

CLUSIS - 5 À 7 EN LIGNE - RÉVISION LPD : QUELS ENJEUX POUR LES ENTREPRISES ?

Nicolas Vernaz 02.02.2021





ASDPO



ASSOCIATION SUISSE DES DÉLÉGUÉS À LA PROTECTION DES DONNÉES

SWISS ASSOCIATION OF DATA PROTECTION OFFICERS

www.asdpo.swiss



BUT DE LA LPD

But de la LPD

La loi vise à protéger la personnalité et les droits fondamentaux des **personnes physiques dont les données personnelles font l'objet d'un traitement**.



REDSTONE Infographie basée sur le texte « Loi fédérale sur la protection des données (LPD) » du 25

septembre 2020

But de la LPD

La loi vise à protéger la personnalité et les droits fondamentaux des personnes physiques dont les données personnelles font l'objet d'un traitement

Définitions

Données personnelles: toutes les informations concernant une personne physique identifiée ou identifiable;

Données personnelles sensibles (données sensibles):

- 1. les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales,
- 2. les données sur la santé, la sphère intime ou l'origine raciale ou ethnique,
- les données génétiques.
- 4. les données biométriques identifiant une personne physique de manière univoque.
- les données sur des poursuites ou sanctions pénales et administratives.
- 6. les données sur des mesures d'aide sociale;

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;

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:

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;

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:

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;

Sous-traitant: la personne privée ou l'organe fédéral qui traite des données personnelles pour le compte du responsable du traitement.



Champ d'application à raison de la personne et de la matière

Les traitements de données personnelles concernant des personnes physiques effectué par:

- des personnes privées:
- des organes fédéraux

Champ d'application territorial

S'applique aux états de fait qui déploient des effets en Suisse, même s'ils se sont produits

à l'étranger. (extraterritorialité)

Risques vis-à-vis du PFPDT

- Enguête / Audit
- Modification, suspension ou cessation de tout ou partie du traitement ainsi que
- l'effacement ou la destruction de tout ou partie des données personnelles
- Suspension ou interdiction de la communication de données personnelles à l'étranger

Risques vis-à-vis des tribunaux cantonaux (pénal)

250 000 francs au plus les personnes privées

Autorité compétente : **PFPDT** https://www.edoeb.admin.ch/edoe b/fr/home.html

REPRÉSENTANT

Les communication de données personnelles à l'étranger nécessitent soit

- Adéquation du pays
- Un traité international
- Des clauses type de protection des données préalablement approuvées, établies ou reconnues par le PFPDT
- D'autres mécanismes demandant l'approbation préalable du PFPDT

TRANSFERT DE

DONNÉES

En cas de sous-traitance Avoir un contrat Respect du sous-traitant de

Forme et conseille le responsable

du traitement privé dans le

domaine de la protection des

Indépendant

Attention aux soustraitance en cascade

la LPD

,,,,,,,,,,, Devoir d'informer en cas de décision

Concours à l'application des

prescriptions relatives à la

protection des données

Connaissances professionnelles

nécessaires

En cas de transfert

CONSEILLER À LA

PROTECTION DES

DONNÉES

Analyse d'impact relative à la protection des données

personnelles

Protection des données

dès la

conception

et par défaut

Sécurité des données / Mesures

techniques et

organisationnelles

Registre des activités

de traitement

(Exceptions si moins)

de 250

collaborateurs +

risque limité)

Devoir

d'informer

lors de la

collecte de

données

personnelles

individuelle automatisée

.........

Annonce des violations de la sécurité des données

Respect des Principes et des Droits

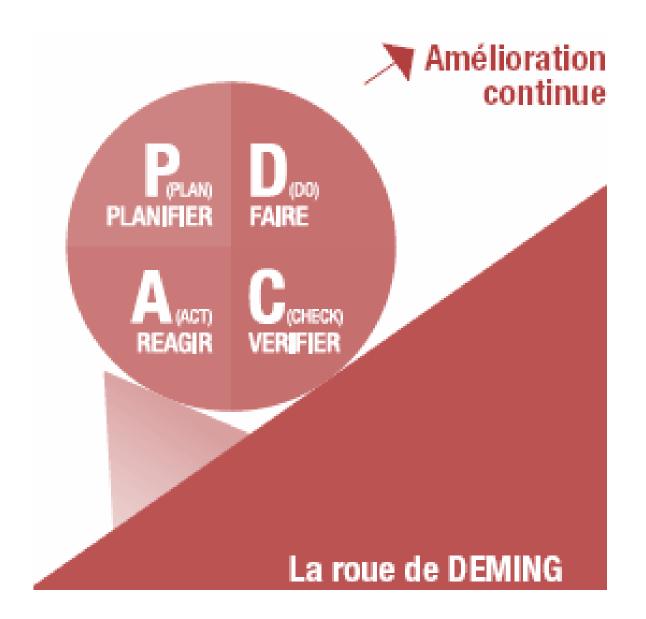
.........

