Les violations de la sécurité des données dans la nouvelle LPD

François Charlet

7 décembre 2023

De quoi parle-t-on ?

Violation

de la sécurité des données

⚠️ Ne concerne que les données personnelles

« 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 »

En plus de gérer la violation

que faut-il faire d’autre ?

1. Chercher à empêcher qu’elle se produise

➡️ se préparer à ce qu’elle survienne

2. Anticiper les actions à réaliser pour gérer la violation et ses conséquences à court et moyen terme

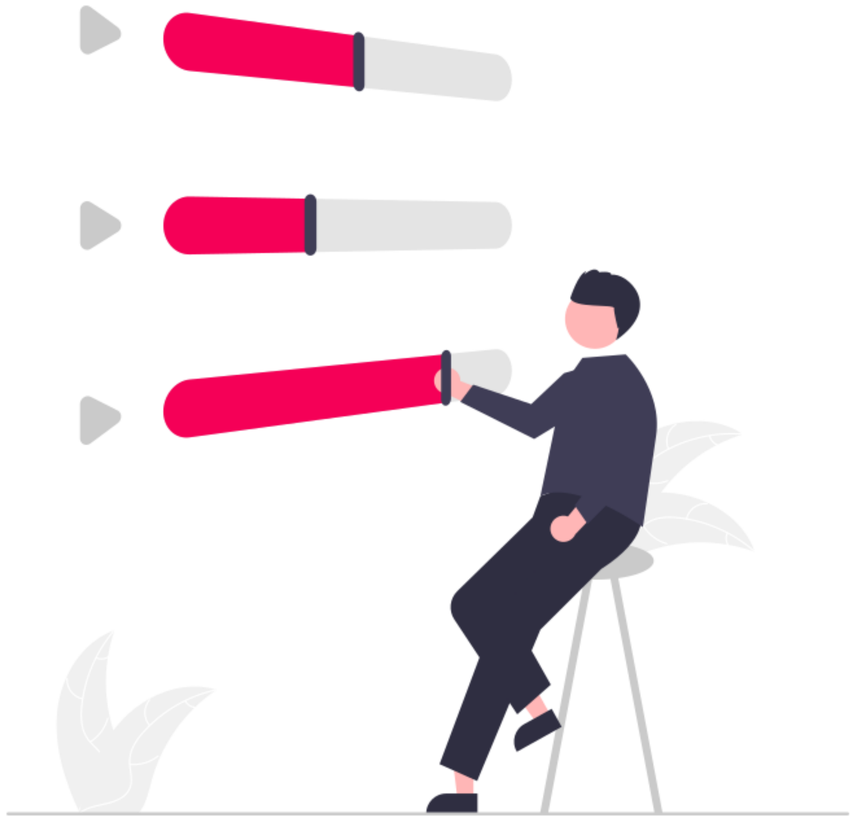
➡️ éviter d’agir sous la panique et sans repères

Conséquences

d’une violation

Droits des personnes concernées atteints, notamment

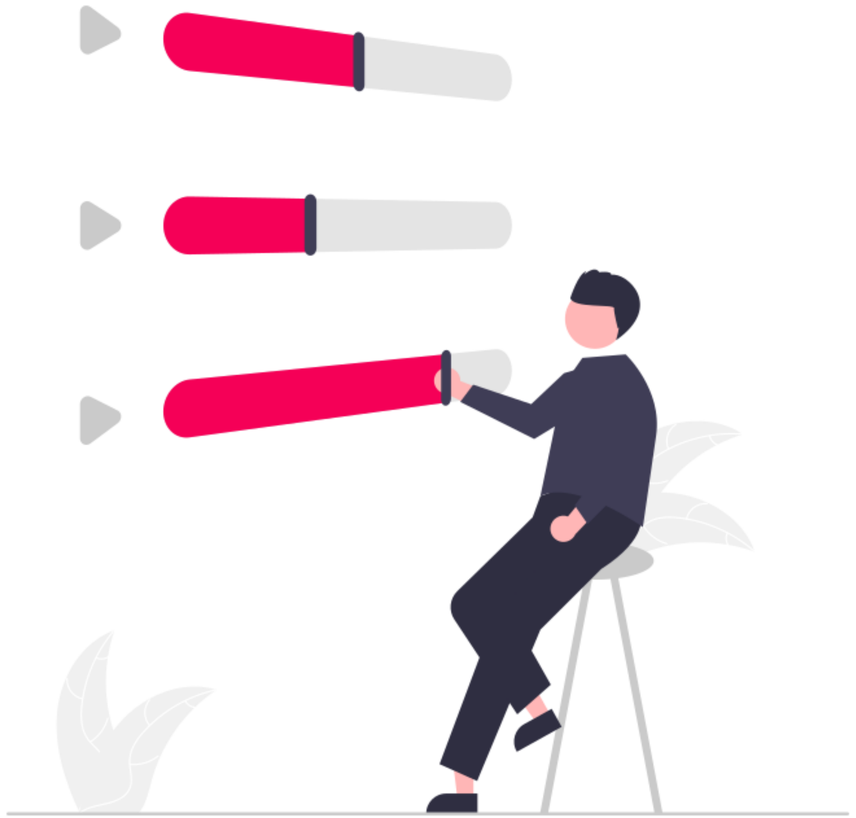
- usurpation d’identité
- réputation entachée
- dommage financier
- difficulté à accéder ou à utiliser des produits ou services



