|  |  |
| --- | --- |
|  | Si rempli, min. : INTERNE |

|  |
| --- |
|  |

Règlement de traitement des personnes privées

< Nom du projet / nom de l’objet à protéger >

|  |
| --- |
|  |

|  |  |
| --- | --- |
| Classification | **INTERNE** / CONFIDENTIEL / SECRET |
| Statut | **en cours d’élaboration**, en cours de vérification, terminé / approuvé |
| Numéro de projet |  |
| Chef de projet |  |
| Version | À partir du modèle V2.1 - P042-Hi04 - Règlement de traitement |
| Date |  |
| Mandant |  |
| Auteurs |  |

Suivi des modifications

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description, remarque | Nom |
| 0.1 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Distribution

|  |  |  |
| --- | --- | --- |
| Fonction | Nom  | Organisation / société |
| Conseiller à la protection des données |  |  |
| CISO |  |  |
|  |  |  |
|  |  |  |

Table des matières

1 Généralités 4

1.1 Description 4

1.2 But du règlement de traitement des personnes privées 4

1.3 Tailoring 4

1.4 Outils 5

1.5 Approbation 6

2 Règlement de traitement des personnes privées 7

2.1 Généralités 7

2.1.1 Objet du traitement de données 7

2.1.2 Catégories de personnes concernées et catégories de données personnelles traitées 7

2.2 Organisation interne 7

2.2.1 Responsable du traitement 7

2.2.2 Sous-traitant 8

2.2.3 Utilisateurs et accès aux données 8

2.2.3.1 Cercle des utilisateurs 8

2.2.3.2 Droits d’accès 8

2.2.3.3 Rôles 8

2.2.3.4 Procédure d’octroi des droits d’accès 8

2.3 Procédure de traitement des données et de contrôle 9

2.3.1 Traitement des données personnelles 9

2.3.1.1 Processus métier 9

2.3.1.2 Communication de données et interfaces 9

2.3.1.3 Vérification des données personnelles saisies 10

2.3.1.4 Processus / procédures de traitement des données 10

2.3.2 Durée de conservation, archivage et effacement 10

2.3.2.1 Durée de conservation 10

2.3.2.2 Archivage 10

2.3.2.3 Effacement 10

2.3.3 Droits des personnes concernées 11

2.4 Mesures visant à garantir la sécurité des données 11

3 Annexe 12

3.1 Répertoire des activités de traitement 12

3.2 Analyse d’impact relative à la protection des données personnelles 13

3.3 Concept d’autorisations / Matrice des droits d’accès 13

3.4 Répertoire 15

3.5 Abréviations 16

3.6 Définitions 17

# Généralités

## Description

Description du traitement automatisé du projet informatique

## But du règlement de traitement des personnes privées

Le **responsable du traitement privé et son sous-traitant privé** (cf. art. 5 de l’ordonnance du 31 août 2022 sur la protection des données [OPDo]) établissent un règlement pour les traitements automatisés en cas :

* de traitement de données sensibles à grande échelle, ou
* de profilage à risque élevé.

Ce règlement doit notamment contenir des informations sur :

* l’organisation interne ;
* les procédures de traitement de données et de contrôle, et
* les mesures visant à garantir la sécurité des données.

Il contient la liste de tous les documents relatifs à la planification, à la réalisation et à l’exploitation du fichier. Le registre des activités de traitement visé aux art. 12 et 15 LPD et une première analyse d’impact relative à la protection des données personnelles (au sens de l’art. 22 LPD) doivent être annexés au règlement de traitement.

Le règlement de traitement doit permettre l’évaluation et l’appréciation correctes des éventuels risques pour la protection des données.

Le responsable du traitement privé et son sous-traitant privé doivent actualiser régulièrement le règlement. Si un conseiller à la protection des données a été nommé, le règlement doit être mis à sa disposition.

