collaborators under form of request of the data collaborator

12 CONFIGURATION OF I.T. RESOURCES

Computer hardware and software used at DFi meets technical standards.

Documentation on the configuration of I.T. resources used for DFi's Information System are stored in the I.T. segment or with external suppliers/partners.

For security reasons, no information is supplied about the configuration of I.T. resources.

13 FINAL PROVISIONS

13.1 Annexes

The annexes form an integral part of these regulations

13.2 Regulation drafts and amendments

Processing regulations are regularly updated by the data controller in accordance with the provisions of art. 11 of the 'OLPD. These regulations may be amended at any time. Amendments must be submitted in writing and approved by DFi Management.
The processing regulations are drafted by the Counsellor on data protection and the head of the Data protection management system and overseen by an external lawyer, an independent counsel specialising in data protection for DFi.
Responsibility for amending these regulations lies with the Governance Division.

13.3 Entry into force

These regulations are effective immediately.

13.4 Publication

These regulations and annexes are published on-line at www.dfi.ch.

ANNEX 1

Categories of data based on the inventory of DFi employee files (Internal access only). Including: Categories of personal data processed (Art. 3, paragraph 1, letter e of OLPD)

ANNEX 2

Categories of data based on the inventory of DFi customer files (Internal access only or upon the customer's request).

Including: Categories of personal data processed (Art. 3, paragraph 1, letter e of OLPD)

ANNEX 3

List of undeclared files affected by data protection (Internal access only)

Including: Categories of personal data processed (Article 3, paragraph 1, letter e OLPD)

DFi Service SA
Chemin des Aulx 18
1228 Plan-les-Ouates
Geneva - Switzerland

Tel. +41 22 706 2288
Fax +41 22 794 8519
www.dfi.ch