[SGPD] RÈGLEMENT GLOBAL DE TRAITEMENT DES DONNÉES V2

Plan-les-Ouates, le 15 Août 2018

TABLE DES MATIERES

1 DISPOSITIONS GÉNÉRALES

1.1 Droit applicable

- Loi fédérale du 19 juin 1992 sur la protection des données (LPD)
- Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD)
- Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT)
- Ordonnance fédérale sur la surveillance de la correspondance par poste et télécommunication (OSCPT)
- RGPD - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

1.2 Point de départ du Règlement de traitement

Selon les art. 11 et 21 OLPD, le présent règlement de traitement a pour objectif de fournir une information transparente quant au traitement des données effectué dans le cadre de la gestion administrative offerte par DFI à ses collaborateurs et ses clients.

1.3 Principes du traitement des données

Le but de la récolte des données ressort des dispositions du contrat de travail et des contrats avec nos clients.
Conformément à l'obtention d'un consentement du collaborateur et du client, DFI est chargée d'appliquer les principes de la LPD et d'en surveiller l'exécution, ainsi elle est habilitée à traiter et à faire traiter les données personnelles, y compris les données sensibles et les profils de la personnalité, qui leur sont nécessaires pour accomplir les tâches administratives à savoir le traitement des Ressources Humaines et le traitement des Relations Commerciales.
Le traitement des données personnelles est assujetti aux principes juridiques suivants en matière de protection des données :
Licéité: le traitement doit être fondé sur une base légale (loi, ordonnance, statuts, règlement, conditions générales ou équivalent) ou effectué avec le consentement des personnes concernées.
Principe de la bonne foi: le traitement doit être réalisé selon le principe de la bonne foi. La collecte des données personnelles ne peut être effectuée sans que la personne concernée en ait connaissance, ni contre son gré.
Proportionnalité: le traitement doit être adéquat, c'est-à-dire proportionnel au but visé et se limiter à ce qui est nécessaire pour atteindre l'objectif fixé.

Finalité: les données personnelles ne peuvent être traitées que dans le but indiqué lors de leur récolte, découlant des circonstances prévues par la loi, les statuts ou les règlements applicables.
Collecte reconnaissable: la collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée; les finalités du traitement doivent être indiquées lors de la collecte des données; elles peuvent aussi découler des circonstances.
Exactitude: les données personnelles doivent être complètes et aussi actuelles que les circonstances le permettent. La personne concernée peut demander la rectification de données inexactes.
Sécurité des données: les données doivent être protégées par des mesures techniques et organisationnelles appropriées contre la perte et les traitements non autorisés.
Droit des personnes concernées: les personnes dont les données sont traitées par DFI ont le droit de les connaître et, le cas échéant, d'en obtenir la correction ou leur effacement. L'effacement des données n'est effectué qu'à la condition que cela ne nuise pas à la bonne gestion du contrat.

1.4 Champ d'application

Le présent règlement vaut pour le traitement des données que DFI effectue pour sa gestion des Ressources Humaines et pour la gestion de ses relations Commerciales.

1.5 Obligations des collaborateurs de DFI et de ses mandataires

On entend par collaborateurs de DFI aussi bien les personnes bénéficiant d'un contrat de travail à durée indéterminée, que celles bénéficiant d'un contrat à durée déterminée les liant au DFI.
On entend par collaborateurs des mandataires de DFI, les personnes au bénéfice d'un contrat de travail les liant à une société mandatée par le DFI.
Obligation de garder le secret
Les personnes qui traitent les données des collaborateurs et des clients gérés par DFI dans le cadre d'un contrat de travail ou sur mandat ou d'un contrat de vente de prestations de services de DFI sont tenues de garder le secret à l'égard des tiers sur tout ce qu'elles apprennent pendant leur activité professionnelle, en particulier en ce qui concerne les données de nature sensibles dans l'activité des Ressources Humaines.
L'obligation de garder le secret reste applicable après la fin du contrat de travail ou du mandat ou du contrat spécifique. Cette obligation figure dans les accords contractuels relatifs à l'engagement ou au mandat ou au contrat spécifique.
Cette obligation fait partie intégrante des contrats de travail de DFI, le règlement du personnel fixant les devoirs du collaborateur, ainsi que les conditions générales avec les tiers (Fournisseurs), les accords de confidentialités, et les Conditions Générales de vente de DFI.

