English is not an official language of the Swiss Confederation. The translation on the right side below has been prepared by the Swiss law firm OBERSON ABELS SA and is provided for information purposes only. It has no legal force and may not be relied upon in legal proceedings.

Ordonnance sur la protection des données (OPDo)

du 31 août 2022

Le Conseil fédéral suisse,

vu les art. 8, al. 3, 10, al. 4, 12, al. 5, 16, al. 3, 25, al. 6, 28, al. 3, 33, 59, al. 2 et 3 de la loi fédérale du 25 septembre 2020 sur la protection des données (LPD) *arrête :*

Chapitre 1: Dispositions générales

Section 1: Sécurité des données

Art. 1 Principes

[1] Pour assurer une sécurité adéquate des données, le responsable du traitement et le sous-traitant établissent le besoin de protection des données personnelles et déterminent les mesures techniques et organisationnelles appropriées à prendre par rapport au risque encouru.

[2] Le besoin de protection des données personnelles est évalué en fonction des critères suivants:

a. le type de données traitées;
b. la finalité, la nature, l'étendue et les circonstances du traitement.

[3] Le risque pour la personnalité ou les droits fondamentaux de la personne concernée est évalué en fonction des critères suivants:

a. les causes du risque;
b. les principales menaces;
c. les mesures prises ou prévues pour réduire le risque;
d. la probabilité et la gravité d'une violation de la sécurité des données, malgré les mesures prises ou prévues.

[4] Lors de la détermination des mesures techniques et organisationnelles, les critères suivants sont de plus pris en compte :

a. l'état des connaissances;
b. les coûts de mise en œuvre.

[5] Le besoin de protection des données personnelles, le risque encouru, ainsi que les mesures techniques et organisationnelles sont réévalués pendant toute la durée du traitement. En cas de besoin, les mesures sont adaptées.

Art. 2 Objectifs

En fonction du besoin de protection, le responsable du traitement et le sous-traitant prennent des mesures

Ordinance on Data Protection (Data Protection Ordinance; DPO)

August 31, 2022

The Swiss Federal Council,

having considered the Art. 8 (3), 10 (4), 12 (5), 16 (3), 25 (6), 28 (3), 33, 59 (2) and (3) of the Federal Act on Data Protection dated September 25, 2020 (DPA) *decrees:*

Chapter 1: General provisions

Section 1: Data security

Art. 1 Principles

[1] To ensure adequate data security, the controller and the processor shall determine the need for protection of personal data and the appropriate technical and organizational measures to be taken regarding the risk involved.

[2] The need for protection of personal data is assessed according to the following criteria:

a. the type of data processed;
b. the purpose, nature, extent, and circumstances of the process.

[3] The risk to the data subjects' privacy or fundamental rights is assessed according to the following criteria:

a. the causes of the risk;
b. the main threats;
c. measures taken or planned to reduce the risk;
d. the likelihood and severity of a data security breach, despite the measures taken or planned.

[4] When determining the technical and organizational measures, the following criteria are additionally considered:

a. the state of knowledge;
b. implementation costs.

[5] The need for protection of personal data, the risk involved, as well as the technical and organizational measures are re-evaluated during the entire processing period. If necessary, the measures are adapted.

Art. 2 Objectives

Depending on the need for protection, the controller and the processor take technical and organizational measures to

techniques et organisationnelles pour que les données traitées:

a. ne soient accessibles qu'aux personnes autorisées (confidentialité);
b. soient disponibles en cas de besoin (disponibilité);
c. ne puissent être modifiées sans droit ou par mégarde (intégrité);
d. soient traitées de manière à être traçables (traçabilité).

ensure that the processed data:

a. are accessible only to authorized persons (confidentiality);
b. are available when needed (availability);
c. cannot be changed without right or by mistake (integrity);
d. be processed in such a way as to be traceable (traceability).

Art. 3 Mesures techniques et organisationnelles

[1] Pour assurer la confidentialité, le responsable du traitement et le sous-traitant prennent des mesures appropriées afin que:

a. les personnes autorisées n'aient accès qu'aux données personnelles dont elles ont besoin pour accomplir leurs tâches (contrôle de l'accès aux données);
b. seules les personnes autorisées puissent accéder aux locaux et aux installations utilisés pour le traitement de données (contrôle de l'accès aux locaux et aux installations);
c. les personnes non autorisées ne puissent pas utiliser les systèmes de traitement automatisé de données personnelles à l'aide d'installations de transmission (contrôle d'utilisation).

[2] Pour assurer la disponibilité et l'intégrité, le responsable du traitement et le sous-traitant prennent des mesures appropriées afin que:

a. les personnes non autorisées ne puissent pas lire, copier, modifier, déplacer, effacer ou détruire des supports de données (contrôle des supports de données);
b. les personnes non autorisées ne puissent pas enregistrer, lire, modifier, effacer ou détruire des données personnelles dans la mémoire (contrôle de la mémoire);
c. les personnes non autorisées ne puissent pas lire, copier, modifier, effacer ou détruire des données personnelles lors de leur communication ou lors du transport de supports de données (contrôle du transport);
d. la disponibilité des données personnelles et l'accès à celles-ci puissent être rapidement restaurés en cas d'incident physique ou technique (restauration);
e. toutes les fonctions du système de traitement automatisé de données personnelles soient disponibles (disponibilité), que les

Art. 3 Technical and organizational measures

[1] To ensure confidentiality, the controller and the processor shall take appropriate measures to ensure that:

a. authorized persons have access only to the personal data they need to perform their duties (data access control);
b. only authorized persons have access to the premises and systems used for data processing (control of access to the premises and systems);
c. unauthorized persons cannot use automated personal data processing systems with the help of transmission systems (usage control).

[2] To ensure availability and integrity, the controller and the processor shall take appropriate measures to ensure that:

a. unauthorized persons cannot read, copy, modify, move, erase, or destroy data carriers (data carrier control);
b. unauthorized persons cannot store, read, modify, erase, or destroy personal data in the memory (memory control);
c. unauthorized persons cannot read, copy, modify, erase, or destroy personal data during communication or during the transport of data carriers (transport control);
d. the availability of and access to personal data can be quickly restored in the event of a physical or technical incident (recovery);
e. all functions of the automated personal data processing system are available (availability), that malfunctions are prevented (reliability) and that the

dysfonctionnements soient signalés (fiabilité) et que les données personnelles stockées ne puissent pas être endommagées en cas de dysfonctionnements du système (intégrité des données);

f. les systèmes d'exploitation et les logiciels d'application soient toujours maintenus à jour en matière de sécurité et que les failles critiques connues soient corrigées (sécurité du système).

[3] Pour assurer la traçabilité, le responsable du traitement et le sous-traitant prennent des mesures appropriées afin que:

a. il soit possible de vérifier quelles données personnelles sont saisies ou modifiées dans le système de traitement automatisé de données, par quelle personne et à quel moment (contrôle de la saisie);

b. il soit possible de vérifier à qui sont communiquées les données personnelles à l'aide d'installations de transmission (contrôle de la communication);

c. les violations de la sécurité des données puissent être rapidement détectées (détection) et que des mesures puissent être prises pour atténuer ou éliminer les conséquences (réparation).

stored personal data cannot be damaged in case of system malfunctions (data integrity);

f. operating systems and application software are always kept up to date regarding security and that known critical flaws are corrected (system security).