## Tailoring

Le règlement de traitement doit être rédigé de manière aussi concise et compréhensible que possible, de sorte que la description du fichier informatique puisse être comprise et évaluée par des profanes (principe).

Le règlement de traitement sera détaillé proportionnellement à l’ampleur et à la sensibilité du traitement des données personnelles. Il doit décrire les principaux aspects du traitement sous l’angle de la protection des données et de la sécurité des informations (sauf si ces informations figurent déjà dans un concept SIPD). Pour plus de détails, il doit renvoyer à des documents fournissant des informations supplémentaires.

Il est important de ne pas copier le contenu de documents existants, mais d'y faire référence avec des indications précises et de joindre ces documents. Le règlement de travail ne doit pas être un exercice de copie et de recopie.

Le texte en bleu correspond aux instructions de remplissage du document.

## Outils

L’élaboration du règlement peut s’appuyer sur les outils suivants :

**Outils :**

* [Directives relatives à la procédure de sécurité et aux outils correspondants à l'échelon de la Confédération du délégué fédéral à la cybersécurité, NCSC](https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html)
* Mesures techniques et organisationnelles (MTO) (dans l'Infothèque Protection des données du PFPDT)

## Approbation

Les signatures d’approbation doivent être apposées avant le début de l’exploitation.

Par sa signature, le conseiller à la protection des données atteste avoir examiné le règlement de traitement. Il a notamment vérifié que le document est intégralement rempli et que toutes les mesures requises sont documentées. Il a vérifié la cohérence des informations et leur exactitude dans le contexte du traitement des données.

Par sa signature, le responsable du traitement approuve le règlement de traitement.

|  |  |
| --- | --- |
| Date / nom / signature **Conseiller à la protection des données** : | …………………………………………………...…... |
| Date / nom / signature **Responsable du traitement** :  | …………………………………………………...…... |
|  |  |

**Il est possible d’ajouter des signatures.**

**Les signatures peuvent aussi être apposées sous forme électronique (dans un PDF).**

# Règlement de traitement des personnes privées

## Généralités

### Objet du traitement de données

(art. 6, al. 3, LPD en relation avec l’art. 1, al. 2, let. b, OPDo, art. 6, al. 4 et 5, 7, al. 3, et 12, al. 2, LPD)

Décrire la finalité, la nature, l’étendue et les circonstances du traitement, de même que le nombre et la nature des personnes concernées.

En exposant le contexte, expliquer brièvement pourquoi on souhaite exploiter un système, quels en sont les buts et quelle est la situation visée.

### Catégories de personnes concernées et catégories de données personnelles traitées

(art. 6, al. 6 et 7, 12, al. 2, et 19 LPD, 1, al. 2, let. a, et 13 OPDo)

Répondre aux questions ci-après sur le contenu des données traitées :

* De quel type sont les données personnelles traitées (données personnelles, données sensibles, profils de la personnalité, autres) ?
* Quelles sont les catégories (ou « groupes ») de personnes et de données personnelles qui seront traitées ?
* Comment les données personnelles ont-elles été obtenues ?

## Organisation interne

(art. 9, 10, 12 à 15 LPD, 7, 8, 17 et 23 OPDo)

### Responsable du traitement

Indiquer ici l’identité du responsable du traitement (y c. celle de son représentant en Suisse si le responsable du traitement privé a son siège ou son domicile à l’étranger) et, le cas échéant, celle de son conseiller à la protection des données, y compris son organisation interne. Préciser qui est responsable, d’une part, des procédures de traitement des données et de contrôle, et d’autre part, du choix (sur la base de l’analyse d’impact relative à la protection des données, p. ex.) et de la mise en œuvre des mesures visant à garantir la sécurité des données.

Informations concernant :

le responsable du traitement :

son représentant en Suisse si le responsable du traitement privé a son siège ou son domicile à l’étranger :

le conseiller à la protection des données :

### Sous-traitant

Indiquer le sous-traitant responsable et un interlocuteur de référence.