2 STRUCTURE DU SYSTÈME D'INFORMATION DU DFI

2.1 Composition du système d'information du DFI

1. Système de gestion technique
2. Un système de gestion des Ressources Humaines
3. Système de gestion du pilotage d'entreprise (tableaux de bord)
4. Système de gestion des Finances

    - Sous-système de gestion de la comptabilité et des frais généraux
    - Sous-système de la gestion financière client
    - Sous-système de gestion du contentieux

5. Système de gestion de la messagerie et des communications

    - Sous-système de gestion des échanges électroniques
    - Sous-système de gestion de la messagerie (e-mail)
    - Sous-système de gestion de la téléphonie et des fax

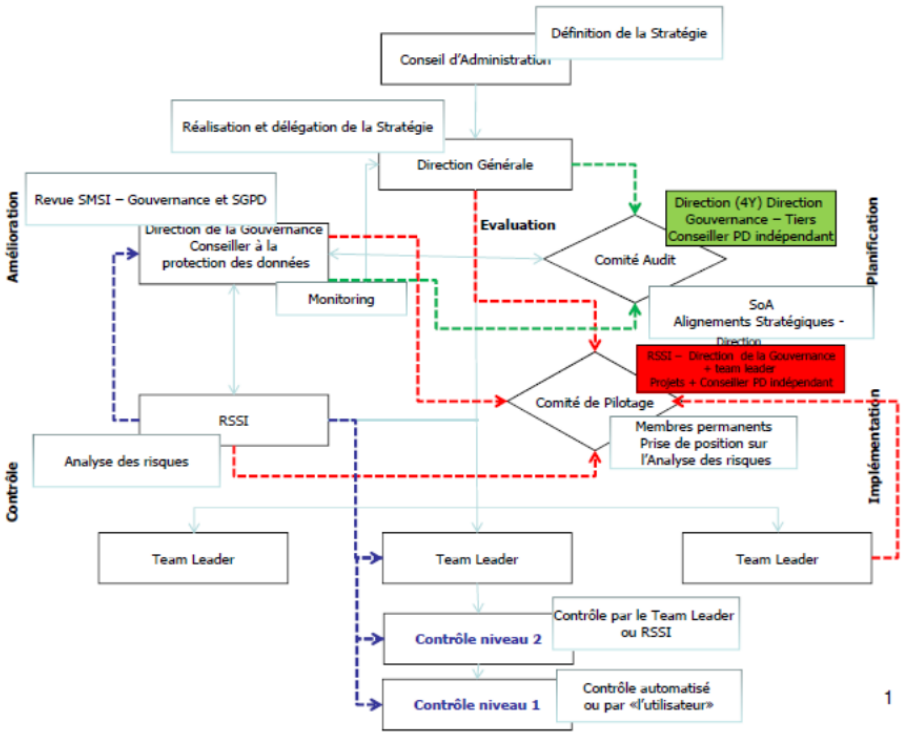
6. Système de gestion documentaire

    - Sous-système d'indexation documentaire
    - Sous-système d'archivage documentaire (papier)

7. Système de gestion Internet / Extranet
8. Système de gestion de l'exploitation informatique

    - Sous-Système de développement informatique
    - Sous-Système de gestion du réseau de télécommunication dirigé aux prestations de DFI
    - Sous-Système de gestion de la sécurité

2.2 Organigramme



1

2.3 Responsabilités

La Direction de DFI assume la responsabilité de la protection et de la sécurité des données. Dans les questions relevant du droit de la protection des données, elle est conseillée par le Conseiller interne et un Conseiller indépendant à la protection des données.
Le tableau ci-dessous décrit la répartition des rôles et responsabilités :

Rôle	Responsabilité
Protection des données en général, SGPD et formation	Conseiller indépendant à la protection des données, Maître des fichiers et RSSI
Demandes d'accès et de consultation de dossiers	Direction, Ressources Humaines
Sécurité technique des données	RSSI
Profils d'accès	Ressources humaines, Directeur de la Gouvernance et RSSI
Destruction des données électroniques	Direction et RSSI

2.4 Participants au traitement des données

2.4.1 Secteurs opérationnels

Les collaborateurs des secteurs mentionnés ci-après ont accès au Système d'information de DFI, afin de pouvoir gérer les Ressources Humaines et la Gestion des Relations Commerciales :
1. Secteur Ressources Humaines
2. Secteur relations commerciales
3. Comptabilité & Finances
4. Direction Générale

2.5 Interfaces

Plusieurs interfaces permettent le traitement des données des collaborateurs.
Plusieurs interfaces permettent le contact direct avec les collaborateurs et les clients.
Il existe des interfaces qui permettent à nos clients, d'accéder en ligne (via Internet) à leurs comptes clients. En principe, les données sont transmises électroniquement ou sur support papier au moyen d'un système d'authentification fort, du chiffrement et des technologies avancées de transmission des données, la protection et la sécurité des données sont garanties.