[3] To ensure traceability, the controller and processor shall take appropriate measures to ensure that:

a. it is possible to check which personal data are entered or modified in the automated data processing system, by which person and at what time (entry control);

b. it is possible to verify to whom the personal data are communicated by means of transmission systems (communication control);

c. data security breaches can be promptly detected (detection) and steps taken to mitigate or eliminate the consequences (remediation).

Art. 4 Journalisation

[1] Lors de traitements automatisés de données sensibles à grande échelle ou de profilage à risque élevé et lorsque les mesures préventives ne suffisent pas à garantir la protection des données, le responsable du traitement privé et son sous-traitant privé journalisent au moins l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction des données. La journalisation est notamment nécessaire lorsque, sans cette mesure, il n'est pas possible de vérifier a posteriori que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées.

[2] Lors du traitement automatisé de données personnelles, l'organe fédéral responsable et son sous-traitant journalisent au moins l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction des données.

[3] Pour les données personnelles généralement accessibles au public, l'enregistrement, la modification, l'effacement et la destruction des données doivent au moins être journalisés.

[4] La journalisation doit fournir des informations sur l'identité de la personne qui a effectué le traitement, la nature, la date et l'heure du traitement et, cas échéant, l'identité du destinataire des données.

[5] Les procès-verbaux de journalisation sont conservés durant au moins un an, séparément du système dans lequel les

Art. 4 Logging

[1] In the case of large-scale automated processing of sensitive data or high-risk profiling, and where preventive measures are not sufficient to guarantee data protection, the private controller and his private processor shall at least log the recording, modification, reading, communication, erasure, and destruction of data. Logging is necessary if it is not otherwise possible to verify a posteriori that the data have been processed in accordance with the purposes for which they were collected or communicated.

[2] In the case of automated processing of personal data, the federal body (controller) and its processor shall at least log the recording, modification, reading, communication, erasure, and destruction of the data.

[3] In the case of personal data that is generally accessible to the public, at least the storage, modification, erasure, and destruction of the data shall be logged.

[4] The logging must provide information on the identity of the person who carried out the processing, the nature, date, and time of the processing and, if applicable, the identity of the recipient of the data.

[5] The logs are kept for at least one year, separate from the system in which the personal data is processed. They shall be

données personnelles sont traitées. Ils sont accessibles uniquement aux organes et aux personnes chargés de vérifier l'application des dispositions relatives à la protection des données personnelles ou de préserver ou de restaurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données, et ne peuvent être utilisés qu'à cette fin.

accessible only to the bodies and persons responsible for verifying the application of the provisions on the protection of personal data or for preserving or restoring the confidentiality, integrity, availability, and traceability of the data, and may only be used for this purpose.

Art. 5 Règlement de traitement des personnes privées

[1] Le responsable du traitement privé et son sous-traitant privé établissent un règlement pour les traitements automatisés en cas:

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

[2] Le règlement comprend en particulier des informations sur l'organisation interne, sur les procédures de traitement et de contrôle des données, ainsi que sur les mesures visant à garantir la sécurité des données.

[3] Le responsable du traitement privé et son sous-traitant privé actualisent régulièrement le règlement. S'ils ont nommé un conseiller à la protection des données, ils mettent le règlement à sa disposition.

Art. 5 Processing regulations for private persons

[1] The private controller and its private processor shall establish a regulation for the automated processing in case:

a. of large-scale processing of sensitive data, or
b. of high risk profiling.

[2] The regulations shall include information on the internal organization, on procedures for data processing and control, and on the measures to ensure data security.

[3] The private controller and its private data processor shall regularly update the regulations. If they have appointed a data protection officer, they shall make the regulations available to him.

Art. 6 Règlement de traitement des organes fédéraux

[1] L'organe fédéral responsable et son sous-traitant établissent un règlement pour les traitements automatisés en cas:

a. de traitement de données sensibles;
b. de profilage;
c. de traitement de données personnelles au sens de l'art. 34, al. 2, let. c, LPD;
d. d'accès aux données personnelles accordé aux cantons, aux autorités étrangères, aux organisations internationales ou aux personnes privées;
e. d'ensembles de données interconnectés, ou
f. d'exploitation d'un système d'information ou de gestion d'ensembles de données conjointement avec d'autres organes fédéraux.

[2] Le règlement comprend en particulier des informations sur l'organisation interne, sur les procédures de traitement et de contrôle des données, ainsi que sur les mesures visant à garantir la sécurité des données.

[3] L'organe fédéral responsable et son sous-traitant actualisent régulièrement le règlement et le mettent à la disposition du conseiller à la protection des données.

Art. 6 Data processing regulations for federal bodies

[1] The federal body (controller) and its processor shall draw up regulations for the automated processing in case:

a. of processing of sensitive data;
b. of profiling;
c. of processing of personal data within the meaning of Art. 34 (2) (c) DPA;
d. of access to personal data granted to cantons, foreign authorities, international organizations, or private persons;
e. of interconnected data sets, or
f. of information system operation or data set management in conjunction with other federal bodies.

[2] The regulations shall include information on the internal organization, on the procedures for data processing and control, and on the measures to ensure data security.

[3] The federal body (controller) and its processor shall regularly update the regulations and make them available to the data protection officer.

Section 2: Sous-traitance

Art. 7

[1] L'autorisation préalable du responsable du traitement permettant au sous-traitant de confier le traitement des données à un tiers peut être de nature spécifique ou générale.

[2] En cas d'autorisation générale, le sous-traitant informe le responsable du traitement lorsqu'il envisage de recourir à d'autres tiers ou de les remplacer. Le responsable du traitement peut s'opposer à cette modification.

Section 3 Communication de données personnelles à l'étranger

Art. 8 Évaluation du niveau de protection adéquat des données d'un État, d'un territoire, d'un secteur déterminé dans un État, ou d'un organisme international

[1] Les États, les territoires, les secteurs déterminés dans un État, et les organismes internationaux avec un niveau de protection adéquat sont mentionnés à l'annexe 1.

[2] Pour évaluer si un État, un territoire, un secteur déterminé dans un État, ou un organisme international garantit un niveau de protection adéquat, les critères suivants sont en particulier pris en compte :

a. les engagements internationaux de l'État ou de l'organisme international, notamment en matière de protection des données;
b. l'état de droit et le respect des droits de l'homme;
c. la législation applicable, notamment en matière de protection des données, de même que sa mise en œuvre et la jurisprudence y relative;
d. la garantie effective des droits des personnes concernées et des voies de droit;
e. le fonctionnement effectif d'une ou de plusieurs autorités indépendantes chargées de la protection des données dans l'État concerné, ou auxquelles un organisme international est soumis, et disposant de pouvoirs et de compétence suffisants.

[3] Le Préposé fédéral à la protection des données et à la transparence (PFPDT) est consulté lors de chaque évaluation. Les appréciations effectuées par des organismes internationaux ou des autorités étrangères chargées de la protection des données peuvent être prises en compte.

[4] L'adéquation du niveau de protection est réévaluée périodiquement.

[5] Les évaluations doivent être publiées.