Informations concernant :

le sous-traitant :

l’interlocuteur de référence chez le fournisseur de la prestation / le sous-traitant :

### Utilisateurs et accès aux données

#### Cercle des utilisateurs

Indiquer les catégories (ou « groupes ») de toutes les unités administratives et de tous les services bénéficiant d’un droit d’accès.

Le cas échéant, renvoyer ici à la matrice de communication du concept SIPD.

#### Droits d’accès

Indiquer et décrire brièvement la nature et l’étendue de l’accès des utilisateurs du fichier et les champs de données. S’il existe déjà une matrice des droits d’accès (ou un concept d’autorisations), l’annexer au règlement de traitement.

#### Rôles

Énumérer les rôles associés aux droits d’accès (collaborateur spécialisé, administrateur, p. ex.) et indiquer l’étendue de l’accès de chaque rôle (consultation, traitement, impression, aucun accès, autres) ?

#### Procédure d’octroi des droits d’accès

Décrire ici les modalités (procédure et responsabilités) d’octroi et de retrait des droits d’accès. Régler les questions suivantes :

* Qui est responsable de l’octroi et du retrait des droits d’accès ?
* Qui vérifie et met à jour régulièrement les droits d’accès octroyés ?
* Quelle est l’étendue du droit d’accès ?
* Existe-t-il une procédure d’octroi et de retrait des droits d’accès ?
* Quelle est cette procédure ?
* Est-elle centralisée ?

## Procédure de traitement des données et de contrôle

(Art. 6 à 14, 16, 19, 21, 22, 24, 25, 28, 30, 32, LPD, 1 à 5, 9 à 13, 15 à 18, 20, 22 à 24 OPDo)

Thèmes :

Destruction des données dès qu’elles ne sont plus nécessaires au regard des finalités du traitement

Mesures de rectification des données personnelles

Consentement au traitement de données personnelles

Protection des données dès la conception et par défaut

Mesures pour la sécurité des données

Gestion de la sous-traitance

Implication des conseillers à la protection des données

Tenue du registre des activités de traitement

Recours à la certification

Conditions légales de communication de données personnelles à l’étranger

Devoir d’informer lors de la collecte de données personnelles

Devoir d’informer en cas de décision individuelle automatisée

Analyse d’impact relative à la protection des données personnelles

Annonce des violations de la sécurité des données

Organisation du droit d’accès

Droit à la remise ou à la transmission des données personnelles

Contrôle et responsabilité en cas de traitements de données personnelles conjoints

Communication de données personnelles

### Traitement des données personnelles

#### Processus métier

Documenter dans cette rubrique les principaux processus métier associés au fichier et importants sous l’angle de la protection des données, ou les exposer sous forme graphique.

#### Communication de données et interfaces

Illustrer ici par un graphique les interfaces avec d’autres objets à protéger tels que systèmes, applications, etc. On peut aussi renvoyer au concept SIPD s’il comporte une telle vue d’ensemble.

La description des interfaces doit contenir les informations ci-après concernant la transmission des données (communication) :

* Qui a fourni les données personnelles ?
* Qui reçoit les données personnelles ?
* Quelle est la finalité de la transmission des données personnelles ?
* Quelles sont les catégories (ou « groupes ») de données personnelles qui sont transmises ?
* Quelle est la périodicité de la transmission des données personnelles ?
* Qui a lancé la transmission ?
* Quel est le moyen de transmission des données personnelles ?

La description des interfaces devrait indiquer la finalité des transmissions régulières de données personnelles.

#### Vérification des données personnelles saisies

Qui vérifie l’exactitude des données personnelles ? Une procédure spécifique est-elle prévue ? Un examen et une rectification réguliers de ces données sont-ils prévus ?

#### Processus / procédures de traitement des données

Définir et décrire les procédures de rectification, de blocage, d’anonymisation, de sauvegarde, de conservation, d’archivage et de destruction des données.

