[SGPD] GLOBAL DATA PROCESSING POLICY V2

Plan-les-Ouates, August 15th, 2018

TABLE OF CONTENTS

DFi Service SA
Chemin des Aulx 18
1228 Plan-les-Ouates
Genève – Suisse

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

1 GENERAL PROVISIONS

1.1 Applicable laws

- Federal Act on Data Protection, June 19th 1992 (FADP- LPD in French)
- Ordinance to the Federal Act on Data Protection, June 14th 1993 (DPO- OLPD in French)
- Federal Act on the Surveillance of Post and Telecommunications (SPTA- LSCPT in French)
- Ordinance on the Surveillance of Post and Telecommunications (SPTO- OSCPT in French)
- GDPR - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regards to the processing of personal data and on the free movement of such data

1.2 Starting Point of this Processing Policy

According to Art. 11 and 21 DPO, the purpose of these Processing Policy is to provide transparent information about its data processing carried out in the context of the administrative management offered by DFI to its employees and customers.

1.3 Principles in data processing

The purpose of the data collection is based on the provisions of the employment contract and the contracts with our customers.
In accordance with the consent of the employee and the customer, DFI is responsible for implementing the principles of the FADP and monitoring its implementation, and is therefore entitled to process and have processed the personal data, including sensitive data and personality profiles, which are necessary for the performance of the administrative tasks, namely the processing of Human Resources and the processing of Business Relations.
Personal data processing is subject to the following legal principles of data protection:
Lawfulness: processing must be based on a legal basis (law, ordinance, statutes, regulations, general conditions or equivalent) or 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. Personal data may not be collected without the knowledge or against the will of the data subject.
Proportionality: processing must be adequate, i.e. proportional to the purpose and limited to what is necessary to achieve the purpose.
Purpose: personal data may only be processed for the purpose indicated at the time of collection, arising from the circumstances provided for by the law, the statutes or the

applicable regulations.
Recognizable collection: the collection of personal data, and in particular the purposes of the processing, must be recognizable to the concerned person; the purposes of the processing must be indicated at the time of collection of the data; they may also derive from the circumstances.
Accuracy: personal data must be complete and as up-to-date as circumstances allow. The data subject may request the rectification of inaccurate data.
Data security: data must be protected by appropriate technical and organizational measures against loss and unauthorized processing.
Rights of the data subjects: the persons whose data are processed by DFI have the right to know the data and, if necessary, to have them corrected or deleted. The deletion of data is only carried out if this does not affect the proper management of the contract.

1.4 Scope of application

This policy applies to the processing of data by DFI for the purpose of Human Resources management and for the management of its Business Relations.

1.5 Obligations of DFI employees and its agents

Employees of DFI include both persons with permanent employment contracts and persons with fixed-term employment contracts with DFI. Furthermore, employees of DFI agents are persons who have an employment contract with a company commissioned by the DFI.
Obligation to maintain secrecy
Persons who process data of employees and manage clients in DFI within the framework of an employment contract or a services contract with DFI are obliged to maintain secrecy with respect to third parties on all information they learn during their professional activity, in particular with respect to data of a sensitive nature in the field of Human Resources.
The obligation to maintain secrecy continues to apply after the end of the employment contract or a mandate or a specific contract. This obligation is included in the contractual agreements relating to employment, mandate or specific contract.
This obligation is an integral part of DFI's employment contracts, the personnel policy setting out the duties of the employee, as well as the general conditions with third parties (suppliers), the confidentiality agreements, and DFI's General Business Conditions.