[6] Lorsque l'évaluation visée à l'al. 4 ou que d'autres informations indiquent que le niveau de protection adéquat

Section 2: Processor

Art.7

[1] The prior authorization of the controller allowing the processor to entrust the processing of data to a third party may be specific or general in nature.

[2] In the case of general authorization, the processor shall inform the controller when it intends to use other third parties or to replace them. The controller may object to this change.

Section 3 Cross-border transfer of personal data

Art. 8 Assessment of the adequacy of data protection of a State, territory, specific sector within a State, or international organization

[1] States, territories, specific sectors within a State, and international organizations with an adequate level of protection are listed in Appendix 1.

[2] In order to assess whether a state, a territory, a specific sector within a state, or an international organization guarantees an adequate level of protection, the following criteria shall be considered:

a. the international commitments of the State or international organization, particularly regarding data protection;
b. the rule of law and respect for human rights;
c. the applicable legislation, regarding data protection, as well as its implementation and the related case law;
d. the effective guarantee of the data subjects rights and of the legal remedies;
e. the effective functioning of one or more independent data protection authorities in the relevant State, or to which an international organization is subject, with sufficient powers and competence.

[3] The Federal Data Protection and Information Commissioner (FDPIC) is consulted in every assessment. Assessments by international bodies or foreign data protection authorities may be considered.

[4] The adequacy of the level of protection is periodically reassessed.

[5] Evaluations must be published.

[6] If the assessment in accordance with paragraph 4 or other information indicates that the adequate level of protection is

n'est plus garanti, l'annexe 1 est modifiée sans effet surles communications de données déjà effectuées.

Art. 9 Clauses de protection des données d'un contrat et garanties spécifiques

[1] Les clauses de protection des données d'un contrat au sens de l'art. 16, al. 2, let. b, LPD et les garanties spécifiques au sens de l'art. 16, al. 2, let. c, LPD comprennent aumoins les points suivants:

a. l'application des principes de licéité, de bonne foi, de proportionnalité, de transparence, de finalité et d'exactitude;
b. les catégories de données communiquées et de personnes concernées;
c. le type et la finalité de la communication des données personnelles;
d. le cas échéant, le nom des États ou des organismes internationaux auxquels sont destinées les données personnelles, et les conditions applicables à la communication;
e. les conditions applicables à la conservation, à l'effacement et à la destruction des données personnelles;
f. les destinataires ou les catégories de destinataires;
g. les mesures visant à garantir la sécurité des données;
h. l'obligation d'annoncer les violations de la sécurité des données;
i. l'obligation pour le destinataire, lorsqu'il est responsable du traitement, d'informer les personnes concernées par le traitement des données;
j. les droits de la personne concernée, en particulier:
    1. le droit d'accès et le droit à la remise ou à la transmission des données personnelles,
    2. le droit de s'opposer à la communication des données,
    3. le droit de demander la rectification, l'effacement ou la destruction desdonnées,
    4. le droit de saisir en justice une autorité indépendante.

[2] Le responsable du traitement, ou, dans le cas de clauses de protection des données d'un contrat, le sous-traitant, prend les mesures adéquates pour s'assurer que le destinataire respecte ces clauses ou les garanties spécifiques.

[3] Une fois les clauses de protection des données d'un contrat ou les garanties spécifiques annoncées au PFPDT, le devoir d'information du responsable du traitement est réputé également rempli pour toutes les communications :

a. qui se fondent sur les mêmes clauses ou garanties,

no longer guaranteed, Appendix 1 shall be amended without affecting the data transfers already made.

Art 9 Data protection clauses of a contract and specific guarantees

[1] The data protection clauses of a contract within the meaning of Art. 16 (2) (b) DPA and the specific guarantees within the meaning of Art. 16 (2) (c) DPA shall include at least the following points:

a. the application of the principles of lawfulness, good faith, proportionality, transparency, purpose, and accuracy;
b. the categories of data communicated and of data subjects;
c. the type and purpose of the personal data communication;
d. where applicable, the names of the States or international bodies to which the personal data are destined, and the conditions applicable to the transfer;
e. the conditions applicable to the retention, erasure, and destruction of personal data;
f. the recipients or categories of recipients;
g. measures to ensure data security;
h. the obligation to notify data security breaches;
i. the obligation of the recipient, when it is controller, to inform the data subjects;
j. the rights of the data subject, in particular:
    1. the right of access and the right to the delivery or transmission of personal data,
    2. the right to object to the communication of data,
    3. the right to request the rectification, erasure, or destruction of data,
    4. the right to seek legal protection from an independent authority.

[2] The controller or, in the case of data protection clauses in a contract, the processor, shall take appropriate measures to ensure that the recipient complies with these clauses or with the specific guarantees.

[3] Once the data protection clauses of a contract or specific guarantees have been notified to the FDPIC, the duty to inform of the controller is deemed to have been fulfilled for all communications:

a. which are based on the same clauses or guarantees,

pour autant que les catégories de destinataires, les finalités du traitement et les catégories de données communiquées soient similaires, ou

b. qui sont effectuées au sein d'une même personne morale ou société ou entre des entreprises appartenant au même groupe.

provided that the categories of recipients, the purposes of the processing and the categories of data communicated are similar, or

b. that are made within the same legal person or company or between companies belonging to the same group.

Art. 10 Clauses types de protection des données

[1] Lorsque le responsable du traitement ou le sous-traitant communique des données personnelles à l'étranger au moyen de clauses types de protection des données au sens de l'art. 16, al. 2, let. d, LPD, il prend les mesures adéquates pour s'assurer que le destinataire les respecte.

[2] Le PFPDT publie une liste des clauses types de protection des données qu'il a approuvées, établies ou reconnues. Il communique le résultat de l'examen sur les clauses types qui lui sont soumises dans un délai de 90 jours.

Art. 10 Standard data protection clauses

[1] If the controller or processor transfers personal data abroad by means of standard data protection clauses within the meaning of Art. 16 (2) (d) DPA, it shall take appropriate measures to ensure that the recipient complies with them.

[2] The FDPIC shall publish a list of the standard data protection clauses that he has approved, established or recognized. He shall communicate the result of the examination of the model clauses submitted to him within 90 days.

Art. 11 Règles d'entreprise contraignantes

[1] Les règles d'entreprise contraignantes au sens de l'art. 16, al. 2, let. e, LPD s'appliquent à toutes les entreprises appartenant au même groupe.

[2] Elles portent au moins sur les points mentionnés à l'art. 9, al. 1, ainsi que sur lespoints suivants:

a. la structure et les coordonnées du groupe d'entreprises et de chacune de ses entités;

b. les mesures mises en place au sein des groupes d'entreprises pour garantir le respect des règles d'entreprise contraignantes.

[3] Le PFPDT communique le résultat de l'examen sur les règles d'entreprise contraignantes qui lui sont soumises dans un délai de 90 jours.

Art. 11 Binding corporate rules

[1] Binding corporate rules within the meaning of Art. 16 (2) (e) DPA apply to all companies belonging to the same group.

[2] They shall cover at least the points mentioned in Art. 9 (1) as well as the following points:

a. the structure and contact details of the group of companies and each of its entities;

b. the measures put in place within groups of companies to ensure compliance with binding corporate rules.

[3] The FDPIC shall communicate the result of the examination on the binding corporate rules submitted to him within 90 days.