des individus Peut nommer

DEVOIRS DES ENTREPRISES consulting

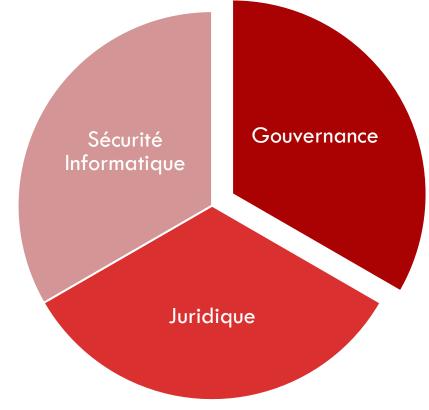
Confidentie Copyrights @ Redstone Consulting SA [4]

www.redstoneconsulting.ch





Incidents TOMs Par défaut et Dès la conception



Politique de confidentialité
Cookies
Disclaimers
Contrats

DPO

Sensibilisation

Registre

DSAR

DPIA

Rétention / Suppression

SAVOIR CE QU'IL SE PASSE!





Protection des données dès la conception et par défaut

Sécurité des données / Mesures techniques et organisationnelles

Registre des activités de traitement (Exceptions si moins de 250 collaborateurs + risque limité)

Guide RGPD du développeur | CNIL

Le guide RGPD du développeur offre une première approche des grands principes du RGPD et des différents points d'attention à prendre en compte dans le déploiement d'applications respectueuses de la vie privée des utilisateurs.

Protection des données dès la conception

Le recours à la pseudonymisation (remplacement des informations permettant d'identifier une personne par des identifiants factices) et au chiffrement (cryptage de messages afin que seules les personnes autorisées puissent les lire).

Protection des données par défaut

Une plateforme de réseau social devrait être encouragée à modifier les paramètres du profil des utilisateurs pour le rendre le plus confidentiel possible, par exemple en limitant dès le départ l'accessibilité du profil des utilisateurs afin qu'il ne soit pas accessible par défaut à un nombre indéterminé de personnes.

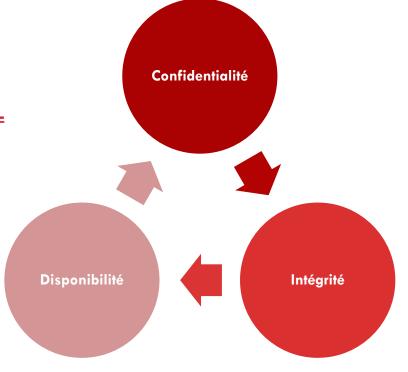


Protection des données dès la conception et par défaut

Sécurité des données / Mesures techniques et organisationnelles

Registre des activités de traitement (Exceptions si moins de 250 collaborateurs + risque limité) Guide de la sécurité des données personnelles | CNIL

FICHE 8	SÉCURISER LES SERVEURS Renforce les mesures de sécurité appliquées aux serveurs. > En sanoir plus
FICHE 9	SÉCURISER LES SITES WEB S'assurer que les bonnes pratiques minimales sont appliquées aux sites web. > De senoir plus
FICHE 10	SAUVEGARDER ET PRÉVOIR LA CONTINUITÉ D'ACTIVITÉ Elfichier des sauvegarden régulières pour limiter l'impact d'une dispartition non destirée de domaine. > D'i sanvoir plus
FICHE 11	ARCHIVER DE MANIÈRE SÉCURISÉE ARCHIVER les MANIÈRE SÉCURISÉE ARCHIVER les données qui ne sont plus utilisées au quotidien mais qui n'ont pas encora stitunt lux durée limite de soncervation, par caemple parce qu'elles sont conservées afin d'être utilisées en cas de contentieux. > Dr. sancor plus
FICHE 12	ENCADEER LA MAINTENANCE ET LA DESTRUCTION DES DONNÉES Garantir la sécurité des données à tout moment du cycle de vie des matériels et des logicals. > Dit sanoir plus
FICHE 13	GÉRER LA SOUS-TRAITANCE Dacodrer la sécurité des données avec les sous-traitants. > En senoir plus
FICHE 14	SÉCURISER LES ÉCHANGES AVEC D'AUTRES ORGANISMES Renfiserer la sécurité de toute transmission de données à caractère personnel. > Des senoir plus
FICHE 15	PROTÉCER LES LOCAUX Ranfacer la sécurité des locaux hébergeant les serveurs informatiques et les matérials réseaux. > Des annoirs glus





Protection des données dès la conception et par défaut

Sécurité des données / Mesures techniques et organisationnelles

Registre des activités de traitement (Exceptions si moins de 250 collaborateurs + risque limité) [Bases légales] [Responsable] [Supports]

Origine des données personnelles

Traitements effectués

Destinataires

[Type de données]

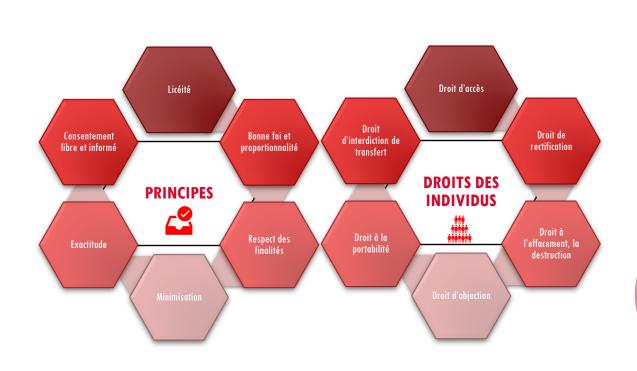
[Données sensibles ?]