3 TRAITEMENT DES DONNÉES / TYPES DE DONNÉES

3.1 Données récoltées

Collaborateurs :
Les données proviennent essentiellement des collaborateurs eux-mêmes, des personnes autorisées par les collaborateurs (ancien employeur, AVS, extrait de casier judiciaire…) administrations, etc.
Clients :
Les données proviennent essentiellement des clients eux-mêmes, et des données dans le domaine public (Internet publique ou registres fédéraux publics).

3.2 Catégories de données

L'annexe 1 recense les catégories de données des collaborateurs figurant dans l'inventaire des fichiers du Système d'information du DFI.
L'annexe 2 recense les catégories de données des clients figurant dans l'inventaire des fichiers du Système d'information du DFI.

3.3 Communication des données

Les données sont communiquées sur la base d'une autorisation du collaborateur ou du client, reposant sur un consentement contractuel, une base légale ou si la communication répond à un intérêt public prépondérant.

3.3.1 Des données sont régulièrement communiquées pour

Les collaborateurs :
Etablir les contrats d'assurances obligatoires
Verser les salaires
Etablir des statistiques internes et fédérales
Vérifier l'exactitude des données
Les Clients :
Etablir les contrats des prestations de service de DFI
Etablir les factures des prestations de services de DFI
Etablir des statistiques internes et fédérales
Vérifier l'exactitude des données

3.3.2 Ces données peuvent être communiquées notamment

Pour les collaborateurs aux :

- ressources humaines de DFI;
- autorités (AVS, AI, Caisse de chômage, etc.);
- assureurs;
- tribunaux;
- dans des cas d'espèces et sur demande écrite et motivée aux autorités compétentes en matière d'aide sociale, aux tribunaux civils, aux tribunaux pénaux et aux organes d'instruction pénale, aux offices des poursuites, au Service de Renseignement de la Confédération (SRC).

Pour les clients aux :

- à l'ensemble des collaborateurs de DFI
- autorités (OfCom, TVA, etc.);
- tribunaux;
- dans des cas d'espèces et sur demande écrite et motivée aux autorités compétentes en matière d'aide sociale, aux tribunaux civils, aux tribunaux pénaux et aux organes d'instruction pénale, aux offices des poursuites, au Service de Renseignement de la Confédération (SRC).

4 DURÉE DE CONSERVATION DES DONNÉES, EFFACEMENT DES DONNÉES

La durée de conservation des données est basée sur les dispositions spécifiques du droit suisse en la matière. Après l'écoulement de la durée de conservation légale, les données doivent être détruites du Système d'information du DFI.

5 DOCUMENTATION DE PLANIFICATION, DE RÉALISATION ET D'EXPLOITATION DU SYSTÈME D'INFORMATION

Les dossiers de documentation de planification, de réalisation et d'exploitation des systèmes et sous-systèmes d'information du DFI sont conservés par la Direction de la Gouvernance.

6 DÉCLARATION DU FICHIER AU PFPDT (ART. 16 OLPD)

Le conseiller indépendant à la protection des données procède à un inventaire des fichiers de données qu'il tient à disposition du PFPDT.

7 PROCESSUS

La collecte, le traitement et la transmission des données du Système d'Information de DFI sont basés sur des processus. Ces derniers sont documentés et sont internes à DFI.

8 PROCÉDURES DE CONTRÔLE ET MESURES TECHNIQUES ET ORGANISATIONNELLES

8.1. Contrôle d'accès

Tous les locaux du DFI dans lesquels des données sensibles personnelles sont traitées sont protégés électroniquement et/ou manuellement contre l'accès de tiers non autorisés.
L'accès aux locaux du DFI n'est accordé qu'aux collaborateurs identifiés par une reconnaissance biométrique.
Les visiteurs sont appelés à s'annoncer à la réception de DFI pour être enregistrés et se voir attribuer un badge « visiteur ».
Les droits d'accès sont attribués selon la fonction et le titre du collaborateur. Ils sont plus ou moins étendus. De plus les accès sont gérés par site, ces accès peuvent être temporaires.
Tous les accès ou tentatives d'accès sont historisés par le logiciel de gestion des accès.
Des systèmes de vidéosurveillance et d'alarmes sont gérés uniquement dans les Data Centres par les Data Centres.
Certains locaux, peuvent être accessibles à l'aide d'un badge fourni au collaborateur. Chaque badge est identifié et un registre des badges remis aux collaborateurs est tenu à jour.
Les accès aux Data Centre sont protégés par un système d'authentification fort, vérification de l'identité, et surveillance vidéo. Des journaux d'accès permettent d'identifier les personnes ayant accédé à ces locaux et à quel moment.

