Le registre des traitements dans la nouvelle LPD

François Charlet

19 octobre 2023

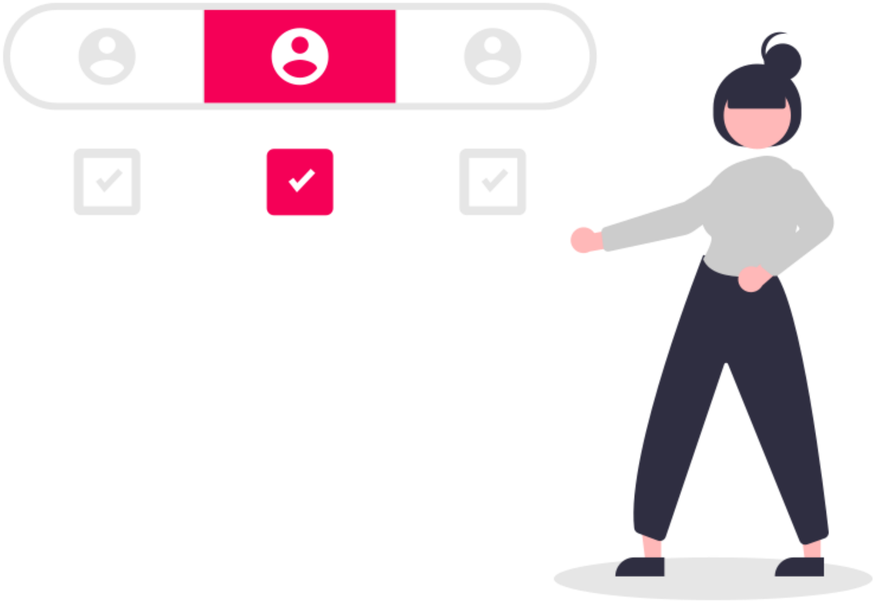
Introduction

Introduction et théorie

Champ d’application de la LPD

« régit le traitement de données personnelles concernant des personnes physiques effectué par des personnes privées et des organes fédéraux »

⚠️ droit cantonal de la protection des données



– Art. 2 Champ d'application à raison de la personne et de la matière

[1] La présente loi régit le traitement de données personnelles concernant des personnes physiques effectué par:

a. des personnes privées;
b. des organes fédéraux.

[2] Elle ne s'applique pas:

a. aux traitements de données personnelles effectués par une personne physique pour un usage exclusivement personnel;
b. aux traitements de données personnelles effectués par les Chambres fédérales et les commissions parlementaires dans le cadre de leurs délibérations;
c. aux traitements de données personnelles effectués par les bénéficiaires institutionnels au sens de l'art. 2, al. 1, de la loi du 22 juin 2007 sur l'État hôte[3] qui jouissent en Suisse de l'immunité de juridiction.

[3] Les traitements de données personnelles effectués dans le cadre de procédures devant des tribunaux ou dans le cadre de procédures régies par des dispositions fédérales de procédure, ainsi que les droits des personnes concernées, obéissent au droit de procédure applicable. La présente loi s'applique aux procédures administratives de première instance.

[4] Les registres publics relatifs aux rapports de droit privé, notamment l'accès à ces registres et les droits des personnes concernées, sont régis par les dispositions spéciales du droit fédéral applicable. À défaut la présente loi s'applique.

Introduction et théorie

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 »

➡️ Tout ? Tout.

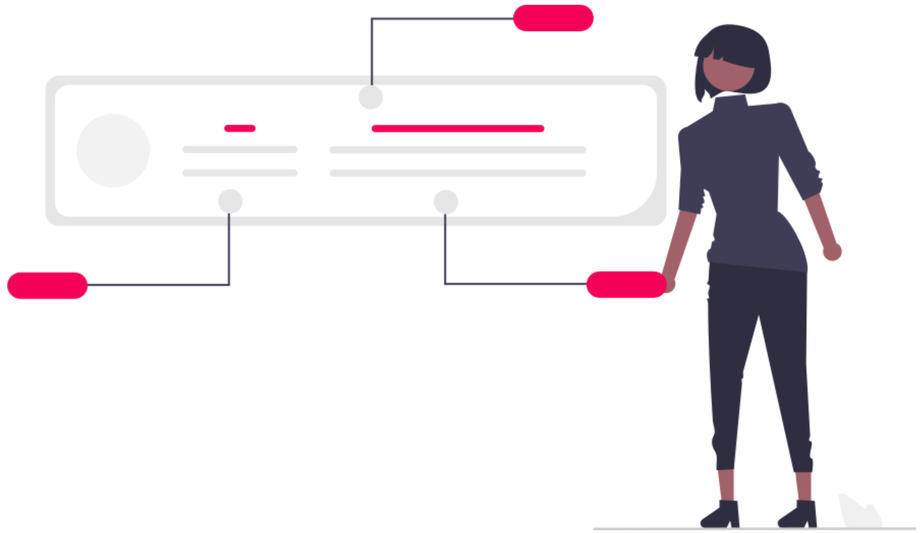
Introduction et théorie

Donnée personnelle

« toutes les informations concernant une personne physique identifiée ou identifiable »

🪪 Identifiée ?

🧩 Identifiable ? Quid du contexte ?



Introduction et théorie

Donnée sensible

« opinions ou activités religieuses, philosophiques, politiques ou syndicales / santé, sphère intime, origine raciale ou ethnique / génétiques / biométriques identifiant une personne physique de manière univoque / poursuites ou sanctions pénales et administratives / mesures d'aide sociale »