Conséquences
d’une violation

Crédibilité de l’entreprise atteinte, notamment

- réputation entachée
- confiance à reconstruire (clients, collaborateurs, partenaires…)
- dommage financier
- procédures administratives, civiles ou pénales

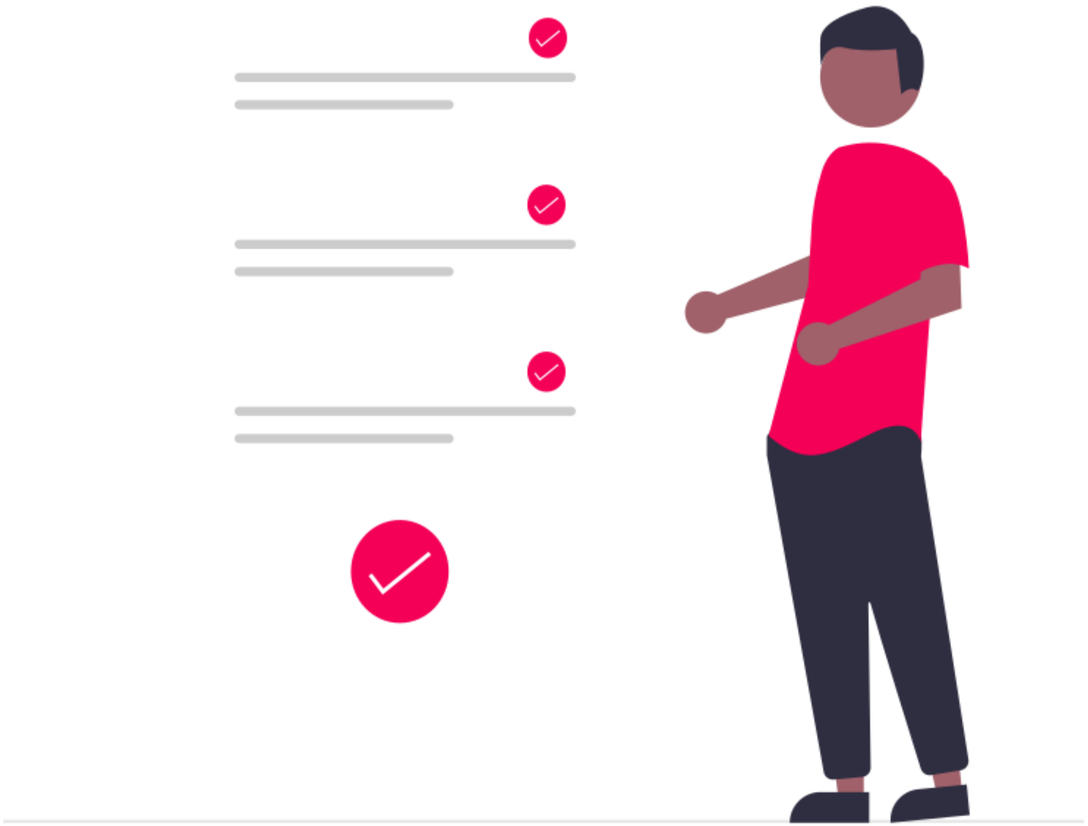


Principe de sécurité

En quoi consiste
le principe de sécurité ?

Il s’agit de

- prendre les mesures techniques et organisationnelles appropriées
- afin d’assurer une sécurité adéquate des données et des traitements,
- en fonction des risques encourus pour les personnes concernées, de l’état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement.



Rappel : la sécurité n’est pas qu’informatique, mais a une composante physique et également humaine.

Rappel (bis) : la sécurité, comme la protection des données, ne rapporte rien en soi ; il s’agit d’un coût d’opportunité.