Art. 12 Codes de conduite et certifications

[1] Des données personnelles peuvent être communiquées à l'étranger à condition qu'un code de conduite ou qu'une certification garantisse un niveau de protection approprié.

[2] Le code de conduite est préalablement soumis au PFPDT pour approbation.

[3] Le code de conduite ou la certification doit être assorti d'un engagement contraignant et exécutoire par lequel le responsable du traitement ou le sous-traitant dans l'État tiers garantit qu'il applique les mesures contenues dans ces instruments.

Art. 12 Codes of conduct and certifications

[1] Personal data may be transferred abroad provided that a code of conduct or certification guarantees an appropriate level of protection.

[2] The code of conduct is first submitted to the FDPIC for approval.

[3] The code of conduct or certification must be accompanied by a binding and enforceable commitment by which the controller or processor in the third State guarantees that it will apply the measures contained in these instruments.

Chapitre 2 Obligations du responsable du traitement

Art. 13 Modalités du devoir d'informer

Le responsable du traitement communique aux personnes

Chapter 2 Obligations of the controller

Art. 13 Modalities of the duty to inform

The controller shall provide the data subjects with information

concernées les informations sur la collecte de données personnelles de manière concise, transparente, compréhensible et facilement accessible.

on the collection of personal data in a concise, transparent, comprehensible, and easily accessible manner.

Art. 14 Conservation de l'analyse d'impact relative à la protection desdonnées personnelles

Le responsable du traitement conserve l'analyse d'impact relative à la protection des données personnelles pendant au moins deux ans après la fin du traitement des données.

Art. 14 Retention of the data protection impact assessment

The controller shall keep the data protection impact assessment for at least two years after the end of the data processing.

Art. 15 Annonce des violations de la sécurité des données

[1] L'annonce au PFPDT d'une violation de la sécurité des données comprend les informations suivantes:

a. la nature de la violation;
b. dans la mesure du possible, le moment et la durée;
c. dans la mesure du possible, les catégories et le nombre approximatif de données personnelles concernées;
d. dans la mesure du possible, les catégories et le nombre approximatif de personnes concernées;
e. les conséquences, y compris les risques éventuels, pour les personnes concernées;
f. les mesures prises ou prévues pour remédier à cette défaillance et atténuer lesconséquences, y compris les risques éventuels;
g. le nom et les coordonnées d'une personne de contact.

[2] Si le responsable du traitement n'est pas en mesure d'annoncer simultanément toutes les informations, il fournit les informations manquantes dans les meilleurs délais.

[3] Si le responsable du traitement est tenu d'informer la personne concernée, il lui communique, dans un langage simple et compréhensible, au moins les informations visées à l'al. 1, let. a et e à g.

[4] Le responsable du traitement documente les violations. La documentation contient les faits relatifs aux incidents, à leurs effets et aux mesures prises. Elle est conservée pendant au moins deux ans à compter de la date d'annonce au sens de l'al. 1.

Art. 15 Notification of data security breaches

[1] The notification to the FDPIC of a data security breach includes the following information:

a. the nature of the breach;
b. to the extent possible, the timing and duration;
c. to the extent possible, the categories and approximate number of personal data involved;
d. to the extent possible, the categories and approximate number of data subjects;
e. the consequences, including possible risks, for the data subjects;
f. measures taken or planned to remedy the failure and mitigate the consequences, including any risks;
g. the name and contact details of a contact person.

[2] If the controller is unable to provide all the information simultaneously, he shall provide the missing information as soon as possible.

[3] If the controller is obliged to inform the data subject, he shall provide him with at least the information referred to in paragraph 1 (a) and (e) to (g).

[4] The controller documents the breaches. The documentation shall contain the facts about the incidents, their effects and the measures taken. It shall be kept for at least two years from the date of notification in accordance with paragraph 1.

Chapitre 3: Droits de la personne concernée

Section 1: Droit d'accès

Art. 16 Modalités

[1] Toute personne qui demande au responsable du traitement si des données personnelles la concernant sont traitées doit le faire par écrit. La demande peut être faite oralement

Chapter 3: Rights of the data subject

Section1: Access right

Art. 16 Modalities

[1] Any person who asks the controller whether personal data relating to him or her is being processed must do so in writing. The request may be made orally with the consent of the

moyennant l'accord du responsable du traitement.
[2] Les renseignements sont communiqués par écrit ou sous la forme dans laquelle les données se présentent. D'entente avec le responsable du traitement, la personne concernée peut consulter ses données sur place. Si elle y consent, les renseignements peuvent lui être fournis oralement.
[3] La demande de renseignement et la communication des renseignements peuvent être effectuées par voie électronique.
[4] Les renseignements sont communiqués sous une forme compréhensible pour la personne concernée.
[5] Le responsable du traitement prend des mesures adéquates pour identifier la personne concernée. Celle-ci est tenue de coopérer.

controller.
[2] The information shall be provided in writing or in the form in which the data is presented. In agreement with the controller, the data subject may inspect his or her data on site. If the data subject consents, the information may be provided orally.

[3] The request for information and the provision of information may be made by electronic means.

[4] The information shall be provided in a form that is comprehensible to the data subject.
[5] The controller shall take appropriate measures to identify the data subject. The data subject is obliged to cooperate.

Art. 17 Responsabilité

[1] Lorsque plusieurs responsables traitent en commun des données personnelles, la personne concernée peut exercer son droit d'accès auprès de chacun d'eux.
[2] Si la demande de renseignement porte sur des données traitées par un sous-traitant,celui-ci aide le responsable du traitement à fournir les renseignements pour autant qu'il ne réponde pas lui-même à la demande pour le compte du responsable du traitement.

Art. 17 Liability

[1] If several controllers process personal data jointly, the data subject may exercise his or her access right with each of them.

[2] If the request for information relates to data processed by a processor, the processor shall assist the controller in providing the information if it does not itself respond to the request on behalf of the controller.

Art. 18 Délais

[1] Les renseignements sont fournis dans les 30 jours suivant la réception de la demande.
[2] Si les renseignements ne peuvent être donnés dans les 30 jours, le responsable du traitement en informe la personne concernée en lui indiquant le délai dans lequel les renseignements seront fournis.
[3] Si le responsable du traitement refuse, restreint ou diffère le droit d'accès, il le communique dans le même délai.

Art. 18 Time limits

[1] Information is provided within 30 days of receipt of the request.
[2] If the information cannot be provided within 30 days, the controller shall inform the data subject of this fact and the time limit within which the information will be provided.

[3] If the controller refuses, restricts, or postpones the access right, he shall notify this within the same deadline.

Art. 19 Exception à la gratuité

[1] Si la communication des renseignements occasionne des efforts disproportionnés, le responsable du traitement peut exiger que la personne concernée participe aux coûts de manière adéquate.
[2] Le montant de la participation s'élève à 300 francs au maximum.
[3] Le responsable du traitement informe la personne concernée du montant avant de lui communiquer les renseignements. Si la personne concernée ne confirme pas sa demande dans les 10 jours, celle-ci est considérée comme retirée sans occasionner de frais. Le délai prévu à l'art. 18, al. 1, commence à courir à l'expiration du délai de réflexion de

Art. 19 Exception to free of charge

[1] If the provision of information involves disproportionate efforts, the controller may require the data subject to contribute to the costs in an appropriate manner.