📝 Liste exhaustive

Introduction et théorie

Personne concernée

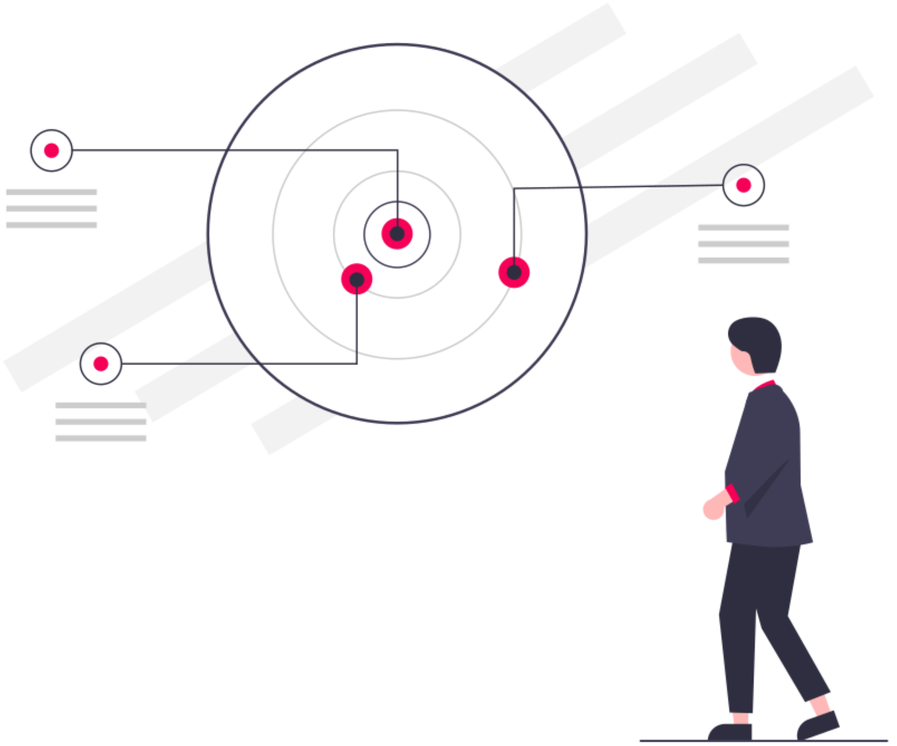
« personne physique dont les données personnelles font l’objet d’un traitement »

Introduction et théorie

Finalité

« but pour lequel des données personnelles sont traitées »

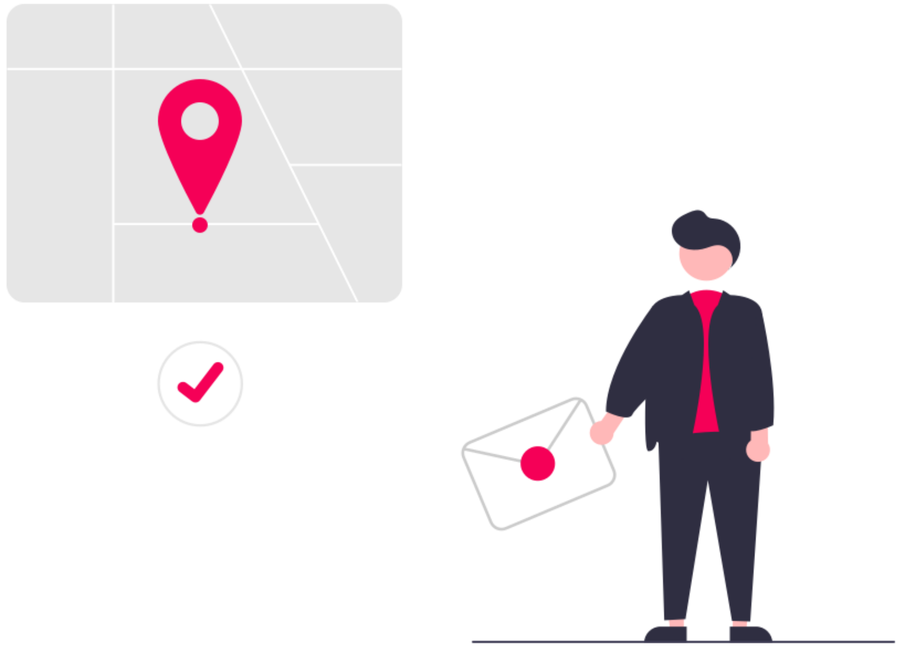
Il ne peut pas être trop général (« ~~mener à bien les activités de l'entreprise~~ ») mais ne devrait pas être trop précis afin de garder une certaine marge de manoeuvre.



Introduction et théorie

Destinataire

« personne, physique ou morale, une autorité ou toute autre entité à qui les données personnelles sont communiquées »

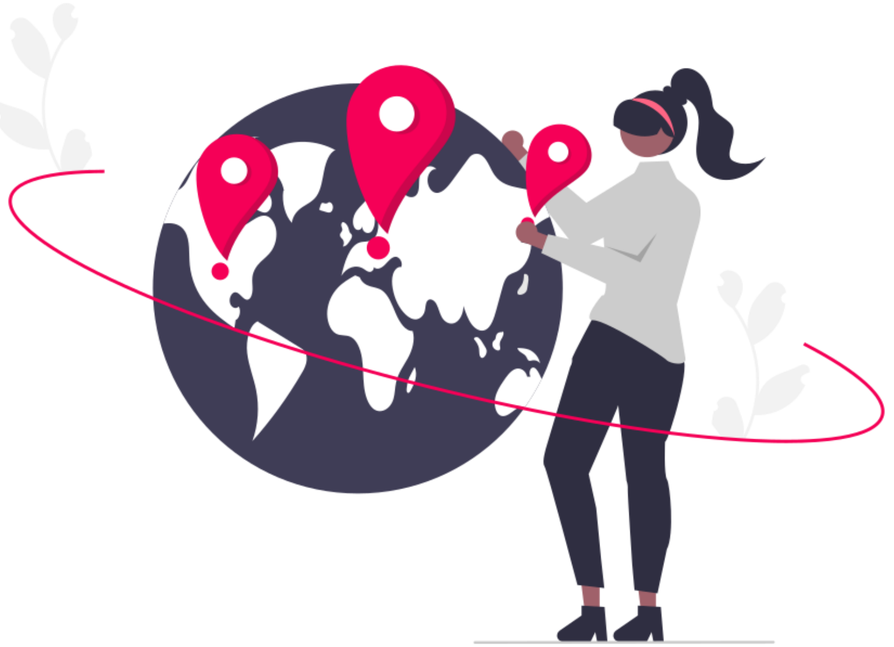


Introduction et théorie

Transfert

« fait de transférer des données personnelles de la Suisse vers un autre pays ou de les rendre accessibles à d’autres pays depuis la Suisse »

Seul l’export de données est un transfert, pas l’import.

