Règlement sur la protection des données

Association Swissdec

Swissdec, 6004 Lucerne
www.swissdec.ch

Règlement sur la protection des données, version 1.0

Table des matières

§ 1 Généralités

[1] Le Comité édicte le présent règlement sur la protection des données sur la base des **paragraphes 26 et 27 alinéa 1 chiffre 14 des statuts de l'Association Swissdec** dans le but de réglementer le traitement de données personnelles conformément aux prescriptions relatives à la protection des données ainsi que les responsabilités actuelles en la matière au sein de l'Association Swissdec.

[2] La désignation des responsables d'organes et titulaires de fonctions de Swissdec vaut aussi bien pour des personnes de sexe masculin que féminin; afin de simplifier la lecture, seule la forme masculine est utilisée ci-après.

§ 2 Champ d'application

[1] Le présent règlement sur la protection des données revêt un caractère impératif pour tous les membres de l'Association Swissdec.

[2] L'ensemble des organes, unités organisationnelles et fonctions mentionnés dans le règlement d'organisation ainsi que les responsables d'organes et titulaires de fonctions sont tenus de respecter le règlement sur la protection des données de Swissdec (cf. paragraphe 1 alinéa 3 du règlement d'organisation).

[3] Les membres de l'Association Swissdec sont tenus d'informer leurs collaborateurs et les tiers auxquels ils sont susceptibles de faire appel dans le cadre de leur collaboration au sein des sections et commissions (cf. paragraphe 4 des statuts) de la teneur du règlement sur la protection des données et de contraindre ces personnes à le respecter.

[4] Les tiers (p. ex. parties contractantes, auxiliaires, sous-traitants) amenés à accéder à des données personnelles ou à intervenir dans la conception de processus de traitement de données ou de normes doivent être contractuellement tenus de se conformer au règlement sur la protection des données.

§ 3 Bases impératives (notamment légales)

[1] Dans le cadre du traitement de données personnelles, de la conception de normes et du maintien de la certification de son système de gestion de la protection des données (SGPD), l'**Association Swissdec** doit observer diverses bases contraignantes, notamment:

a) Le paragraphe 1 alinéa 7 des statuts de l'Association;
b) La loi fédérale sur la protection des données du 19 juin 1992 (LPD; RS 235.1);
c) L'ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993 (OLPD; RS 235.11);
d) L'ordonnance sur les certifications en matière de protection des données du 28 septembre 2007 (OCPD; RS 235.13);
e) La version en vigueur du règlement sur les exigences en matière de certification d'un système de gestion de la protection des données selon le label GoodPriv@cy;
f) Les contrats conclus avec les destinataires de données au sujet de la transmission de données via le répartiteur (conditions générales du répartiteur).

[2] Dans le cadre du traitement de données personnelles, les **membres de l'Association** et l'**Office fédéral de la statistique** doivent aussi observer les lois spécifiques qui les concernent et les éventuelles lois cantonales sur la protection des données. Ces textes engagent directement les membres de l'Association et l'Office fédéral de la statistique et ils ont une incidence sur la conformité légale du traitement de données personnelles par l'Association Swissdec mais aussi des normes Swissdec.

§ 4 Définitions

Les termes importants utilisés dans le présent règlement sur la protection des données sont définis ci-après dans un souci de clarté. En cas de divergence, les définitions transmission par la loi fédérale sur la protection des données font foi.

a) Données personnelles: données concernant une personne physique ou morale identifiée ou identifiable. On considère qu'une personne est identifiable si la fourniture d'informations supplémentaires permet de déterminer son identité.
b) Données sensibles: données sur des opinions ou activités religieuses, philosophiques, politiques ou syndicales; données sur la santé, la sphère intime ou l'appartenance à une race ou ethnie; données génétiques ou biométriques permettant d'identifier une personne physique sans équivoque; données sur des poursuites ou sanctions pénales et administratives; données sur des mesures d'aide sociale.

c) Traitement: toute opération relative à des données personnelles, notamment la collecte, la communication ou la destruction des données. Le simple enregistrement (sans modification) de données personnelles est aussi considéré comme un traitement.
d) Responsable: personne privée ou organe fédéral décidant seul(e) ou avec d'autres de la finalité et des moyens du traitement.
e) Sous-traitant: personne privée ou organe fédéral traitant des données personnelles pour le compte du responsable.