2 STRUCTURE OF THE INFORMATION SYSTEM OF DFI

2.1 Components of the information system of DFI

1. Technical management system
2. A Human Resources management system
3. Business monitoring system (dashboards)
4. Financial management system

- Sub-system of accounting and expense management
- Sub-system of customer financial management
- Sub-system of litigation management

5. Messaging and Communications Management System

- Sub-system of Electronic Exchange Management
- Sub-system of Email Management
- Sub-system of Telephony and Fax Management

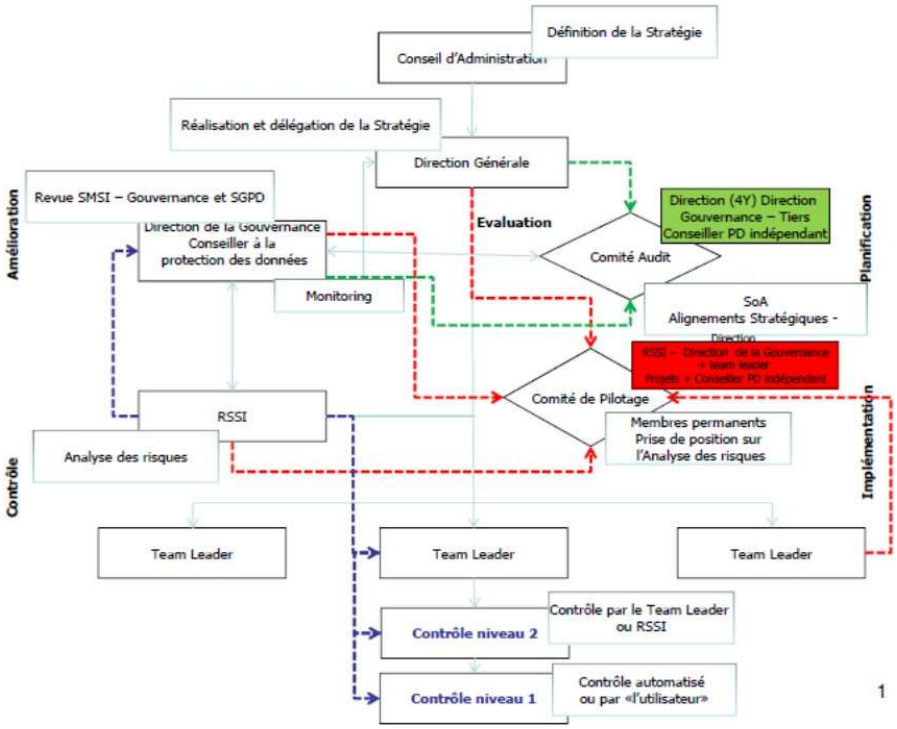
6. Document management system

- Sub-system of Document indexing Management
- Sub-system of Document archiving (paper)

7. Internet / Extranet Management system
8. IT operations Management system

- Sub-system of IT development
- Sub-system of Telecommunication network Management for DFI services
- Sub-system of Security Management

2.2 Organization chart



2.3 Responsabilities

The DFI management is responsible for data protection and data security. It is advised in matters of data protection law by the Internal Advisor and an independent Data Protection Advisor.
The table below describes the roles and responsibilities:

Role	Responsability
Data protection in general, SGPD and education	Independent Data Protection Advisor Conseiller indépendant à la protection des données, Processing and IT Security Officer
Requests for access and files consultation	Executive Management, HR
Technical Data security	IT Security Officer
Acces profiles	HR, Governance Manager and IT Security Officer
Electronic Data Destruction	IT Security Officer and IT Security Officer

2.4 Data Processing Participants

2.4.1 Operational areas

Employees in the following areas have access to the DFI Information System in order to manage Human Resources and Business Relationship Management:
1. Human Resources
2. Commercial Relations
3. Accounting & Finance
4. Executive Management

2.5 Interfaces

Several interfaces allow the processing of employee data.
Several interfaces allow direct contact with employees and customers.
There are interfaces that allow our customers to access their customer accounts online (via the Internet). In principle, data is transmitted electronically or on paper by means of a strong authentication system, encryption and advanced data transmission technologies, data protection and security are guaranteed.

3 DATA PROCESSING / TYPES OF DATA

3.1 Collected data

Employees:
The data mainly comes from the employees themselves, persons authorized by the employees (former employer, social security nr, criminal record extract...) administrations, etc.
Clients :
The data comes mainly from the customers themselves, and from public domain available data (public Internet or federal public registers).

3.2 Data categories

Appendix 1 lists the categories of employee data in the DFI Information System file inventory.
Appendix 2 identifies the categories of client data contained in the DFI Information System file inventory.