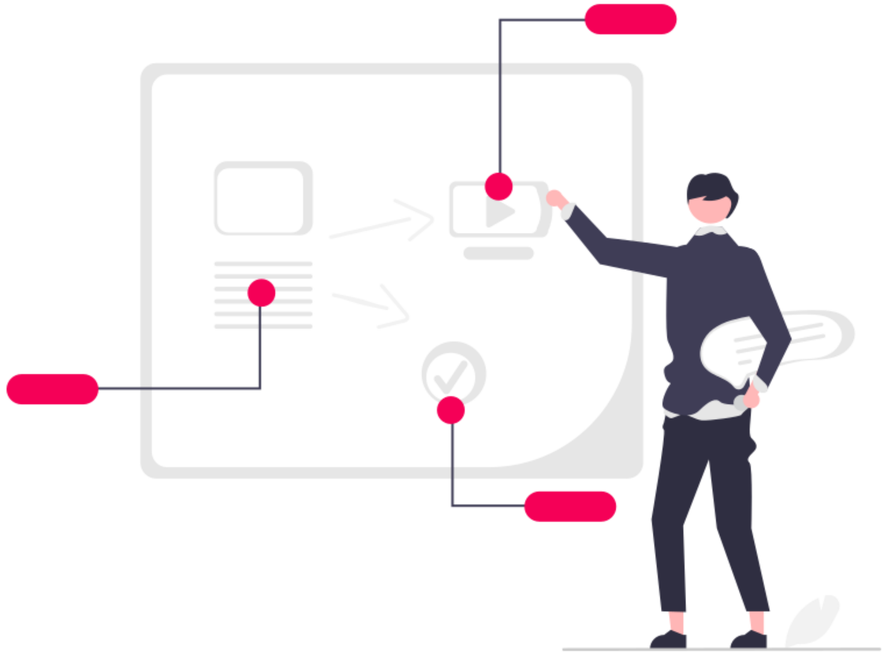


Introduction et théorie

Responsable du traitement

« personne privée ou organe fédéral qui, seul ou conjointement avec d’autres, détermine les finalités et les moyens du traitement de données personnelles »

⚠️ Supporte une responsabilité quasi illimitée quant aux traitements



Introduction et théorie

Sous-traitant

« personne privée ou organe fédéral qui traite des données personnelles pour le compte du responsable du traitement »

⚠️ Supporte une responsabilité limitée en principe à ses propres actions

Introduction et théorie

Organe fédéral

« l’autorité fédérale, le service fédéral ou la personne chargée d’une tâche publique de la Confédération »

➡️ y compris fondation LPP, caisse maladie, EPF, caisse privée de compensation, etc.

A quoi ça sert ?

Introspection

Être conscient-e

des coûts certains d’un incident

Mobilisation de ressources internes

Mobilisation de ressources externes

Dégât d’image, perte de crédibilité/clientèle, renégociation de contrats, clauses pénales activées pour violation du contrat, etc.

Être conscient-e

des mesures ou sanctions

Mesures administratives du PFPDT (p. ex. interdiction de traiter des données, ordre de supprimer des données)

Sanctions pénales (visant les personnes physiques prenant des décisions dans l'entreprise)

Procédures administratives (art. 41 LPD) ou civiles

Gouvernance

Information

et données personnelles

Permet d’avoir une vue macro des flux de données (d’où, où, vers où)

Comment appliquer le principe de sécurité en prenant des mesures de sécurité adéquates alors qu’on ne sait pas quelles données protéger, où et dans quelle situation ?

Compliance

Démontrer aux autorités qu’on a « fait le job » et que le sujet est pris au sérieux

Détecter les risques

Répondre aux demandes des personnes concernées

…

C’est obligatoire ?

Obligatoire si

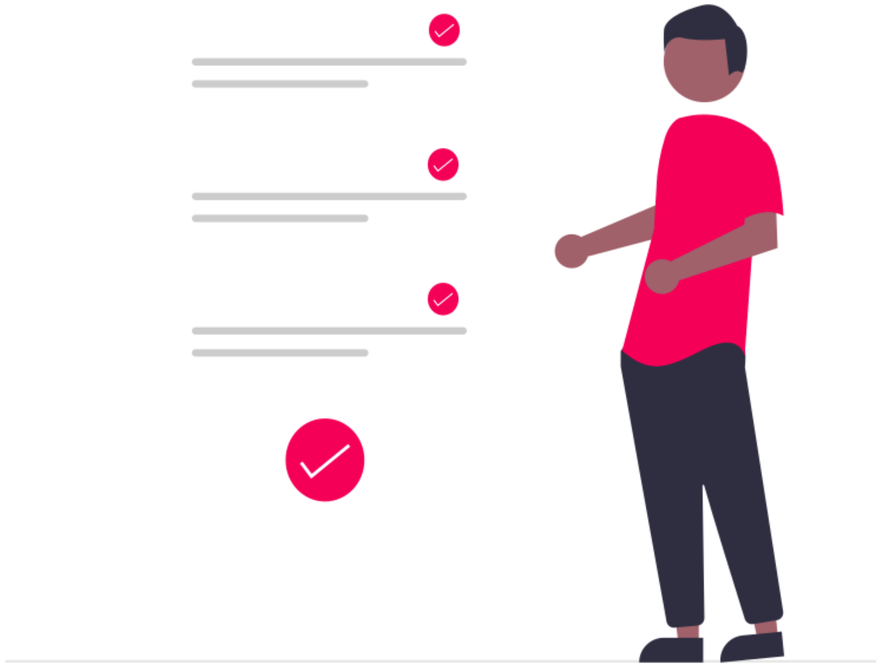
vous êtes un organe fédéral

ou si

vous employez au moins 250 collaborateurs (≠ EPT) au 1er janvier de l’année en cours

et si

le traitement présente un risque élevé d’atteinte à la personnalité des personnes concernées



Facultatif si

vous n’êtes pas un organe fédéral

et

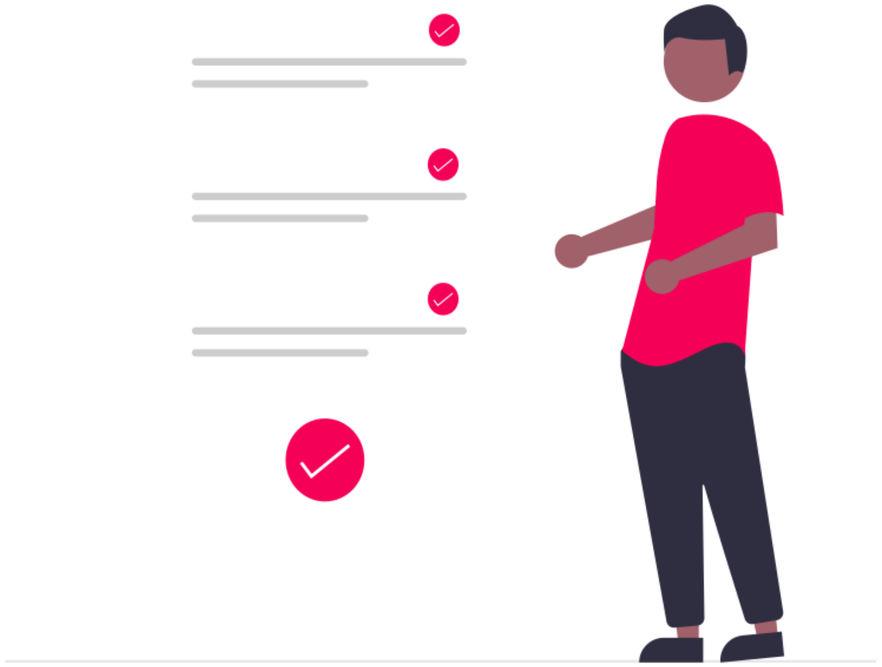
vous employez moins de 250 collaborateurs (≠ EPT) au 1er janvier de l’année en cours