Composantes

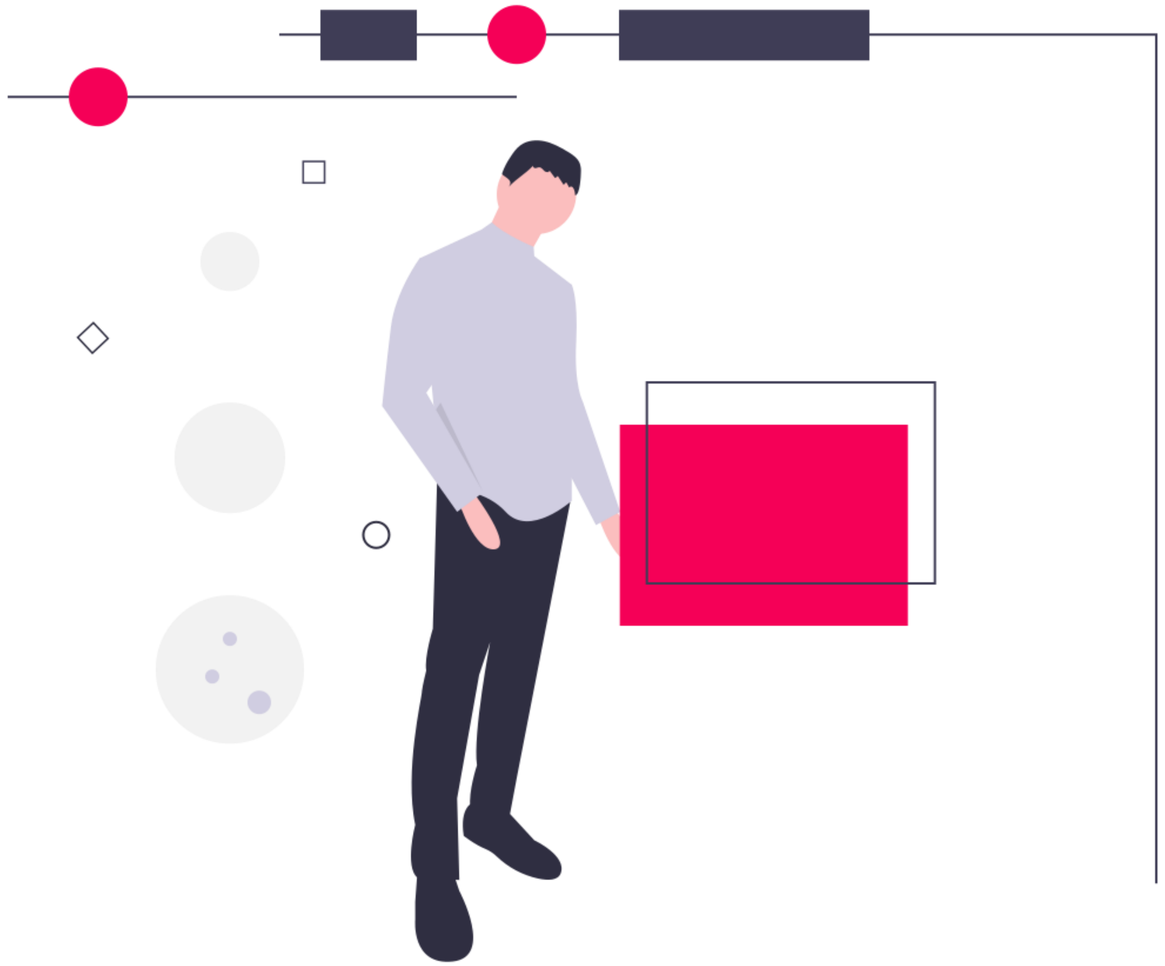
du principe de sécurité

Confidentialité

- seules les personnes qui ont besoin de traiter les données personnelles concernées peuvent y avoir accès (= need-to-know)
- cet accès est d'ailleurs limité aux actes que la personne a effectivement besoin de réaliser (= least priviledge)