### Durée de conservation, archivage et effacement

#### Durée de conservation

Régler les questions suivantes :

* Combien de temps les données personnelles ou les catégories (« groupes ») de données personnelles peuvent-elles ou doivent-elles être conservées ?
* Quel est le lieu de conservation des données personnelles, et qui en est responsable ?
* Quand ces données seront-elles effacées ou versées aux Archives fédérales ?

#### Archivage

Détailler ici les modalités organisationnelles et techniques (formats de données, interfaces) de proposition ou de remise des données personnelles aux Archives fédérales.

#### Effacement

À quel moment les données personnelles devenues inutiles sont-elles effacées du fichier ? Cette formulation doit faire l’objet d’une concertation avec le DSIO et le responsable de l’application.

### Droits des personnes concernées

Indiquer notamment à qui la personne concernée doit s’adresser (interlocuteur) et comment se déroule la procédure interne.

Créer les instruments et procédures permettant l’exercice des droits de rectification, de destruction et de blocage, et du droit d’annotation en cas de contestation. Les instruments permettant le blocage de la communication à des tiers doivent être disponibles et utilisables.

Le devoir d’informer lors de la collecte de données personnelles par des personnes privées doit être pris en compte et réglé en conséquence (art. 19 et 20 LPD).

## Mesures visant à garantir la sécurité des données

(art. 7, 8, 10 à 13, 22 et 24 LPD ; art. 1 à 5, 15 et 23 OPDo)

Indiquer ici les mesures techniques et organisationnelles garantissant une protection appropriée des données et qui ne figurent pas dans le concept SIPD.

# Annexe

## Répertoire des activités de traitement

Le responsable du traitement, son représentant en Suisse s’il a son siège ou son domicile à l’étranger et le sous-traitant tiennent chacun un registre de leurs activités de traitement.

Le registre du responsable du traitement et celui du représentant contiennent au moins les indications suivantes :

* l’identité du responsable du traitement ;
* la finalité du traitement ;
* une description des catégories de personnes concernées et des catégories de données personnelles traitées ;
* les catégories de destinataires ;
* dans la mesure du possible, le délai de conservation des données personnelles ou les critères pour déterminer la durée de conservation ;
* dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données selon l’art. 8 LPD ;
* en cas de communication de données personnelles à l’étranger, le nom de l’État concerné et les garanties prévues à l’art. 16, al. 2, LPD.

Le registre du sous-traitant contient des indications concernant l’identité du sous-traitant et du responsable du traitement, les catégories de traitements effectués pour le compte du responsable du traitement et au moins les indications suivantes :

* dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données selon l’art. 8 LPD ;
* en cas de communication de données personnelles à l’étranger, le nom de l’État concerné et les garanties prévues à l’art. 16, al. 2, LPD.

Le Conseil fédéral prévoit des exceptions à l’obligation de tenir un registre des activités pour les entreprises qui emploient moins de 250 collaborateurs et dont le traitement des données présente un risque limité d’atteinte à la personnalité des personnes concernées.

## Analyse d’impact relative à la protection des données personnelles

Lorsque certaines conditions sont réunies, le responsable du traitement doit procéder à une analyse d’impact relative à la protection des données personnelles.

Une copie de l’analyse doit être annexée au règlement de traitement.

## Concept d’autorisations / Matrice des droits d’accès

Le concept d’autorisations ou la matrice des droits d’accès doit être annexé au règlement de traitement.