8.2. Contrôle des supports de données personnelles

Seules les personnes dûment autorisées obtiennent les accès au Système d'information de DFI et seules les personnes autorisées peuvent traiter les données enregistrées sur les supports électroniques.

8.3. Authentification des utilisateurs

L'accès aux modules du système d'information du DFI n'est possible qu'en disposant des moyens d'authentification nécessaires.

8.4. Contrôle du transport

Les mesures techniques appropriées sont mises en place afin de sécuriser la transmission des données, de sorte à ce que les personnes non autorisées ne puissent pas lire, copier, modifier ou effacer des données lors de leur communication ou lors du transport de supports de données.

8.5. Contrôle de communication

Les destinataires de données qui accèdent aux données personnelles au moyen d'installations de transmission de données sont identifiés, en particulier les fournisseurs de prestations qui accèdent aux données relatives aux Ressources Humaines, aux données de nos clients et nos données techniques de notre système de télécommunication.

8.6. Contrôle de mémoire

Les mesures techniques appropriées sont mises en place afin que des personnes non autorisées ne puissent ni introduire de données dans la mémoire ni prendre connaissance des données mémorisées, respectivement les modifier ou les effacer.

8.7. Contrôle d'utilisation

Seuls des terminaux agréés par le DFI peuvent être raccordés au réseau informatique du DFI.

8.8. Contrôle d'accès

Les personnes autorisées ont accès uniquement aux données dont elles ont besoin pour accomplir leurs tâches. La nature et l'étendue de l'accès des utilisateurs du fichier sont décrites dans le présent règlement.

8.9. Contrôle de l'introduction (journalisation)

En plus du contrôle de l'accès au Système d'information de DFI, les traitements automatisés de données font l'objet d'une journalisation afin qu'il soit possible de vérifier à posteriori que les données ont été traitées conformément aux finalités pour lesquelles elles ont été

collectées ou communiquées. Les procès-verbaux de journalisation sont conservés sous une forme répondant aux exigences de la révision. Ils sont accessibles aux seuls organes ou personnes chargés de vérifier l'application des dispositions de protection des données personnelles, et ils ne sont utilisés qu'à cette fin.

8.10 Développement d'applications

Les environnements de développement, de test et de production sont strictement séparés.

8.11 Supervision et responsabilité

Le maître des fichiers s'assure que les utilisateurs se conforment aux instructions, au présent Règlement de traitement et à ses annexes.

9 DESCRIPTION DES CHAMPS DE DONNÉES ET DES UNITÉS D'ORGANISATION QUI Y ONT ACCÈS

Les droits d'accès au système d'information de DFI sont réglés au moyen d'un système d'autorisations d'accès.

10 NATURE ET ÉTENDUE DE L'ACCÈS DES UTILISATEURS AU SYSTÈME D'INFORMATION

10.1 Utilisateurs

Les personnes autorisées à accéder au Système d'information du DFI sont :
1. les collaborateurs de DFI.
2. Les administrateurs systèmes de DFI.

10.2 Gestion des droits d'accès

La Sécurité du Système d'Information a pour but d'assurer la confidentialité, l'intégrité et la disponibilité des informations. Une composante importante de la sécurité repose sur la notion de gestion des accès qui comporte deux pôles principaux, les accès physiques qui permettent à un utilisateur d'accéder aux différents bâtiments et locaux de l'entreprise et les accès logiques qui lui permettent de se connecter aux systèmes et applications pour accéder aux informations dont il a besoin.

10.3 Contrôle des accès aux applications de gestion

Les données des collaborateurs et des clients sont gérées sur des plateformes informatiques distinctes.
Les accès logiques sont gérés, d'une part par le secteur Informatique pour les applications standard, d'autre part par les métiers pour certaines applications spécifiques. Un workflow initial permet d'attribuer une authentification à tout nouveau collaborateur. Des accès supplémentaires peuvent ensuite être demandés. Un workflow de validation permet aux responsables d'accepter ou non les demandes formulées. La gestion des accès se base sur le principe du moindre privilège, c'est-à-dire qu'un collaborateur n'aura accès qu'aux éléments pertinents pour la réalisation de ses tâches. Le principe veut qu'initialement tous les accès soient verrouillés et que les droits ne soient accordés que sur demande.
Lorsqu'un collaborateur quitte l'entreprise, les accès sont radiés et il n'est plus possible pour le collaborateur de se connecter aux systèmes logiques, ni d'accéder aux locaux.