sauf si

vous mettez en œuvre des traitements portant sur des données sensibles à grande échelle

ou si

vous mettez en œuvre des traitements constituant un profilage à risque élevé

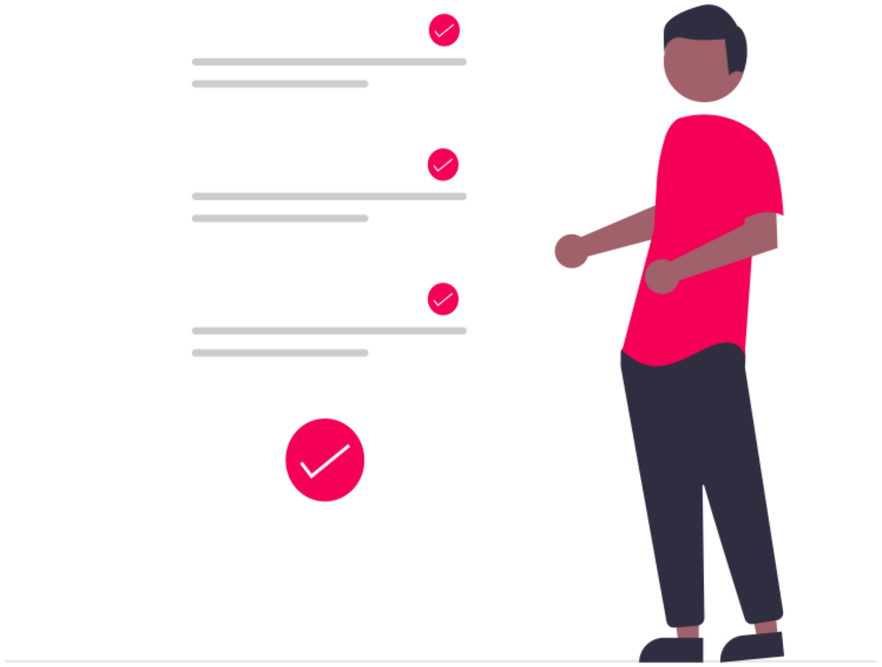


Traitements portant sur

des données sensibles à grande échelle

La notion de « grande échelle » doit être interprétée selon plusieurs critères, en particulier le volume de données traité, la durée du traitement, le nombre de personnes concernées par le traitement, l'étendue géographique de ce dernier

➡️ assurance santé et hôpitaux sont concernés à tout le moins



Traitements constituant

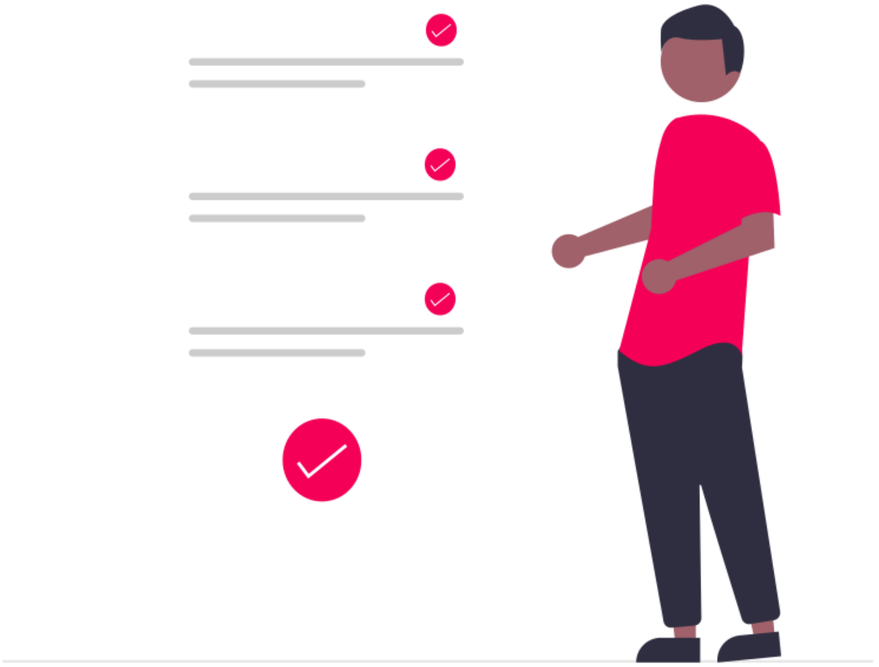
un profilage à risque élevé

Profilage qui doit permettre d'apprécier les caractéristiques essentielles de la personnalité d'un individu

et

Profilage qui représente un risque élevé au vu de la manière dont il est mis en œuvre

➡️ analyse de risque obligatoire



On y met quoi ?

On y mets quoi ?

Pour le responsable du traitement

Pour chaque processus/activité répondant aux conditions légales de création du registre :

- **Identité**
- **Finalité(s)**
- **Catégories de données et de personnes**
- **Catégories de destinataires (y c. ST)**
- **Délais de conservation**
- **Mesures de sécurité**
- **Pays en cas de transfert**

On y mets quoi ?

Pour le sous-traitant

Pour chaque processus/activité :

- **Identité + celle du RT**
- **Finalité(s) des traitements mis en œuvre pour le compte du RT**
- **Catégories de données et de personnes**
- **Catégories de destinataires (y c. ST)**
- **Délais de conservation**
- **Mesures de sécurité**
- **Pays en cas de transfert**

On y mets quoi ?

Informations facultatives supplémentaires

Pour chaque processus/activité :

- Base(s) juridique(s)
- Source(s) des données
- Analyse(s) de risques
- Décision automatisée
- Règles d’archivage et d’effacement
- Instructions du RT (pour le ST)

On y mets quoi ?

et comment surtout ?

Aucune exigence de forme, tant que l’autorité peut aisément consulter (et comprendre) le registre.

Comment on le crée ?