Composantes

du principe de sécurité



Intégrité

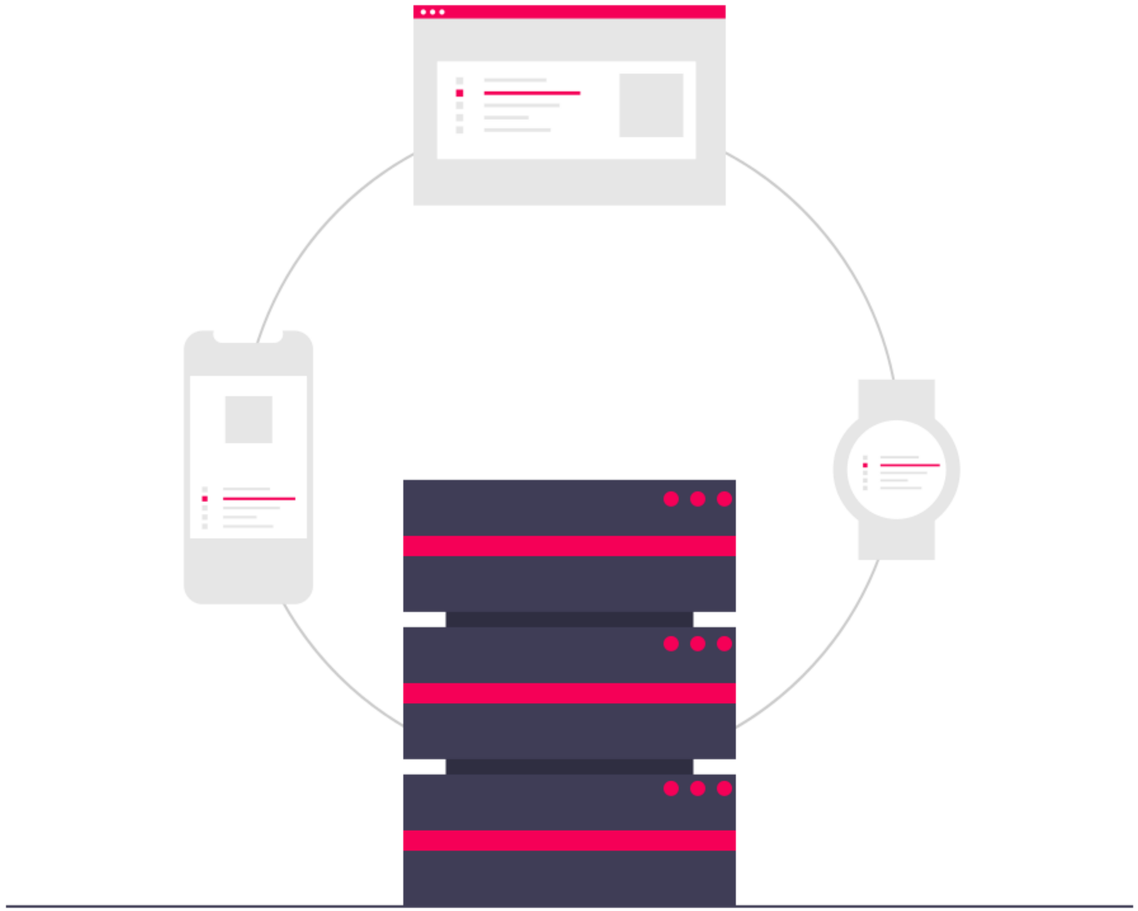
- les données personnelles sont correctes et dans un état ou format conforme à leur but.
- les données ne doivent pas pouvoir être modifiées de manière non autorisée pendant leur stockage, transmission ou utilisation.

Composantes

du principe de sécurité

Disponibilité

- les données sont toujours accessibles aux personnes qui en ont besoin (et qui sont donc autorisées à y accéder).
- tous les systèmes fonctionnent correctement et les éventuels problèmes qui surviendraient ne perturbent pas – ou le moins possible – les utilisateurs ou autres systèmes.