10.4 Accès aux documents bureautiques

Les données gérées au travers des différentes applications de gestion de DFI peuvent être transférées dans des fichiers bureautiques.
Ces documents de travail sont enregistrés dans un répertoire bureautique spécifique à chaque secteur de DFI. Le responsable hiérarchique définit les droits d'accès à ce répertoire sur la base de la fonction du collaborateur. La gestion des droits (attribution, modification, suppression) est assurée par le Responsable de la sécurité du système d'information de DFI qui attribue chaque collaborateur à un groupe d'utilisateurs autorisés à accéder aux données enregistrées dans chaque répertoire.
Les accès aux documents enregistrés dans les répertoires bureautiques font l'objet peuvent faire l'objet d'une journalisation. L'accès aux journaux d'audit générés sera dans ce cas limité aux collaborateurs du secteur informatique chargés de la sécurité du système d'information.

10.5 Accès des collaborateurs travaillant en mode télétravail (astreinte)

Le DFI dispose de collaborateurs pouvant travailler depuis leur domicile à des tâches d'astreinte. Cette activité consiste à se mettre à disposition de DFI en dehors des heures d'ouverture pour intervenir sur le système d'information de DFI en cas d'anomalies. L'accès aux applications depuis le domicile est régi par les mêmes principes que ceux concernant les collaborateurs travaillant sur site. La connexion au système informatique de
DFI est effectuée au travers d'une méthode d'authentification forte.

10.6 Contrôle des accès aux données disponibles sur les plates-formes Extranet

Un nombre restreint de données personnelles sont rendues accessibles sur les plates-formes Extranet de DFI. Leur accès, par des personnes autorisées, est protégé par une méthode d'authentification forte.

11 DROITS DES PERSONNES CONCERNÉES

Les demandes d'accès selon l'art. 8 LPD doivent être adressées par écrit au Service Protection des Données de DFI, accompagnées d'une preuve de l'identité du requérant (copie d'une attestation officielle, avec photo), à l'adresse suivante :

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

Au moyen des formulaires suivants :

- sur le site www.dfi.ch sous la rubrique contact pour les données client
- dans l'outil interne de documentation pour les collaborateurs sous Formulaire de demande des données collaborateur

12 CONFIGURATION DES MOYENS INFORMATIQUES

Le matériel informatique et les logiciels utilisés par DFI correspondent aux standards techniques.
Les documentations relatives à la configuration des moyens informatiques utilisés pour le système d'information de DFI sont conservées dans le secteur IT ou auprès des fournisseurs/partenaires externes.
Pour des raisons de sécurité, aucune indication n'est fournie sur la configuration des moyens informatiques.

13 DISPOSITIONS FINALES

13.1 Annexes

Les annexes mentionnées dans le présent règlement de traitement font partie intégrante du présent règlement.

13.2 Elaboration et modifications du règlement

Le règlement de traitement est mis à jour régulièrement par le maître des fichiers conformément aux dispositions de l'art. 11 de l'OLPD.
Ce règlement peut être modifié en tout temps. Les modifications doivent être apportées sous forme écrite et approuvées par la Direction de DFI.
Le règlement de traitement est élaboré par le Conseiller indépendant à la protection des données et le maître des fichiers.
La responsabilité pour la modification du règlement incombe à la Direction de la Gouvernance.

13.3 Entrée en vigueur

Ce règlement entre en vigueur immédiatement.

13.4 Publication

Le présent règlement et ses annexes sont publiés sur internet, sous www.dfi.ch.

ANNEXE 1

Catégories des données basées sur l'inventaire des fichiers des collaborateurs de DFI. (Accès uniquement interne).
Incluant : Catégories des données personnelles traitées (Art. 3, alinéa 1, lettre e OLPD)

ANNEXE 2

Catégories des données basées sur l'inventaire des fichiers des clients de DFI. (Accès uniquement interne ou sur demande du client).
Incluant : Catégories des données personnelles traitées (Art. 3, alinéa 1, lettre e OLPD)

ANNEXE 3

Liste des fichiers non déclarés concernés par la protection des données (Accès uniquement interne)

Incluant : Catégories des données personnelles traitées (Art. 3, alinéa 1, lettre e OLPD)

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