[2] The amount of the contribution is a maximum of 300 Swiss francs.
[3] The controller shall inform the data subject of the amount before providing the information. If the data subject does not confirm his or her request within 10 days, the request is deemed to have been withdrawn without incurring any costs. The period provided for in Art. 18 (1) begins to run on the expiry of the 10 days.

10 jours.

Section 2: Droit à la remise ou à la transmission des donnéespersonnelles

Art. 20 Étendue du droit

[1] Sont considérées comme des données personnelles que la personne concernée a communiquées au responsable du traitement:

a. les données qu'elle a mises à sa disposition délibérément et en connaissance de cause;
b. les données que le responsable du traitement a collectées au sujet de la personne concernée et qui concernent son comportement dans le cadre de l'utilisation d'un service ou d'un appareil.

[2] Ne sont pas considérées comme des données personnelles que la personne concernée a communiquées au responsable du traitement, les données personnelles que celui-ci a générées en évaluant les données personnelles mises à disposition ou observées.

Art. 21 Exigences techniques de mise en œuvre

[1] Les formats électroniques couramment utilisés sont les formats qui permettent, moyennant un effort proportionné, de transmettre les données personnelles en vue de leur réutilisation par la personne concernée ou par un autre responsable du traitement.

[2] Le droit à la remise ou à la transmission des données personnelles ne crée pas d'obligation pour le responsable du traitement d'adopter ou de conserver des systèmes de traitement de données techniquement compatibles.

[3] L'effort est disproportionné lorsque la transmission de données personnelles à un autre responsable du traitement n'est pas possible pour des raisons techniques.

Art. 22 Délais, modalités et responsabilité

Les art. 16, al. 1 et 5, et 17 à 19 s'appliquent par analogie à la remise ou à la transmission des données personnelles.

Chapitre 4 Dispositions particulières pour le traitement de données personnelles par des personnes privées

Art. 23 Conseiller à la protection des données

Le responsable du traitement:

a. met les ressources nécessaires à la disposition du conseiller à la protection des données;
b. donne accès au conseiller à la protection des données à tous les renseignements, les documents, les registres des activités de traitement et à toutes les

Section 2: Right to the delivery or transmission of personal data

Art. 20 Extent of the right

[1] Personal data that the data subject has provided to the controller are:

a. data that the data subject has made available to the controller deliberately and knowingly;
b. data that the controller has collected about the data subject and that relate to his or her behavior in connection with the use of a service or device.

[2] Personal data that the data subject has provided to the controller shall not include personal data that the controller has generated by evaluating the personal data provided or monitored.

Art. 21 Technical requirements for implementation

[1] Commonly used electronic formats are those formats that allow, with a proportionate effort, personal data to be transmitted for re-use by the data subject or by another controller.

[2] The right to hand over or transfer personal data does not create an obligation for the controller to adopt or maintain technically compatible data processing systems.

[3] The effort is disproportionate if the transmission of personal data to another controller is not possible for technical reasons.

Art. 22 Time limits, procedures, and liability

Art. 16 (1) and (5), and (17) to (19) apply by analogy to the provision or transmission of personal data.

Chapter 4 Special provisions for the processing of personal data by private persons

Art. 23 Data protection officer

The controller:

a. provides the necessary resources to the data protection officer;
b. gives the data protection officer access to all information, documents, registers of processing activities and personal data that he needs to carry out

données personnelles dont il a besoin pour l'accomplissement de ses tâches;

c. donne au conseiller à la protection des données le droit d'informer l'organe supérieur de direction ou d'administration dans les cas importants.

his duties;

c. gives the data protection officer the right to inform the higher management or administrative body in important cases.

Art. 24 Exception à l'obligation de tenir un registre des activités detraitement

Les entreprises et autres organismes de droit privé employant moins de 250 collaborateurs au 1er janvier d'une année, ainsi que les personnes physiques, sont déliés de leur obligation de tenir un registre des activités de traitement, à moins que l'une des conditions suivantes soit remplie:

a. le traitement porte sur des données sensibles à grande échelle;

b. le traitement constitue un profilage à risque élevé.

Art. 24 Exception to the obligation to keep a register of processing activities

Companies and other private organizations with fewer than 250 employees as of January 1 of a year, as well as natural persons, are exempted from the obligation to keep a register of processing activities, unless one of the following conditions is fulfilled:

a. the processing involves large-scale sensitive data;

b. the processing constitutes high-risk profiling.

Chapitre 5: Dispositions particulières pour le traitement de données personnelles par des organes fédéraux

Section 1: Conseiller à la protection des données

Art. 25 Désignation

Tout organe fédéral désigne un conseiller à la protection des données. Plusieurs organes fédéraux peuvent désigner ensemble un conseiller

Chapter 5: Special provisions applicable to the processing of personal data by federal bodies

Section 1: Data protection officer

Art. 25 Designation

Each federal body shall appoint a data protection officer. Several federal bodies may jointly appoint a data protection officer.

Art. 26 Exigences et tâches

[1] Le conseiller à la protection des données remplit les conditions suivantes:

a. il dispose des connaissances professionnelles nécessaires;

b. il exerce sa fonction de manière indépendante par rapport à l'organe fédéral et sans recevoir d'instruction de celui-ci.

[2] Il accomplit les tâches suivantes:

a. participer à l'application des dispositions relatives à la protection des données,en particulier:

b. en contrôlant le traitement de données personnelles et en proposant des mesures correctives lorsqu'une violation des dispositions relatives à la protection des données est constatée;

c. en conseillant le responsable du traitement lors de l'établissement de l'analyse d'impact relative à la protection des données et en vérifiant sonexécution;

d. servir d'interlocuteur pour les personnes concernées;

e. former et conseiller les collaborateurs de l'organe fédéral en matière de protection des données.

Art. 26 Requirements and tasks

[1] The data protection officer fulfils the following requirements:

a. he has the necessary professional knowledge;

b. he exercises his function independently of the federal body and without receiving instructions from it.

[2] He performs the following tasks:

a. participating in the application of the provisions relating to data protection, in particular:

b. monitoring the processing of personal data and proposing corrective measures when a breach of data protection provisions is detected;

c. advising the controller in the preparation of the data protection impact assessment and verifying its execution;

d. serving as a point of contact for the data subjects;

e. training and advising the staff of the federal body on data protection.