§ 5 Système de gestion de la protection des données

L'Association Swissdec exploite un système de gestion de la protection des données certifié OCPD (ordonnance sur les certifications en matière de protection des données, RS 235.13) et GoodPriv@cy (label de protection des données élaboré par l'Association Suisse pour Systèmes de Qualité et de Management SQS).

§ 6 Responsabilité

[1] Organe faitier de l'Association Swissdec, l'assemblée générale répond de la conformité légale des actions menées par l'Association dans le cadre des tâches qui lui sont confiées en vertu des statuts. Lors du processus décisionnel relatif au budget annuel de l'Association, elle met à disposition les ressources financières nécessaires à la garantie systématique de la protection et de la sécurité des données.

[2] Dans le cadre de ses obligations statutaires, le Comité possède notamment les compétences et responsabilités suivantes en matière de garantie de la conformité des actions menées par l'Association aux dispositions de la protection des données:

a) Établissement et modification du règlement sur la protection des données;
b) Établissement et modification de la politique de protection des données;
c) Évaluation des risques en matière de protection et de sécurité des données et définition de mesures de gestion des risques idoines;
d) Réception des rapports du préposé à la protection des données;
e) Évaluation du système de gestion de la protection des données lors d'une révision annuelle;
f) Communication avec des tiers, par exemple avec le préposé fédéral à la protection des données et à la transparence (PFPDT) et d'autres autorités de surveillance, en cas de violation présumée ou avérée de la protection ou de la sécurité des données, sauf si cette compétence est déléguée au centre opérationnel ou au préposé à la protection des données;
g) Demande à l'assemblée générale des moyens financiers nécessaires pour garantir la protection et la sécurité des données.

[3] Le préposé à la protection des données exerce pour l'Association Swissdec la fonction de conseiller à la protection des données telle que définie dans la LPD et l'OLPD. Son identité est communiquée au préposé fédéral à la protection des données et à la transparence (PFPDT). Il conseille l'Association Swissdec dans le cadre de la mise en œuvre des dispositions relatives à la protection des données. Son affectation organisationnelle et ses obligations sont précisées aux paragraphes 17 à 19 du règlement d'organisation ainsi que dans son cahier des charges. Au besoin, le préposé à la protection des données fournit des modèles, des listes de contrôle ou d'autres documents visant à faciliter la mise en œuvre des prescriptions légales relatives à la protection des données ainsi que le présent règlement sur la protection des données.

[4] Le centre opérationnel et l'unité organisationnelle Standardisation travaillent en étroite collaboration avec le préposé à la protection des données et endossent notamment les responsabilités suivantes:

a) Planification des tâches récurrentes (formations, audits internes et externes) conjointement avec le préposé à la protection des données;
b) Exploitation du système de gestion de la protection des données;
c) Identification et traitement d'incidents en matière de protection et de sécurité des données, en accord avec le préposé à la protection des données et le Comité;
d) Transmission au préposé à la protection des données de questions en lien avec la protection des données;
e) Sollicitation du préposé à la protection des données lors de la planification de nouveaux projets.

[5] Toutes les personnes physiques et morales entrant dans le champ d'application du présent règlement sur la protection des données (cf. paragraphe 2) sont tenues de collaborer avec le préposé à la protection des données, de le contacter spontanément en cas de problème ou de question en lien avec l'application de la législation en matière de protection des données, de lui donner accès à des traitements de données et systèmes s'il le demande et de répondre à ses questions concernant des traitements de données. Qui plus est, toutes ces personnes doivent participer à des formations sur la protection des données.

§ 7 Rôles définis par la législation sur la protection des données

[1] L'Association Swissdec endosse le rôle de responsable – au sens de la législation en matière de protection des données – du traitement des données personnelles en lien avec la gestion des affaires de l'Association Swissdec. Sont notamment concernées les informations sur les personnes représentées au sein de l'Association Swissdec ou participant à l'exécution des tâches de l'Association Swissdec en tant qu'externes. Dans le cadre du traitement de ces données personnelles, l'Association Swissdec répond directement de la satisfaction des obligations en matière de protection des données visées par la LPD ainsi que des dispositions du présent règlement sur la protection des données.