3.3 Data disclosure

Data is disclosed on the basis of an authorization from the employee or client, based on contract consent, a legal basis or if the disclosure meets an overriding public interest.

3.3.1 Data is regularly disclosed for

For employees to :
Establish mandatory insurance contracts
Payrolls
Drawing up internal and federal statistics Checking the accuracy of data
Clients:
Draw up contracts for DFI services Draw up invoices for DFI services Draw up internal and federal statistics
Verify the accuracy of data

Clients:
Establish DFI services contracts
Establish DFI invoices
Establish internal and federal statistics
Verify the accuracy of data

3.3.2 This data may be communicated in particular

For employees to :

- DFI HR;
- authorities (social security agencies, etc.);
- insurance companies;
- courts;
- in individual cases and upon written and motivated request to the competent authorities for social assistance, civil courts, criminal courts and criminal investigation bodies, prosecution offices, the Federal Intelligence Service (SRC).

For clients to :

- all DFI employees
- authorities (OfCom, VAT, etc.);
- courts;
- in individual cases and upon written and justified request to the authorities responsible for social welfare, civil courts, criminal courts and criminal investigation bodies, prosecution offices, the Federal Intelligence Service (FIS).

4 DATA RETENTION PERIOD, DATA DELETION

The data retention period is based on the specific provisions of Swiss law. After the legal retention period has expired, the data must be deleted from the DFI Information System.

5 PLANNING DOCUMENTATION, IMPLEMENTATION AND OPERATION OF THE INFORMATION SYSTEM

The planning, implementation and operational documentation files for the DFI's information systems and sub-systems are kept by the Governance Management.

6 FILE REGISTER TO THE COMMISSIONER (ART. 16 OLPD)

The Independent Data Protection advisor makes an inventory of the Data files that he keeps available to the Commissioner.

7 PROCESSES

The collection, processing and transmission of Data in the DFI Information System are based on processes. These processes are documented and are internal to DFI.

8 CONTROL PROCEDURES, TECHNICAL AND ORGANIZATIONAL MEASURES

8.1. Access control

All DFI premises where sensitive personal data is processed are electronically and/or manually protected against access by any unauthorized third party. Access to DFI premises is only granted to employees identified by biometric recognition.
Visitors are required to announce themselves to the DFI reception desk to be registered and recieve a "visitor" badge.
Access rights are assigned according to the employee's function and title. There access is consequently more or less extensive. In addition, access is managed by site and access can be temporary. All accesses or access attempts are logged by the access management software.
Video surveillance and alarm systems are managed only in the Data Centers and by the Data Centers.
Some premises can be accessed using a badge provided to the employee. Each badge is identified and are registered and kept up to date.
Access to the Data Centers is protected by a strong authentication system, identity verification, and video surveillance. Access logs identify who has accessed the premises and when.
Authorized persons have access only to the data they need to perform their duties. The nature and extent of access by users of the file are described in this policy.

8.2. Control of personal data supports

Only duly authorized persons are granted access to the DFI Information System and only authorized persons may process data stored on electronic media.

8.3. User authentication

Access to the modules of the DFI Information System is only possible with the necessary means of authentication.

8.4. Transport control

Appropriate technical measures are put in place to secure the transmission of data so that unauthorized persons cannot read, copy, modify or delete data during communication or during the transport of data carriers.

8.5. Communication control

Data recipients who access personal data by means of data transmission facilities are identified, in particular service providers who access our Human Resources data, client data and technical data from our telecommunications system.

8.6. Memory control

Appropriate technical measures are taken to ensure that unauthorized persons cannot enter data into the memory or access, modify or delete stored data.

8.7. Control of use

Only terminals approved by the DFI may be connected to the DFI computer network.

8.8. Access control

Authorized persons have access only to the data they need to perform their tasks. The nature and extent of access by users of the file are described in these regulations.

8.9. Entry Control (logging)

In addition to the access control to the DFI Information System, automated data processing is subject to logs so that it is possible to verify a posteriori that the data has been processed in accordance with the purposes for which it was collected or communicated. The logs are kept in a form that meets the audit requirements. They are accessible only to the bodies or persons responsible for verifying the application of the provisions on personal data protection and are used only for this purpose.