Art. 27 Devoirs de l'organe fédéral	**Art. 27 Duties of the federal body**
[1] L'organe fédéral doit:	[1] The federal body shall:
a. donner au conseiller à la protection des données accès à tous les renseignements, les documents, les registres des activités de traitement et à toutes les données personnelles dont celui-ci a besoin pour l'accomplissement de ses tâches;	a. provide the data protection officer with access to all information, documents, registers of processing activities and personal data that the data protection officer needs to perform his duties;
b. veiller à ce que le conseiller à la protection des données soit informé de toute violation de la sécurité des données.	b. Ensure that the data protection advisor is informed of any data security breach.
[2] Il publie les coordonnées du conseiller à la protection des données en ligne et les communique au PFPDT.	[2] It publishes the contact details of the data protection officer online and communicates them to the FDPIC.
Art. 28 Interlocuteur du PFPDT	**Art. 28 FDPIC contact person**
Le conseiller à la protection des données personnelles est l'interlocuteur du PFPDT pour les questions relatives au traitement des données par l'organe fédéral concerné.	The data protection officer is the FDPIC's contact person for questions relating to the processing of data by the relevant federal body.
Section 2 Devoir d'informer	**Section 2 Duty to inform**
Art. 29 Devoir d'informer lors de la communication des données personnelles	**Art. 29 Duty to inform when communicating personal data**
L'organe fédéral indique au destinataire l'actualité, la fiabilité et l'exhaustivité des données personnelles qu'il communique, dans la mesure où ces informations ne ressortent pas des données elles-mêmes ou des circonstances.	The federal body shall inform the recipient of the timeliness, reliability, and completeness of the personal data it provides, insofar as this information is not derived from the data itself or from the circumstances.
Art. 30 Devoir d'informer lors de la collecte systématique des données personnelles	**Art. 30 Duty to inform when personal data are systematically collected**
Si la personne concernée n'est pas tenue de fournir des renseignements, l'organe fédéral qui collecte systématiquement des données personnelles doit l'en informer.	If the data subject is not required to provide information, the federal body that systematically collects personal data must inform the data subject.
Section 3: Annonce au PFPDT des projets pour le traitement automatisé des données personnelles	**Section 3: Notification to the FDPIC of projects for the automated processing of personal data**
Art.31	**Art. 31**
[1] L'organe fédéral responsable annonce au PFPDT les activités prévues de traitement automatisé au moment de l'approbation du projet ou de la décision de le développer.	[1] The controller (federal body) shall notify the FDPIC of planned automated processing activities at the time of project approval or decision to develop the project.
[2] L'annonce contient les indications prévues à l'art. 12, al. 2, let. a à d, LPD, ainsi que la date prévue pour le début des activités de traitement.	[2] The notification shall include the information specified in Art. 12 (2) (a) to (d) DPA, as well as the planned start date of the processing activities.
[3] Le PFPDT enregistre cette annonce dans le registre des activités de traitement.	[3] The FDPIC records this notification in the register of processing activities.
[4] L'organe fédéral responsable actualise cette annonce lors du passage à la phase de production ou lorsque le projet est	[4] The federal body (controller) shall update this notification when the project enters the production phase or is

abandonné.

Section 4: Essais pilotes

Art. 32 Caractère indispensable de l'essai pilote

Un essai pilote est indispensable si l'une des conditions suivantes est remplie:

a. l'accomplissement des tâches nécessite l'introduction d'innovations techniques dont les effets doivent être évalués;
b. l'accomplissement des tâches nécessite la prise de mesures organisationnelles ou techniques importantes dont l'efficacité doit être examinée, notamment dans le cadre d'une collaboration entre les organes fédéraux et les cantons;
c. l'accomplissement des tâches nécessite de rendre accessibles en ligne les données personnelles.

Art. 33 Procédure d'autorisation de l'essai pilote

[1] Avant de consulter les unités administratives concernées, l'organe fédéral responsable de l'essai pilote communique au PFPDT de quelle manière il est prévu d'assurer que les conditions de l'art. 35 LPD soient remplies et l'invite à prendre position.

[2] Le PFPDT prend position sur le respect des conditions de l'art. 35 LPD. À cet effet,l'organe fédéral lui remet tous les documents nécessaires et en particulier:

a. un descriptif général de l'essai pilote;
b. un rapport démontrant que l'accomplissement des tâches légales nécessite un traitement selon l'art. 34, al. 2, LPD et rend indispensable une phase d'essai avant l'entrée en vigueur de la loi au sens formel;
c. un descriptif de l'organisation interne et des processus de traitement et de contrôle des données;
d. un descriptif des mesures de sécurité et de protection des données;
e. un projet d'ordonnance réglant les modalités de traitement ou les grandes lignes de cet acte législatif;
f. la planification des différentes phases de l'essai pilote.

[3] Le PFPDT peut exiger d'autres documents et procéder à des vérifications complémentaires.

[4] L'organe fédéral informe le PFPDT de toute modification essentielle portant sur le respect des conditions de l'art. 35 LPD. Si nécessaire, le PFPDT prend à nouveau position.

[5] La prise de position du PFPDT est annexée à la proposition adressée au Conseil fédéral.

[6] Le traitement automatisé est réglé par voie d'ordonnance.

abandoned.

Section 4: Pilot projects

Art. 32 Imperative nature of the pilot project

A pilot project is required if either of the following conditions is fulfilled:

a. the accomplishment of tasks requires the introduction of technical innovations whose effects must be evaluated;
b. the fulfilment of the tasks requires important organizational or technical measures, the effectiveness of which must be examined, within the framework of collaboration between the federal bodies and the cantons;
c. the completion of tasks requires making personal data available online.

Art. 33 Procedure for authorizing the pilot project

[1] Before consulting the relevant administrative units, the federal body (controller) for the pilot project shall inform the FDPIC of how it intends to ensure that the requirements of Art. 35 DPA are met and shall invite him to take position.

[2] The FDPIC shall take a position on whether the requirements of Art. 35 DPA are met. To this end, the federal body shall provide it with all the necessary documents, in particular

a. a general description of the pilot project;
b. a report demonstrating that the fulfilment of the legal tasks requires processing in accordance with Art. 34 (2) DPA and makes a test phase indispensable before the formal law comes into force;
c. a description of the internal organization and processes for data processing and control;
d. a description of the security and data protection measures;
e. a draft ordinance regulating the processing methods or the broad outlines of this legislative act;
f. the planning of the different phases of the pilot project.

[3] The FDPIC may require additional documentation and conduct additional audits.

[4] The federal body shall inform the FDPIC of any significant changes in the fulfilment of the requirements of Art. 35 DPA. If necessary, the FDPIC shall take a new position.

[5] The FDPIC's position paper is attached to the proposal to the Federal Council.

[6] Automated processing shall be regulated by ordinance.

Art. 34 Rapport d'évaluation

[1] L'organe fédéral responsable soumet le projet de rapport d'évaluation à l'intention du Conseil fédéral au PFPDT pour prise de position.

[2] Il soumet le rapport d'évaluation accompagné de la prise de position du PFPDT au Conseil fédéral.

Art. 34 Evaluation report

[1] The federal body (controller) submits the draft evaluation report intended to the Federal Council to the FDPIC for comment.

[2] It shall submit the evaluation report together with the FDPIC's position paper to the Federal Council.

Section 5: Traitement des données à des fins ne se rapportant pas àdes personnes

Art. 35

Lorsque des données personnelles sont traitées à des fins ne se rapportant pas à des personnes, en particulier à des fins de recherche, de planification ou de statistique, et que le traitement sert également une autre finalité, les dérogations prévues à l'art. 39, al. 2, LPD ne s'appliquent qu'au seul traitement effectué à des fins ne se rapportant pas à des personnes.

Section 5: Data processing for purposes not relating to individuals

Art. 35

Where personal data are processed for purposes that do not relate to individuals, in particular for research, planning or statistical purposes, and the processing also serves another purpose, the exemptions provided for in Art. 39 (2) DPA apply only to the processing for purposes that do not relate to individuals.

Chapitre 6 Préposé fédéral à la protection des données et à la transparence

Art. 36 Siège et secrétariat permanent

[1] Le siège du PFPDT est à Berne.