[2] En ce qui concerne la transmission de données personnelles via le répartiteur aux destinataires de données salariales concernés et pour le compte de ces derniers, à leurs clients, l'Association Swissdec intervient en tant que sous-traitant pour les destinataires de données salariales. Ce faisant, l'Association Swissdec ne traite ces données personnelles que pour le compte et dans l'intérêt des destinataires de données salariales et prend des mesures appropriées pour garantir la sécurité des données. Qui plus est, l'Association Swissdec n'a recours à des sous-traitants qu'avec l'accord des destinataires de données salariales.

§ 8 Principes relatifs au traitement de données personnelles

[1] L'Association Swissdec observe les bases légales applicables dans le cadre du traitement de données personnelles ainsi que de l'élaboration et du développement de normes Swissdec.

[2] L'Association Swissdec procède au traitement de données personnelles dans le strict respect de la législation:

a) En tant que responsable, elle traite des données personnelles en vertu des statuts ou de contrats;

b) En tant que sous-traitant, elle traite des données personnelles en vertu d'un contrat et aux fins du destinataire de données salariales;

c) Elle prend des mesures appropriées pour que les destinataires de données salariales ne reçoivent via le répartiteur que les données personnelles pour lesquelles ils disposent d'une légitimation légale ou contractuelle.

[2] Les données personnelles ne sont transmises par l'Association Swissdec via le répartiteur qu'aux destinataires prévus. Aucun autre traitement des données n'a lieu.

[3] L'Association Swissdec organise ses systèmes informatiques et ses traitements de données de façon à ne traiter que le volume de données effectivement nécessaire pour atteindre le but recherché (principe de «Privacy by Design»).

[4] Les données personnelles sont traitées de manière confidentielle. L'accès à des données personnelles n'est octroyé qu'aux personnes qui en ont besoin pour mener à bien leurs tâches.

[5] L'Association Swissdec prend des mesures techniques et organisationnelles adéquates pour garantir la sécurité du traitement des données.

[6] Si des sous-traitants sont sollicités pour traiter des données personnelles, l'Association Swissdec veille par voie contractuelle à ce qu'ils traitent ces données exclusivement dans l'intérêt de l'Association Swissdec, et uniquement dans la mesure où l'Association Swissdec est elle-même autorisée à le faire. Qui plus est, l'Association Swissdec s'assure, dans un tel cas, que les prestataires de services protègent au moyen de mesures techniques et organisationnelles appropriées les données personnelles qui leur sont confiées.

[7] L'Association Swissdec exploite le répartiteur sur des infrastructures techniques situées en Suisse.

[8] L'Association Swissdec informe de manière appropriée – généralement au moyen de publications sur son site Internet – l'opinion publique et les personnes concernées de ses traitements de données.

§ 9 La protection des données dans le cadre de projets

[1] Lorsque sont planifiés des projets portant sur le traitement de données personnelles ou leur gestion (p. ex. en cas d'élaboration de nouvelles normes), l'Association Swissdec s'assure que les exigences en matière de protection et de sécurité des données sont clarifiées et prises en compte au plus tôt.

[2] Le préposé à la protection des données est prié de donner son avis dès l'établissement de la demande de projet.

[3] Si le préposé à la protection des données évoque, au sujet du traitement de données prévu, un risque élevé pour les personnes concernées, l'équipe de projet doit réaliser une analyse d'impact relative à la protection des données conjointement avec le préposé à la protection des données (cf. paragraphe 10).

§ 10 Répertorier et analyser l'impact relatif à la protection des données

[1] L'Association Swissdec consigne dans des répertoires les activités de traitement de données personnelles qu'elle entreprend.

[2] Le préposé à la protection des données aide l'Association Swissdec, respectivement les personnes responsables d'un traitement de données, à examiner la nécessité d'analyses d'impact relatives à la protection des données et, le cas échéant, à mener de telles analyses. Le préposé à la protection des données fournit des modèles et des listes de contrôle à cet effet. Si la loi le prescrit, le préposé à la protection des données avise l'autorité de surveillance en charge de la protection des données en accord avec le Comité, l'unité organisationnelle Standardisation et le centre opérationnel.

[3] Si nécessaire, l'Association Swissdec aide les responsables à compiler des répertoires et à réaliser les analyses d'impact relatives à la protection des données lorsqu'elle traite des données personnelles pour eux en tant que sous-traitant.

§ 11 Audits et contrôles

[1] Chaque année, un organisme de certification externe examine le système de gestion de la protection des données de l'Association Swissdec pour s'assurer de sa conformité à l'OCPD et au label GoodPriv@cy.