8.10 Application development

The development, test and production environments are strictly separated.

8.11 Supervision and responsibility

The data processor ensures that users comply with the instructions, these policies and its annexes.

9 DATA FIELDS AND ORGANIZATIONAL UNITS THAT HAVE ACCESS TO THEM

Access rights to the DFI information system are regulated by means of an access authorization system.

10 NATURE AND SCOPE OF USER ACCESS TO THE INFORMATION SYSTEM

10.1 Users

The persons authorized to access the DFI Information System are:
1. DFI employees.
2. DFI system administrators.

10.2 Management of access rights

The purpose of Information System Security is to ensure the confidentiality, integrity and availability of information. An important component of security is based on the notion of access management, which has two main components: physical access, which allows a user to access the company's various buildings and premises, and logical access, which allows the user to connect to systems and applications to access the information he or she needs.

10.3 Access control to business applications

Employee and customer data are managed on separate and distinct IT platforms.
Logical access is managed on the one side by the IT department for standard applications and on the other by the assigned one on specific applications. An initial workflow is used to assign an authentication to each new employee. Additional access can then be requested. A validation workflow allows managers to accept or reject the requests made. Access management is based on the principle of least privilege, i.e. an employee will only have access to those elements that are relevant for the performance of his or her tasks. The principle is that initially all access is locked and rights are only granted on request.
When an employee leaves the company, the accesses are deleted and it is no longer possible for the employee to log in to the logical systems or to access the premises.

10.4 Access to office documents

The data managed through the various DFI management applications can be transferred to office files.
These working documents are stored in an office directory specific to each DFI sector. The line manager defines the access rights to this directory on the basis of the employee's function. Rights management (allocation, modification, deletion) is ensured by the DFI IT Security Manager who assigns each employee to a group of users authorized to access the data stored in each directory.
Access to documents stored in the office directories can be logged. Access to the generated audit logs will in this case be limited to the IT staff responsible for the security of the information system.

10.5 Access for employees working from home (restricted)

The DFI has employees who can work from home on restricted duties. This activity consists of making themselves available to DFI outside business hours to intervene on the DFI information system in case of anomalies. Access to the applications from home is governed by the same principles as for employees working on site. The connection to the DFI's system is done through a strong authentication method.

10.6 Controlling access to data available on Extranet platforms

A limited amount of personal data is made available on DFI's Extranet platforms. Access by authorized persons is protected by a strong authentication method.

11 RIGHTS OF THE CONCERNED PERSONS

Requests for access in accordance with Art. 8 FADP must be addressed in writing to the DFI Data Protection Department, accompanied by proof of the applicant's identity (copy of an official certificate, with photo), to the following address :

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

By means of the following forms:

- on the website www.dfi.ch under the contact heading pour les données client
- in the internal documentation tool for employees under Employee data request form

12 CONFIGURATION OF IT RESOURCES

The hardware and software used by DFI correspond to the technical standards.

Documentation on the configuration of the IT resources used for DFI's information system is kept in the IT department or with external suppliers/partners.

For security reasons, no information is provided on the configuration of the IT resources.

13 FINAL PROVISIONS

13.1 Annexes

The mentioned annexes of the present policy are an integral part of this policy.

13.2 Preparation and amendment of this policy

The policies are regularly updated by the processor in accordance with the provisions of Art. 11 of the DPO.
This policy may be amended at any time. Amendments must be made in writing and approved by the DFI Executive Management.
The processing regulations are drawn up by the Independent Data Protection Advisor and the processor.
The responsibility for amending the policy lies with the Governance Management.

13.3 Entry into force

This policy comes into force immediately.

13.4 Publication

This policy and their annexes are published on the Internet at www.dfi.ch.

ANNEX 1

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

ANNEX 2

Categories of data based on the inventory of DFI's customer files. (Access only internal or upon request of the client).
Including: Categories of personal data processed (Art. 3, paragraph 1, letter e DPO)

ANNEX 3

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

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

DFi Service SA
Chemin des Aulx 18
1228 Plan-les-Ouates
Genève – Suisse

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