**Exemple** simplifié de matrice d’autorisations :

|  |  |  |  |
| --- | --- | --- | --- |
| Nom du champ de données | Entreprise | Filiale | Tiers |
|  | UA I | UA II | UA III | … | … | … | Finances | … | … | … | … | … | … | … |
|  |
| I. Données de base |
| Nom (s) | A | A | B | … | … | … | A | … | … | … | … | … | … | … |
| Prénom(s) | A | A | B | … | … | … | A | … | … | … | … | … | … | … |
| Date de naissance |  | A | A | … | … | … | A | … | … | … | … | … | … | … |
| Nationalité |  | A | A | … | … | … | B | … | … | … | … | … | … | … |
| … | … | … | … | … | … | … | … | … | … | … | … | … | … | … |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| II. Informations sur le dossier |
| Détenteur du dossier | B | B | B | … | … | … | A | … | … | … | … | … | … | … |
| Statut du dossier | B | B | B | … | … | … |  | … | … | … | … | … | … | … |
| No de référence : | A | B | B | … | … | … | B | … | … | … | … | … | … | … |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| III. Titre X |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Niveaux d’accès**

A = Consultation

B = Traitement

Case vide = pas d’accès

Autres

**Unités administratives**

UA I : p. ex. service juridique de l’UA concernée

UA II : p. ex. collaborateur spécialisé de l’UA concernée

UA III : p. ex. administrateur de l’UA concernée

…

Filiale : Finances, p. ex.

…

## Répertoire

Liste de tous les textes pertinents pour le fichier concerné (lois, ordonnances, directives, réglementations, spécifications techniques, etc.). Il faut y ajouter les documents internes à l’entreprise.

|  |  |
| --- | --- |
| Type de document | Titre |
| Lois | [Loi fédérale du 19 juin 1992 sur la protection des données (LPD; RS *235.1*)](http://www.admin.ch/ch/f/sr/c235_1.html) |
| Ordonnances | [Ordonnance du 31 août 2022 sur la protection des données (OPDo ; RS 235.11)](https://www.fedlex.admin.ch/eli/cc/2022/568/fr) |
| Instructions |  |
| Documents internes | Concept d’autorisations |
|  | Représentation du flux de données / diagramme du flux de données |
|  | Architecture informatique |
|  | … |

## Abréviations

|  |  |
| --- | --- |
| Abréviation | Signification |
| al. | alinéa |
| art. | article |
| CISO | Chief Information Security Officer |
| Concept SIPD | Concept de sécurité de l’information et de protection des données |
| let. | lettre |
| LPD | loi fédérale sur la protection des données (RS 235.1) |
| OPDo | ordonnance sur la protection des données (RS 235.11) |
| PFPDT | Préposé fédéral à la protection des données et à la transparence |
| UA | Unités administratives |
| … | … |

## Définitions

|  |  |
| --- | --- |
| Définition | Signification |
| Traitement | Toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, l’enregistrement, la conservation, l’utilisation, la modification, la communication, l’archivage, l’effacement ou la destruction de données (art. 5, let. d, LPD). |
| Communication | Le fait de transmettre des données personnelles ou de les rendre accessibles (fart. 5, let. e, LPD). |
| Données sensibles | Données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales, sur la santé, la sphère intime ou l’origine raciale ou ethnique, sur les données génétiques, sur des mesures d’aide sociale et sur des poursuites ou sanctions pénales et administratives (art. 5, let. c, LPD). |
| Violation de la sécurité des données | Toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données (art. 5, let. h, LPD). |
| Responsable du traitement | la personne privée ou l’organe fédéral qui, seul ou conjointement avec d’autres, détermine les finalités et les moyens du traitement de données personnelles (art. 5, let. j, LPD). |
| Sous-traitant | La personne privée ou l’organe fédéral qui traite des données personnelles pour le compte du responsable du traitement (art. 5, let. k, LPD). |
| Données personnelles, personne concernée | Toutes les informations concernant une personne physique identifiée ou identifiable (art. 5, let. a et b, LPD). |
| Profilage | Toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique (art. 5, let. f, LPD). |
| Profilage à risque élevé | Tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu’il conduit à un appariement de données qui permet d’apprécier les caractéristiques essentielles de la personnalité d’une personne physique (art. 5, let. g, LPD). |
| … | … |