[2] L'Association Swissdec mène en outre tous les ans des audits internes qui sont planifiés plusieurs années à l'avance et menés en tenant compte des risques vis-à-vis de la législation en matière de protection des données pour l'Association Swissdec et les personnes concernées ainsi que des exigences des normes certifiées.

[3] Le préposé à la protection des données mène à bien sa mission de contrôle comme suit:

a) Dans une optique préventive, par son implication obligatoire dans le cadre de projets (cf. paragraphe 9);
b) Via sa participation à des séances de la commission spécialisée et de la commission technique;
c) À la demande d'un membre de l'Association, d'un organe ou d'un tiers en cas de soupçon de violation de la protection ou de la sécurité des données;
d) Par le contrôle ponctuel de processus de traitement de données existants.

§ 12 Écarts par rapport aux prescriptions légales ou d'une autre nature (non-conformité)

[1] Les constatations auxquelles aboutissent les audits et contrôles (cf. paragraphe 11) sont consignées et évaluées afin d'identifier d'éventuelles mesures nécessaires pour l'Association Swissdec et d'évaluer les risques pour les personnes concernées.

[2] Toute violation avérée ou présumée de prescriptions de protection des données personnelles ou de garantie de la sécurité des données qui ne serait pas décelée par un audit ou un contrôle doit être signalée au centre opérationnel, lequel tranchera et décidera de la marche à suivre en concertation avec le préposé à la protection des données.

[3] Si la violation présumée porte sur des données personnelles d'un destinataire de données salariales que l'Association Swissdec traite en qualité de sous-traitant, l'Association Swissdec la signale dans les plus brefs délais au destinataire de données salariales compétent.

[4] Le préposé à la protection des données:

a) recommande des mesures de correction s'il constate des violations des dispositions en matière de protection des données;
b) détermine si les violations de la sécurité des données sont soumises à une obligation de communiquer et, le cas échéant, procède à l'annonce prescrite par la loi en accord avec le Comité;
c) fournit des modèles et des listes de contrôle en vue de l'évaluation.

[5] La responsabilité du contrôle de la liquidation de cas de non-conformité constatés et/ou signalés incombe au préposé à la protection des données, au centre opérationnel et à l'unité organisationnelle Standardisation.

[6] Toutes les personnes entrant dans le champ d'application du présent règlement sur la protection des données sont tenues de collaborer à l'examen et à la liquidation de ces cas.

§ 13 Droits des personnes concernées

[1] Les personnes concernées sont les personnes physiques au sujet desquelles des données sont traitées. Elles disposent notamment des droits suivants:

- Droit de savoir si des données les concernant sont traitées et, si oui, de quelles données il s'agit;
- Droit de faire corriger ou effacer des données personnelles les concernant, ou encore d'en restreindre le traitement.

[2] Toute demande soumise à l'Association Swissdec par une personne concernée en vertu de l'un de ces droits doit être transmise au directeur du centre opérationnel, lequel décide si la demande porte sur un traitement de données de l'Association Swissdec ou d'un destinataire de données salariales. Si elle porte sur un traitement de données d'un destinataire de données salariales, la demande est transmise à ce dernier. Si elle concerne l'Association Swissdec, le directeur du centre opérationnel transmet la demande au préposé à la protection des données en vue de son traitement ultérieur.

[3] Toutes les personnes entrant dans le champ d'application du présent règlement sur la protection des données sont tenues d'aider le préposé à la protection des données à répondre aux demandes de personnes concernées et à lui fournir l'ensemble des informations dont il a besoin.

§ 14 Formations

[1] Le préposé à la protection des données forme toutes les personnes amenées à intervenir dans la conception de processus de traitement de données et dans l'établissement de normes au sein de l'Association Swissdec.

[2] Les formations visent à fournir aux personnes qui y participent les connaissances de base en matière de protection et de sécurité des données dont elles ont besoin pour mener leurs activités pour l'Association en conformité avec les dispositions relatives à la protection des données. Au besoin, des formations sont organisées pour des groupes d'intérêt spécifiques.

§ 15 Dispositions finales

Le présent règlement a été édicté par le Comité le 11 décembre 2019 et entre en vigueur à la même date.

Lucerne, le 11.12.2019

Felix Weber
Président de l'Association Swissdec

Claudio Fischer
Vice-président de l'Association Swissdec

Règlement approuvé lors de la séance du comité du 11.12.2019