[2] Les rapports de travail du personnel du secrétariat permanent du PFPDT sont régis par la législation sur le personnel de la Confédération. Le personnel est assuré auprès de la Caisse de prévoyance de la Confédération.

Chapter 6 Federal Data Protection and Information Commissioner

Art. 36 Headquarters and permanent secretariat

[1] The FDPIC is based in Bern.

[2] The employment relationship of the staff of the FDPIC permanent secretariat is governed by the legislation on federal employees. The staff is insured with the Swiss Federal Pension Fund.

Art. 37 Voie de communication

[1] Le PFPDT communique avec le Conseil fédéral par l'intermédiaire du chancelier de la Confédération. Celui-ci transmet les propositions, les prises de positions et les rapports au Conseil fédéral sans les modifier.

[2] Le PFPDT transmet les rapports destinés à l'Assemblée fédérale par l'intermédiairedes Services du Parlement.

Art. 37 Communication channel

[1] The FDPIC communicates with the Federal Council through the Federal Chancellor. The Federal Chancellor shall forward proposals, statements, and reports to the Federal Council unchanged.

[2] The FDPIC shall forward the reports to the Federal Assembly via the Parliamentary Services.

Art. 38 Communication des décisions, des directives et des projets

[1] En matière de protection des données, les départements et la Chancellerie fédérale communiquent au PFPDT leurs décisions sous forme anonyme, ainsi que leurs directives.

[2] Les organes fédéraux soumettent au PFPDT tous leurs projets législatifs concernant le traitement de données personnelles, la protection des données et l'accès aux documents officiels.

Art. 38 Communication of decisions, directives, and projects

[1] The departments and the Federal Chancellery shall notify the FDPIC of their data protection decisions in anonymous form as well as of their directives.

[2] The federal bodies shall submit all their legislative proposals concerning the processing of personal data, data protection and access to official documents to the FDPIC.

Art. 39 Traitement des données

Le PFPDT peut traiter les données personnelles, y compris les données sensibles, notamment aux fins suivantes:

a. exercer ses activités de surveillance;
b. exercer ses activités de conseil;
c. collaborer avec les autorités cantonales, fédérales et étrangères;
d. exécuter des tâches dans le cadre des dispositions pénales au sens de la LPD;
e. mettre en œuvre des procédures de conciliation et émettre des recommandations au sens de la loi du 17 décembre 2004 sur la transparence (LTrans)[1];
f. mettre en œuvre des évaluations au sens de la LTrans;
g. mettre en œuvre des procédures de demande d'accès au sens de la LTrans;
h. informer la surveillance parlementaire;
i. informer le public;
j. exercer ses activités de formation.

Art. 39 Data processing

The FDPIC may process personal data, including sensitive data, for the following purposes:

a. to carry out its monitoring activities;
b. to carry out its consulting activities;
c. to collaborate with cantonal, federal, and foreign authorities;
d. to perform tasks within the framework of the criminal provisions of the DPA;
e. to implement conciliation procedures and issue recommendations within the meaning of the Freedom of Information Act dated December 17, 2004 (FoIA)[2];
f. to implement assessments under the FoIA;
g. to implement access request procedures under the FoIA;
h. to inform parliamentary oversight;
i. to inform the public;
j. to carry out its training activities.

Art. 40 Autocontrôle

Le PFPDT établit un règlement pour tous les traitements automatisés; l'art. 6, al. 1, ne s'applique pas.

Art. 40 Self-control

The FDPIC shall issue regulations for all automated processing operations; Art. 6 (1) shall not apply.

Art. 41 Collaboration avec le NCSC

[1] Le PFPDT peut, avec l'accord du responsable du traitement tenu d'annoncer, transmettre l'annonce d'une violation de la sécurité des données au Centre national pour la cybersécurité (NCSC) pour que celui-ci analyse l'incident. La communication peut contenir des données personnelles.

[2] Le PFPDT invite le NCSC à se prononcer avant d'ordonner à l'organe fédéral de prendre les mesures visées à l'art. 8 LPD.

Art. 41 Collaboration with the NCSC

[1] The FDPIC may, with the consent of the controller required to notify, transfer the notification of a data security breach to the National Center for Cyber Security (NCSC) for analysis of the incident. The communication may contain personal data.

[2] The FDPIC invites the NCSC to comment before ordering the federal body to act under Art. 8 DPA.

Art. 42 Registre des activités de traitement des organes fédéraux

[1] Le registre des activités de traitement des organes fédéraux contient les informations fournies par les organes fédéraux conformément aux art. 12, al. 2, LPD et 31, al. 2, de la présente ordonnance.

[2] I est publié en ligne. Les inscriptions au registre concernant les activités de traitement automatisé prévues, au sens de l'art. 31, ne sont pas publiées.

Art. 42 Register of processing activities of federal bodies

[1] The register of processing activities of federal bodies contains the information provided by the federal bodies in accordance with Art. 12 (2) DPA and 31 (2) of this ordinance.

[2] It shall be published online. Entries in the register concerning planned automated processing activities in accordance with Art. 31 shall not be published.

Art. 43 Codes de conduite

Si un code de conduite est soumis au PFPDT, celui-ci indique dans sa prise de positionsi le code de conduite remplit les

Art. 43 Code of conduct

If a code of conduct is submitted to the FDPIC, the FDPIC will indicate in its statement whether the code of conduct meets

[1] RS **152.3**

conditions de l'art. 22, al. 5, let. a et b, LPD.

Art. 44 Émolument

[1] L'émolument perçu par le PFPDT se calcule en fonction du temps consacré.

[2] Le tarif horaire varie entre 150 et 250 francs, selon la fonction exercée par la personne concernée.

[3] Pour les prestations d'une ampleur extraordinaire, présentant des difficultés particulières ou ayant un caractère urgent, des suppléments pouvant atteindre 50 % de l'émolument prévu à l'al. 2 peuvent être perçus.

[4] Si la prestation du PFPDT peut être réutilisée à des fins commerciales par la personne assujettie à l'émolument, des suppléments pouvant atteindre 100 % de l'émolument prévu à l'al. 2 peuvent être perçus.

[5] L'ordonnance générale du 8 septembre 2004 sur les émoluments[2] s'applique pour le reste.

Chapitre 7 Dispositions finales

Art. 45 Abrogation et modification d'autres actes

L'abrogation et la modification d'autres actes sont réglées à l'annexe 2.

Art. 46 Dispositions transitoires

[1] Pour les traitements qui ne sont pas soumis à la directive (UE) 2016/680[3], l'art. 4, al. 2, s'applique au plus tard après trois ans à compter de l'entrée en vigueur de la présente ordonnance ou au plus tard à la fin du cycle de vie du système. Dans l'intervalle, ces traitements sont régis par l'art. 4, al. 1.

[2] L'art. 8, al. 5, ne s'applique pas aux évaluations effectuées avant l'entrée en vigueurde la présente ordonnance.

[3] L'art. 31 ne s'applique pas aux activités de traitement automatisé prévues pour lesquelles l'approbation du projet ou la décision de le développer a déjà été prise au moment de l'entrée en vigueur de la présente ordonnance.

Art. 47 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er septembre 2023.

… Au nom du Conseil fédéral suisse :

the requirements of Art. 22 (5) (a) and (b) DPA.