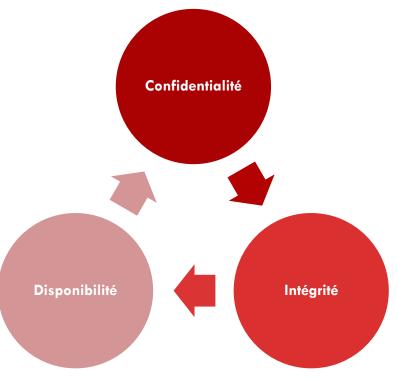
[Transferts hors UE/Suisse ?]



Analyse d'impact relative à la protection des données personnelles

Annonce des violations de la sécurité des données









Que faire en cas d'incident?

Étape 1 - Découverte de l'incident ☐ Rapporter Fincident en Interne et réunir l'équipe 'Gestion des Incidents' (ou équivalent) □ Axalyser l'incident et documenter les premiers éléments découverts. □ Date et heure de l'incident. □ TOM's* en place ☐ Circonstances de l'incident □ Sous-traitant impliqué ? □ Nature et teneur des données concernées ☐ Contenir immédiatement l'incident (possiblement contacter l'équipe informatique) Consultor le responsable de la protection des données si des données perspenelles sont concernées ☐ Notifier les autorités de supervision de l'UE (e.g. CNL) l'ersque cela est légalement demandé atification initials : Terms : 1 + ress. 249 Étape 2 - Enquête ☐ Enquêter sur l'incident de manière approfondie afin de : ☐ Établir les causes exactes de l'incident. ☐ Analyser les implications / risques légaux de l'incident (LPO/RGPO/Autres) ☐ Considérer l'élaboration d'une stratégie de communication □ Considérer quelles autres ressources pourrait être récessaires Étape 3 - Remédiation □ Déterminer les personnes internes et externes qui doivent être notifiées de l'incident conformément à la loi (RGPD/LPD/Autres): □ Votre assurance ? □ Les employés ? □ Les clients ? □ Des seus-traitants ? ☐ Autre 7 □ Reveir les causes de l'incident et l'ancer un processus de remédiation, développes des actions pour remédier à □ Notifier les autorités de supervisions des informations sugalémentaires nécessaires Étape post-incident - Amélioration continue ☐ Nipondez aux clients, autorités, médias etc. selon la nécesaité ☐ Revoyez l'incident et capitalisez le retour d'expérience : ☐ Corrigez les lacunes sécuritaires et organisationnelles pour réduire les risques futurs ☐ Mettec à jour le registre des incidents, les PIA et le registre des traitements en conséquence

Analyse d'impact relative à la protection des données personnelles

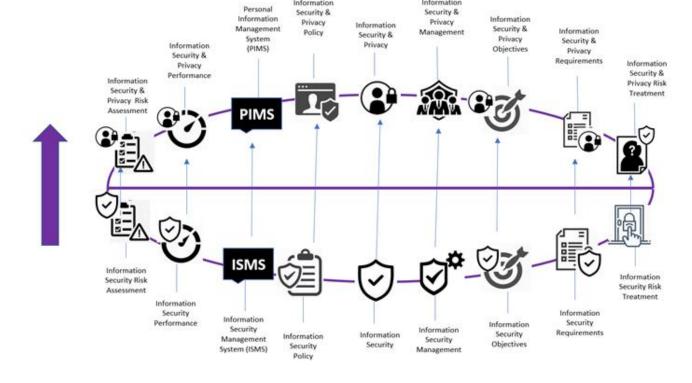
Annonce des violations de la sécurité des données



FRAMEWORKS

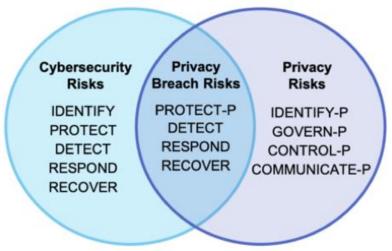
ISO 27701:2019 - Annex F - How to apply ISO 27701











FRAMEWORKS

CONTACTS



Nicolas Vernaz

Fondateur et Directeur

Redstone Consulting SA

Rue Emile-Yung 10, 1205, GENEVE Tél.: +41(0) 78 762 77 81

nv@redstoneconsulting.ch

Web: www.redstoneconsulting.ch