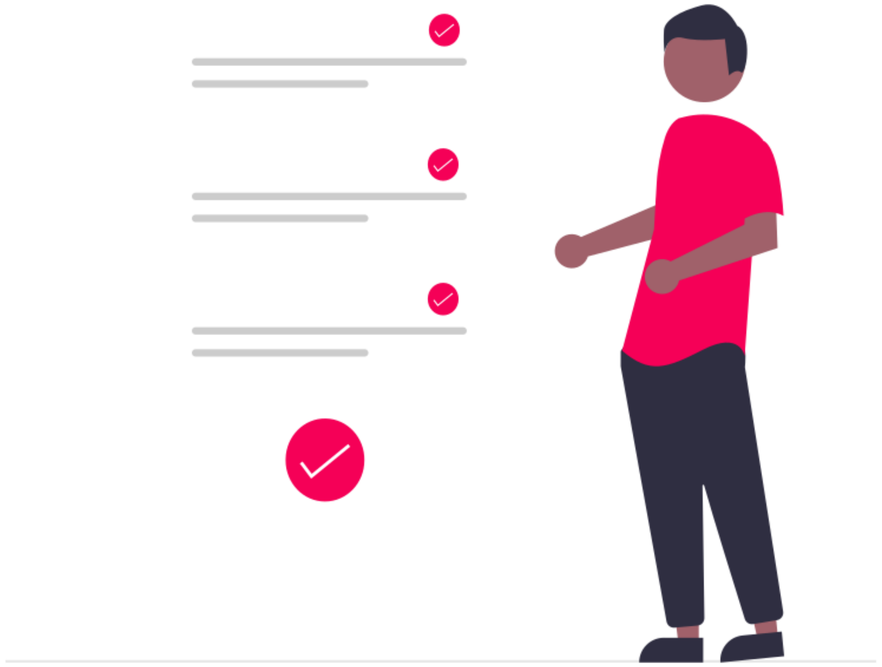
Comment on le crée ?

Préparer le terrain

Approche par « processus » ? (1 processus = 1 traitement)

Approche par « activité » ? (1 activité = 1 traitement)

Format et structure ? Niveau de détail ?



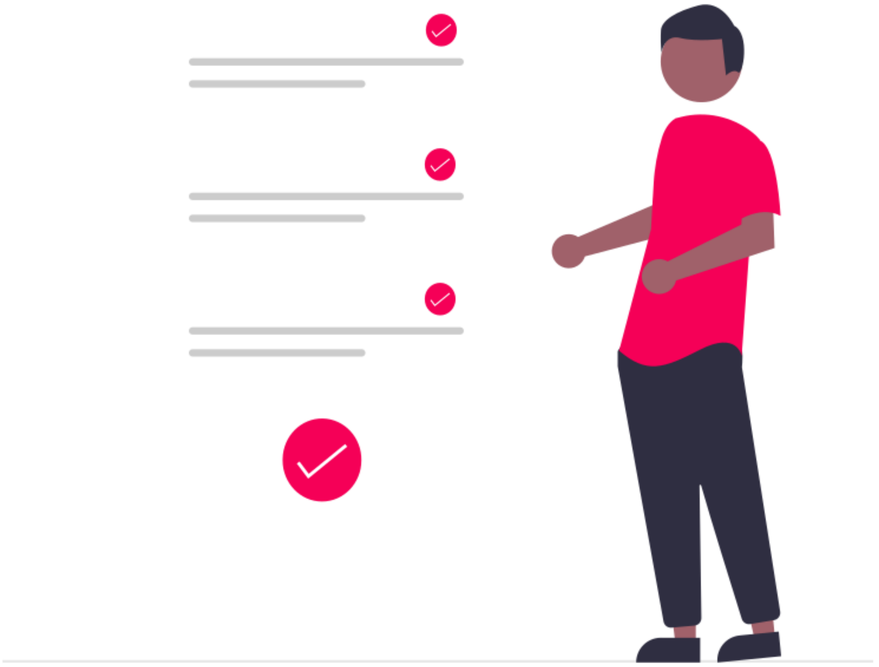
Comment on le crée ?

Préparer le terrain

Créer des listes de

- processus/activités (= traitements)
- applications
- catégories de données
- catégories de destinataires
- catégories de personnes concernées
- personnes de contact en interne

etc.

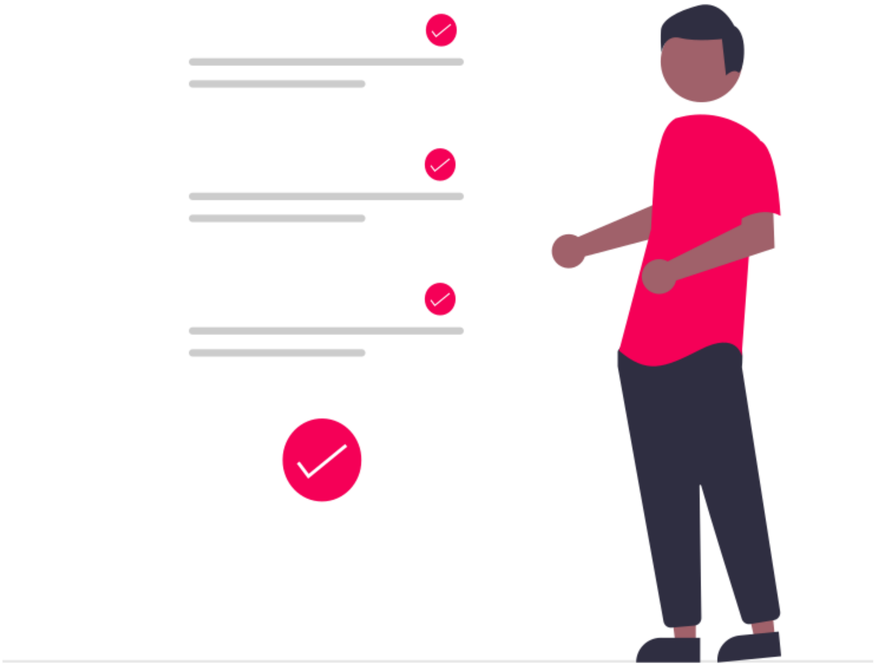


Comment on le crée ?

Informer et expliquer

Informer les parties prenantes en interne sur la démarche

- c’est quoi un registre ?
- ça sert à quoi ?
- comment on le crée ?
- qui sera impliqué ?
- ce que chacun y gagne ?
- le temps de travail estimé ?



Comment on le crée ?