Art. 44 Fee

[1] The fee charged by the FDPIC is based on the time spent.

[2] The hourly rate varies between 150 and 250 Swiss francs, depending on the function performed by the relevant person.

[3] In the case of services that are of an extraordinary nature, particularly difficult or urgent, supplements of up to 50 % of the amount specified in (2) may be charged.

[4] If the service provided by the FDPIC can be used for commercial purposes by the person liable to pay the fee, a surcharge of up to 100 % of the fee provided for in paragraph 2 may be levied.

[5] The General ordinance on fees dated September 8, 2004[3] applies in all other respects.

Chapter 7 Final provisions

Art. 45 Repeal and amendment of other acts

The repeal and amendment of other acts are regulated in Appendix 2.

Art. 46 Transitional provisions

[1] For processing operations that are not subject to Directive (EU) 2016/680[4], Art. 4 (2) applies at the latest after three years from the entry into force of this ordinance or at the end of the life cycle of the system. In the meanwhile, such processing is governed by Art. 4 (1).

[2] Art. 8 (5) does not apply to assessments carried out before the entry into force of this ordinance.

[3] Art. 31 does not apply to planned automated processing activities for which the approval of the project or the decision to develop it has already been taken when this ordinance enters into force.

Art. 47 Entry into force

This ordinance shall become effective on September 1, 2023.

… On behalf of the Swiss Federal Council:

[2] RS **172.041.1**

[3] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4.5.2016, p. 89.

[4] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals regarding the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89.

Le président de la Confédération, Ignazio Cassis
Le chancelier de la Confédération, Walter Thurnherr

The President of the Confederation, Ignazio Cassis
The Chancellor of the Confederation, Walter Thurnherr

États, territoires, secteurs déterminés dans un État et organismes internationaux dans lesquels un niveau de protection adéquat desdonnées est garanti

1. Allemagne*
2. Andorre***
3. Argentine***
4. 4 Autriche*
5. Belgique*
6. Bulgarie***
7. Canada***

Un niveau de protection adéquat est réputé garanti lorsque la loi fédérale canadienne du 13 avril 2000 sur la protection des renseignements personnels et les documents électroniques[4] ou lorsqu'une loi essentiellement similaire adoptée par une province canadienne s'applique dans le domaine privé. La loi fédérale s'applique aux renseignements personnels recueillis, utilisés ou communiqués dans le cadre d'activités commerciales, que celles-ci relèvent d'organisations telles que des associations, des sociétés de personnes, des personnes individuelles ou des organisations syndicales ou d'entreprises fédérales telles que des installations, des ouvrages, des entreprises ou des secteurs d'activité qui relèvent de la compétence législative du Parlement canadien. Les provinces du Québec, de la Colombie-Britannique et de l'Alberta ont adopté des lois essentiellement similaires à la loi fédérale; l'Ontario, le Nouveau-Brunswick, Terre-Neuve-et-Labrador et la Nouvelle-Écosse ont adopté des lois essentiellement similaires à la loi fédérale dans le domaine des

States, territories, specified sectors within a State and international organizations where an adequate level of data protection is guaranteed

1. Germany*
2. Andorra***
3. Argentina***
4. Austria*
5. Belgium*
6. Bulgaria***
7. Canada***

An adequate level of protection is deemed to be guaranteed where the Canadian Federal Personal Information Protection and Electronic Documents Act dated April 13, 2000, or substantially similar legislation enacted by a Canadian province applies in the private sector. The federal act applies to personal data collected, used, or disclosed during commercial activities, whether those activities are carried out by organizations such as associations, partnerships, individuals, or trade unions, or by federal works, undertakings or businesses that fall within the legislative authority of the Canadian Parliament. The provinces of Quebec, British Columbia and Alberta have enacted legislation that is substantially like the federal act; Ontario, New Brunswick, Newfoundland and Labrador and Nova Scotia have enacted legislation that is substantially similar to the federal act in health information. In all provinces in Canada, the federal law applies to all personal information collected, used, or disclosed by federal works, undertakings, or businesses, including personal data about employees of federal works,

[4]La loi fédérale canadienne est disponible à l'adresse suivante : https://laws-lois.jus-tice.gc.ca/fra/lois/P-8.6.textecomplet.html.

[5]The Canadian federal legislation is available at: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html.

renseignements sur la santé. Dans toutes les provinces du Canada, la loi fédérale s'applique à tous les renseignements personnels recueillis, utilisés ou communiqués par les entreprises fédérales, y compris les renseignements personnels au sujet des employés de celles-ci. La loi fédérale s'applique également aux renseignements personnels qui circulent d'une province ou d'un pays à l'autre dans le cadre d'activités commerciales.

undertakings, or businesses.
The federal act also applies to personal data that moves interprovincially or internationally during commercial activity.

8. Chypre***
9. Croatie***
10. Danemark*
11. Espagne*
12. Estonie*
13. Finlande*
14. France*
15. Gibraltar***
16. Grèce*
17. Guernesey***
18. Hongrie*
19. Île de Man***
20. Îles Féroé***
21. Irlande***
22. Islande*
23. Israël***
24. Italie*
25. Jersey***
26. Lettonie*
27. Liechtenstein*
28. Lituanie*
29. Luxembourg*
30. Malte*
31. Monaco***
32. Norvège*
33. Nouvelle-Zélande***
34. Pays-Bas*
35. Pologne*
36. Portugal*
37. Tchéquie*
38. Roumanie***
39. Royaume-Uni**
40. Slovaquie*
41. Slovénie*
42. Suède*

8. Cyprus***
9. Croatia***
10. Denmark*
11. Spain*
12. Estonia*
13. Finland*
14. France*
15. Gibraltar***
16. Greece*
17. Guernesey***
18. Hungary*
19. Isle of Man***
20. Faroe Islands***
21. Ireland***
22. Iceland*
23. Israel*
24. Italy*
25. Jersey***
26. Latvia*
27. Liechtenstein*
28. Lithuania*
29. Luxembourg*
30. Malta*
31. Monaco***
32. Norway*
33. New-Zealand***
34. The Netherlands*
35. Poland*
36. Portugal*
37. Czech Republic*
38. Romania***
39. United Kingdom**
40. Slovakia*
41. Slovenia*
42. Sweden*

43. Uruguay***

* L'évaluation du niveau de protection adéquat inclut les transferts de données selon la Directive (UE) 2016/680[5].

** L'évaluation du niveau de protection adéquat inclut les transferts de données en vertu d'une décision d'exécution de la Commission européenne constatant le caractère adéquat du niveau de protection des données selon la Directive (UE) 2016/680.

*** L'évaluation du niveau de protection adéquat n'inclut pas les transferts de données dans le cadre de la coopération prévue par la Directive (UE) 2016/680.

43. Uruguay***

* The assessment of the level of adequate protection includes data transfers under Directive (EU) 2016/680[6].

** The adequacy assessment includes data transfers pursuant to an implementing decision of the European Commission finding the level of data protection adequate under Directive (EU) 2016/680.

***The assessment of the adequate level of protection does not include data transfers under the cooperation provided for in Directive (EU) 2016/680.

[5] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAIdu Conseil, JO L 119 du 4.5.2016, p. 89.

[6]Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals regarding the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89.