Nouvelle loi sur la protection des données : que faire, comment et avec quelle priorité?

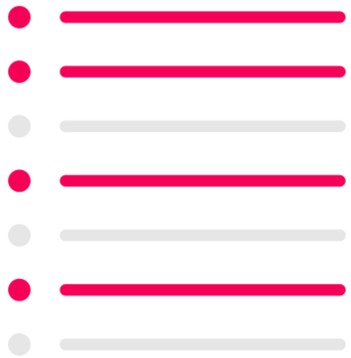
François Charlet

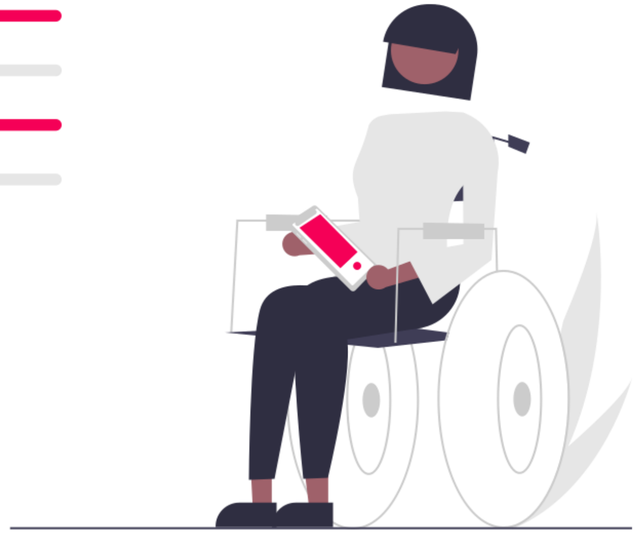
21 juin 2023

Mesures prioritaires/urgentes

Qu’est-ce qui rend une mesure urgente ou prioritaire ?

A mon avis





Introspection

Registre des traitements

Déclaration de protection des données

Contrats

Contrat de travail

Contenu spécifique

Clause de confidentialité (pendant et après les rapports)

Protection des données des collaborateurs (information) et celles traitées par les collaborateurs (sécurité)

Annexes (directives, règlements, télétravail, BYOD, etc.)

Contrat de sous-traitance

Contenu minimal

- Objet et durée
- Nature et finalité
- Catégories de données/ personnes
- Obligations et droits du RT
- Instructions
- Confidentialité
- Sécurité
- Sous-traitance ultérieure
- Droits des personnes
- Notification des violations
- Droit d’audit
- Documentation
- Fin de contrat

Contrats avec un autre RT

Contenu

Contenu similaire au contrat pour un ST, sauf que les parties sont sur un **pied d'égalité**, l'une n'est pas subordonnée aux instructions de l'autre en vertu de la LPD, elles peuvent donc négocier librement dans les limites de la loi.

Réduction des risques

Analyse de risques

Analyse de risques

pour les personnes concernées

Traiter les données est une opération risquée

Protéger qui contre quoi ?

Qui = vos clients, vos collaborateurs, les clients de vos clients, vos fournisseurs et partenaires, les employés de vos partenaires, etc.

Quoi = plein de risques

Analyse de risques

Quels risques pour les personnes concernées ?

- Perte de confidentialité
- Vol d'identité ou utilisation frauduleuse des données
- Impossibilité ou difficulté pour les personnes concernées d'accéder à des produits ou services, ou de s'en servir
- Dommage financier ou économique, ainsi que tout autre désavantage similaire y compris un désavantage social
- Atteinte à la vie, à l'intégrité physique, à la liberté de mouvement
- Discrimination
- Réidentification des personnes concernées à partir de données pseudonymisées ou anonymisées
- Atteinte à l'honneur, à la réputation, au droit à l'image, à la vie affective, à la piété filiale, à la vie intime ou à la vie privée.

etc.

Analyse de risques

Déclencheurs

- Programmation périodique
- Nouveau traitement
- Nouvelles données
- Modification d’un traitement (finalités/moyens)
- Prise de décision (automatisée ou non)
- Communication de données à des tiers
- Nouvelles technologies
- Transferts
- Modification des mesures de sécurité

etc.