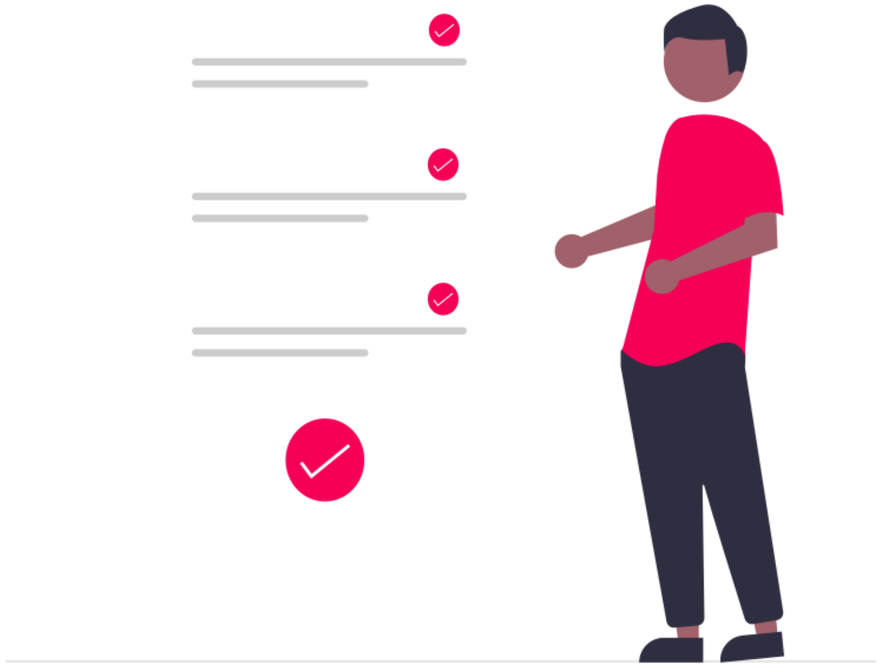
Informer et expliquer

Générer de l’adhésion (si possible)

Obtenir des réactions

Anticiper des écueils et corriger l’approche

Montrer une esquisse du résultat final



Comment on le crée ?

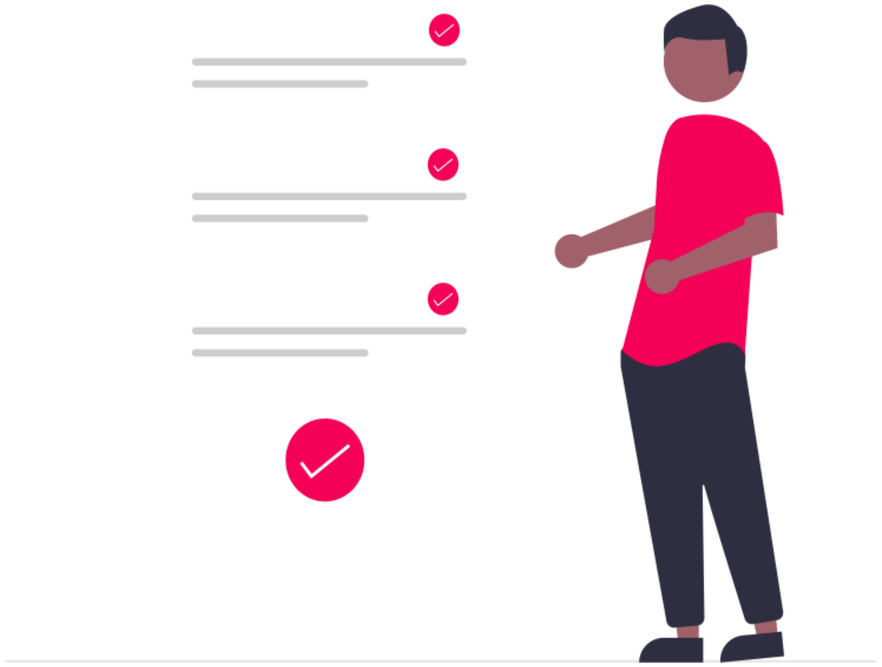
Récolter les informations

Questionnaires en ligne ?

Interviews ?

Combinaison des deux ?

Selon la taille de votre entité, la complexité de ses activités, la quantité de données traitées, le nombre de traitements, etc.



Comment on le crée ?

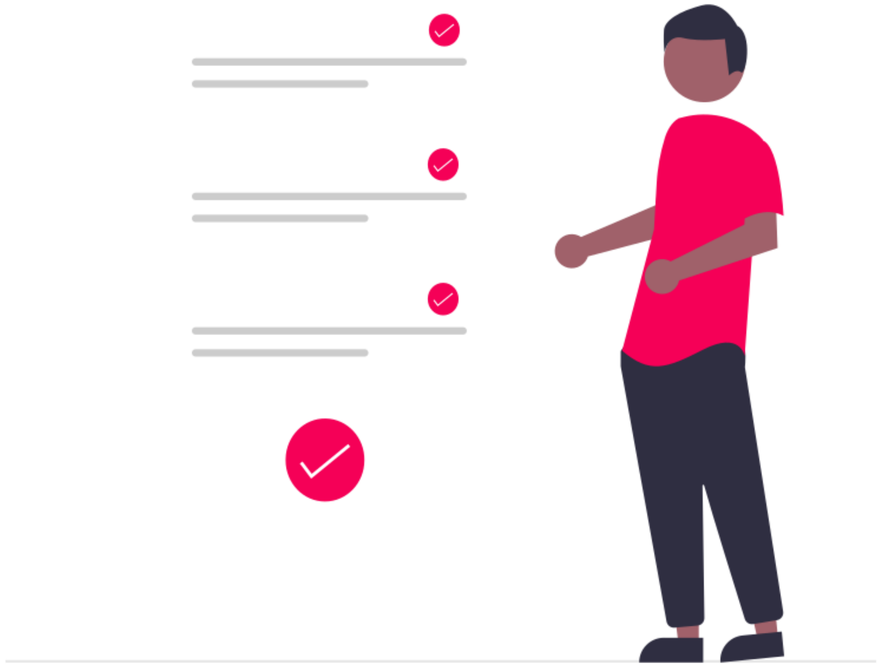
Récolter les informations

Fournir autant d’éléments que possibles pour

- aider à répondre et

- encadrer les réponses (listes d’éléments à choisir au lieu de réponses ouvertes)

➡️ utilité des inventaires constitués en amont

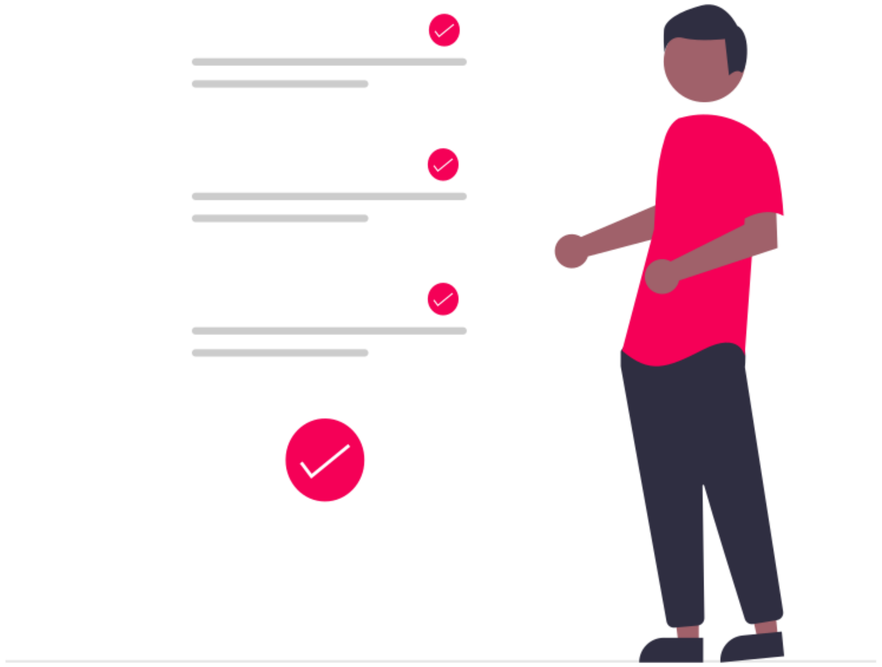


Comment on le crée ?

Récolter les informations

La récolte doit se faire processus par processus (ou activité par activité), en posant les mêmes questions à chaque fois

➡️ assurer la cohérence et la complétude



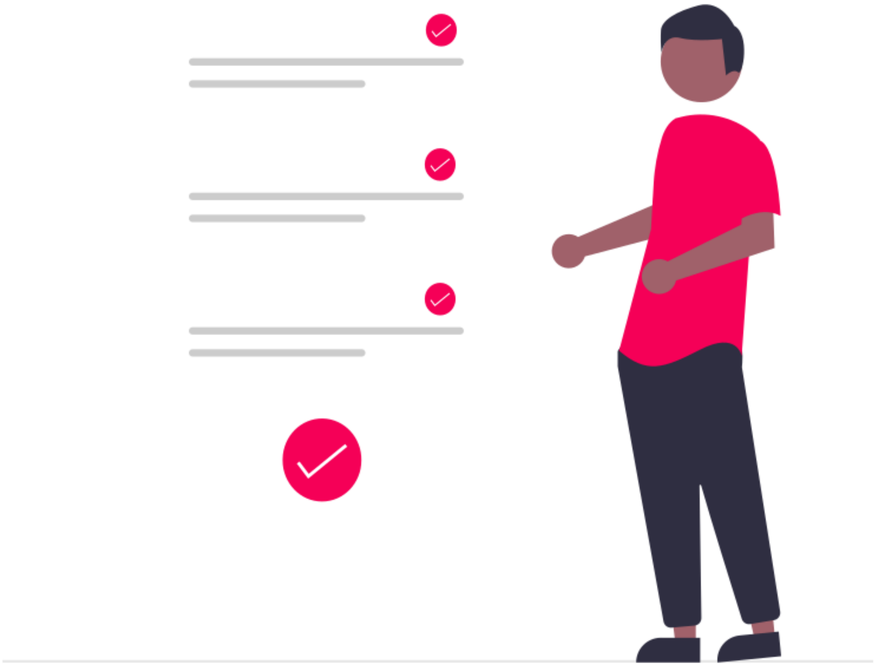
Comment on le crée ?

Analyser, clarifier, consolider

Errare humanum est.

Il faut analyser toutes les réponses, repérer les incohérences, corriger d'office ce qui est faux et demander une confirmation en cas de doute, etc.

⚠️ lorsqu'on déclare qu'aucune donnée personnelle n'est traitée

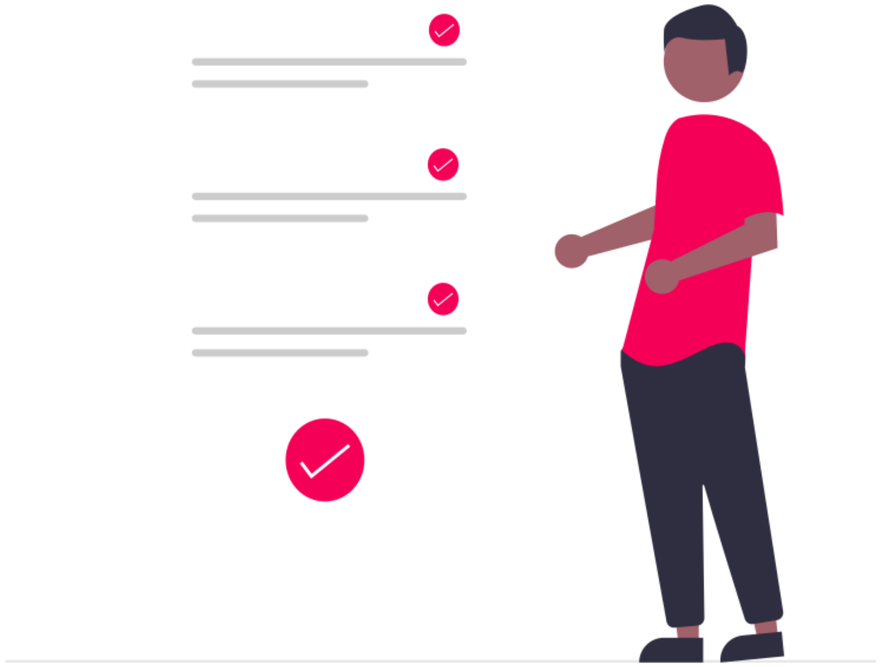


Comment on le crée ?