Analyse de risques

Contenu

Description du traitement

- Nature (ce qu'on va faire)
- Portée (ce qu'il englobe)
- Contexte (interne et externe)
- Finalités

Application des principes

Droits des personnes

Risques

- Evénements redoutés (impact sur les personnes)
- Menaces (opération considérée comme possible)
- Source du risque (quelqu'un ou quelque chose réalisant la menace)
- Vulnérabilité (élément utilisé pour réaliser la menace)

Analyse de risques

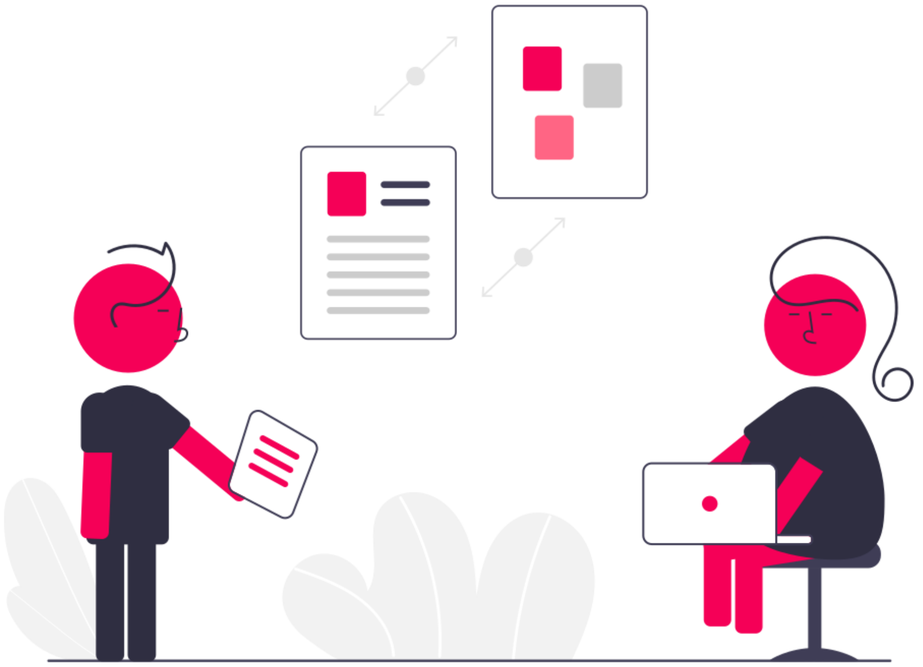
Décisions

Réduire

Accepter

Eviter

Transférer (lorsque c’est possible)



Analyse de risques

Quelques mesures

Préventives (~~vulnérabilités~~)

Correctrices (réduire les conséquences)

Compensatoires (agir ailleurs)

Dissuasives (acteur de la menace)

Détectrices (informer de la concrétisation d’une menace)

Transferts de données

Transferts

Rappels & Conseils

Inévitables

Accéder aux données en CH depuis l'étranger = transfert

Eviter les transferts hors UE pour s'éviter des ennuis/complications

Sous-traitants (ultérieurs) ⚠️

Lire attentivement les contrats et négocier (quand c'est possible)

Transferts

Mécanismes

Décisions d’adéquation (CH/UE)

Garanties appropriées (SCC, BCR, etc.)

Dérogations

Si aucun mécanisme n’est « disponible », aucun transfert n’est possible.

Transferts

Décisions d’adéquation

Cf. Annexe 1 OPDo

Pas de formalité particulière quant au transfert

Tout va bien ! 🥳
(jusqu’au moment où le pays en question disparait de l’annexe 1)