Analyser, clarifier, consolider

⚠️ aux traitements où il y a des données sensibles

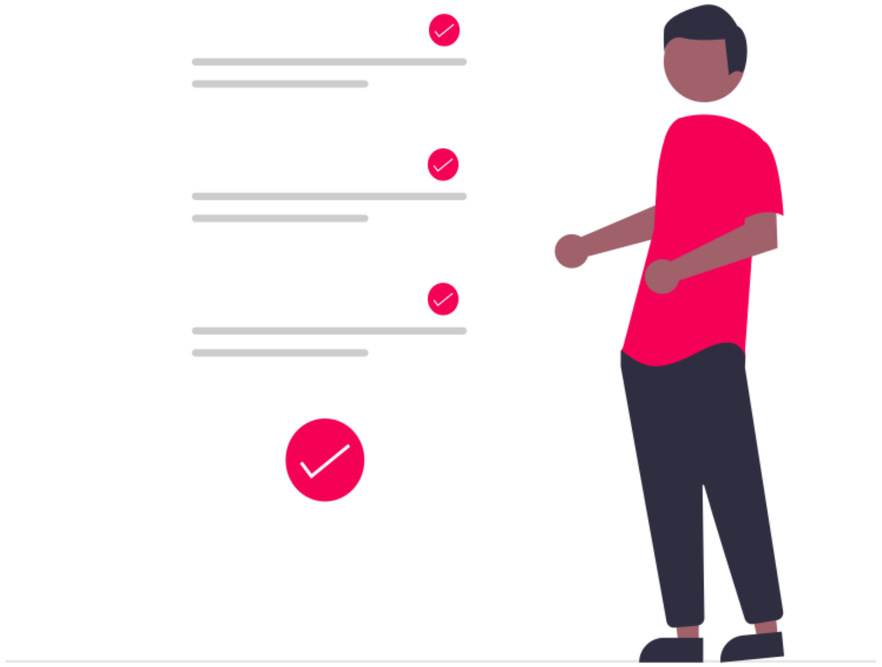
Les résultats doivent aussi permettre d’évaluer la nécessité de conduire une analyse de risques pour adapter d’éventuelles mesures de sécurité ou adapter le traitement, par exemple.



Comment on le crée ?

On le crée avec plaisir !

Les activités/processus qui ne traitent pas de données personnelles ne sont pas soumises à la LPD et n’ont pas besoin de figurer au registre



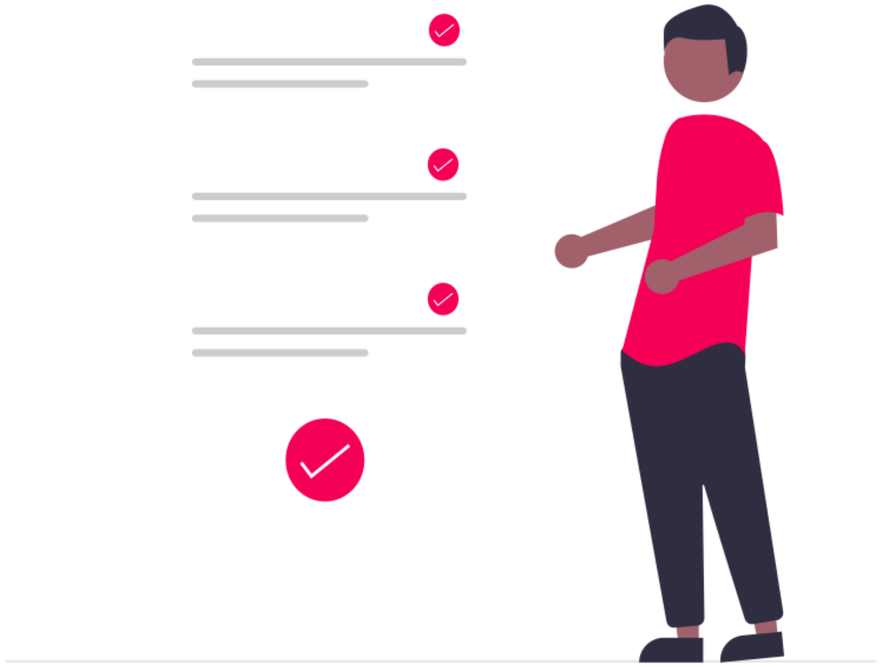
Responsable du traitement	**Nom du traitement (= processus/ activité)**	**Finalité**	Base juridique	**Catégorie de données**	**Catégorie de personnes concernées**	**Durée de conservation**	Origine des données	**Destinataires** ou sous-traitants	**Transferts des données vers**	**Mesures de sécurité**
Mon entreprise / une autre entreprise en tant que responsable conjoint	Gestion des données clients	Gérer les relations avec les clients (facturation, support, communication)	Contrat, intérêt légitime, consentement	Nom, prénom, adresse, téléphone, email, historique d'achats	Clients et prospects	5 ans à compter de la dernière activité	Personne concernée	Microsoft Azure	Irlande	Gestion des droits d'accès, chiffrement des données en transit
Mon entreprise	Analyse d'audience du site web	Analyser le comportement des utilisateurs sur le site web pour optimiser la navigation et les contenus	Intérêt légitime, consentement	Adresse IP, cookies, pages visitées, temps passé sur chaque page	Utilisateurs du site web	1 an	Site web, Sous-traitant	Google Analytics	Etats-Unis	Chiffrement des données en transit, anonymisation
Mon entreprise	Gestion des candidatures	Recrutement et sélection de nouveaux employés	Contrat, Consentement	CV, lettre de motivation, diplômes, expérience professionnelle	Candidats	2 ans à compter de la fin du processus de recrutement	Personne concernée, ex-employeur	Jobcloud	-	Gestion des droits d'accès, chiffrement des données en transit
Mon entreprise	Gestion des fournisseurs	Gérer les relations avec les fournisseurs (facturation, communication)	Contrat, intérêt légitime	Nom, prénom, adresse, téléphone, email, informations bancaires	Fournisseurs	10 ans à compter de la fin de la relation commerciale	Personne concernée, société d'évaluation de la solvabilité	Stripe, PayPal	Irlande, Pays-Bas, Etats-Unis	Gestion des droits d'accès, chiffrement des données en transit
Mon entreprise	Gestion des réseaux sociaux	Animer les comptes de l'entreprise sur les réseaux sociaux	Intérêt légitime, consentement	Contenu publié sur les réseaux sociaux, identifiants des utilisateurs qui interagissent	Utilisateurs des réseaux sociaux	2 ans à compter de la dernière interaction	Personne concernée, réseaux sociaux	Hootsuite, Buffer	Irelande, Allemagne, Etats-Unis	Gestion des droits d'accès, chiffrement des données en transit

Comment on le met à jour ?

On prend les mêmes et on recommence

En principe, à chaque modification de traitement, ou lors de chaque création/ suppression d’un traitement

Méthode similaire ou différente de celle utilisée pour la création



Conclusion

Conclusion

Réfléchissez. Ne faites pas un registre dans l’urgence.

Préparez le terrain, collectez des informations en amont.

Sensibilisez, expliquez et responsabilisez.

Fournissez de l’aide et soyez clairs sur le résultat attendu.

Challengez les réponses sans les mettre en doute.

Publiez le résultat à l’interne.

Merci

de votre
attention
patience
endurance