Transferts

Garanties appropriées

Traités internationaux

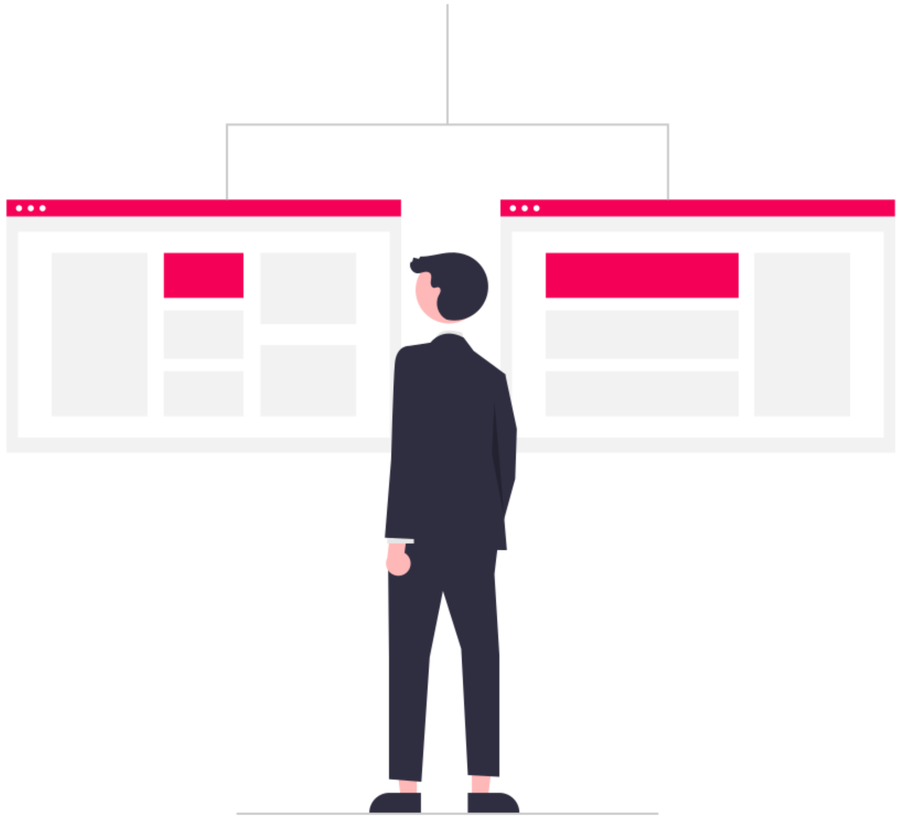
SCC (clauses contractuelles types)

BCR (règles d’entreprise contraignantes)

Clauses contractuelles

Codes de conduite

Certifications (cf. OCPD)



Transferts

Principales dérogations

Mécanismes exceptionnels

Consentement

Exécution d’un contrat avec ou en faveur de la personne concernée

Défense des droits en justice

Intérêts vitaux

Transferts

Comment documenter ?

Connaître les traitements et flux de données (⚠️ au cloud)

Déterminer les destinataires et les pays concernés, puis le(s) mécanisme(s)

Si nécessaire, évaluer le droit et les pratiques du pays de destination, prendre des mesures supplémentaires

Informer les personnes concernées (pays + mécanismes)

Archivage et effacement

Archivage

non définitif

Durées de conservation

Mesures de sécurité

Tri

Migration de données

Effacement

spontané et sur demande

Obligatoire dès que tous les buts sont atteints

Buts incluent l'archivage pour respecter des délais légaux, des délais de prescription, ou vos propres besoins (objectivement justifiés)

Mesures alternatives à adopter si l'effacement est impossible

Anonymisation

une alternative pas moins difficile

Anonymisation doit empêcher toute possibilité de réidentification

Valable à un moment donné, vérifier régulièrement qu'elle tient toujours

Plusieurs méthodes possibles

Droits des personnes

Conclusion

Conclusion

Ne paniquez pas à cause des sanctions pénales

Faites les choses les unes après les autres (p. ex. introspection, puis registre, puis mesures de sécurité, puis information aux personnes concernées, puis aspects contractuels, etc.)

Donnez des instructions à vos collaborateurs

Sensibilisez-les à la sécurité et aux bonnes pratiques

Adoptez une approche *by design* (cela coûte moins cher)

Conclusion

Analysez les risques (pour les personnes mais aussi pour vous)

Mettez à jour les contrats, en particulier avec vos sous-traitants

Préparez-vous à recevoir et gérer les demandes des personnes

N’ayez pas peur d’effacer des données si vous n’en avez plus besoin

Attention à la différence entre consentement et contrat

Prenez des décisions, documentez ce que vous faites

Merci

de votre
attention
patience
endurance