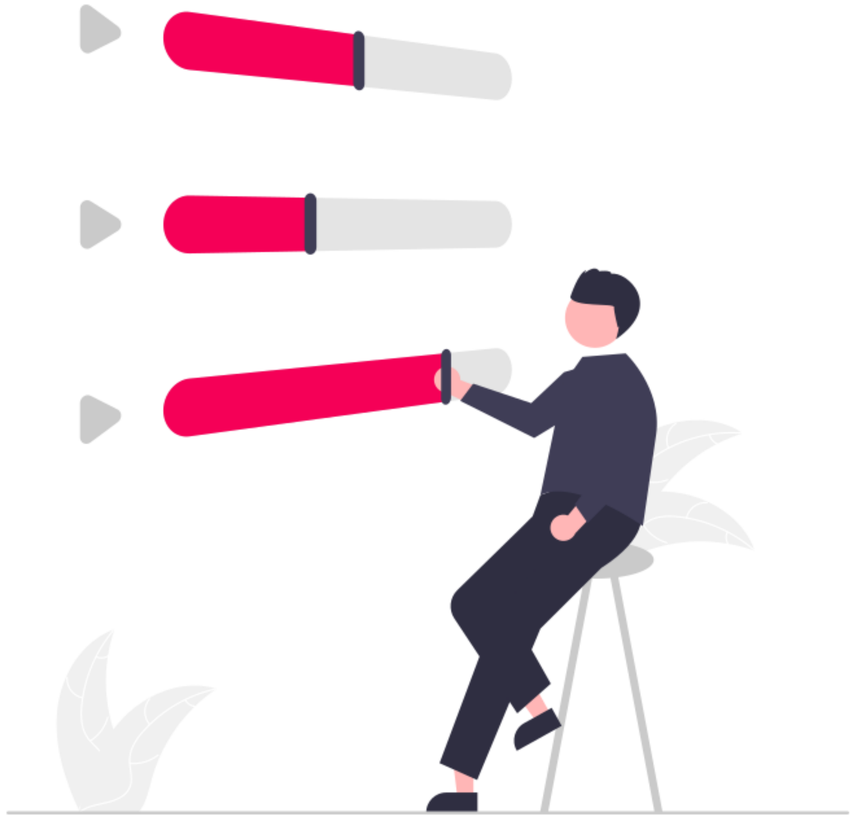
Comment savoir quelle mesure de sécurité adopter ?

Il faut conduire des analyses de risques pour choisir et implémenter les mesures techniques et organisationnelles qui sont adaptées.

Il n’est pas raisonnable d’adopter trop de mesures de sécurité, mais il peut aussi s’avérer périlleux de ne pas en implémenter suffisamment ; de même, adopter des mesures qui n’atteignent pas leur cible est inutile.

Critères à considérer

pour sélectionner les mesures adéquates



Notamment

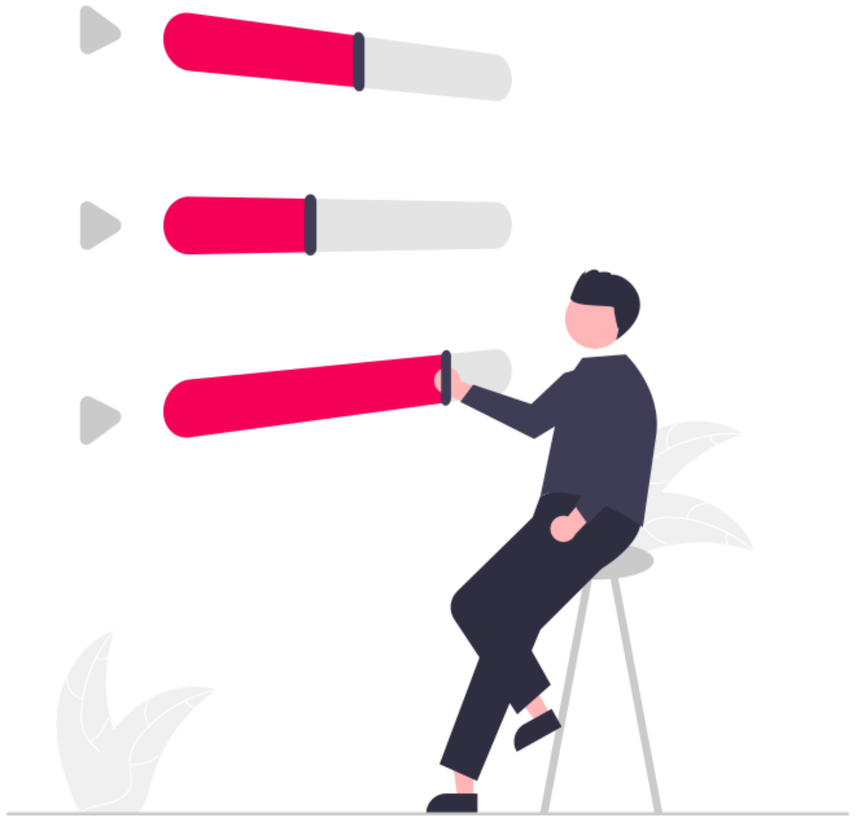
- Nature et finalité du traitement
- Etendue et circonstances du traitement
- Probabilité et impact d’une violation de la sécurité
- Coûts de mise en oeuvre des mesures de sécurité envisagées
- Etat des connaissances

Evaluer si les mesures

sont adéquates

Permet notamment de

- déceler des failles
- découvrir l'inefficacité d'une mesure
- démontrer les améliorations du niveau de sécurité



Exemple

Données médicales d'une clinique

- Nature et finalité du traitement
  Traitement automatisé, buts d'étudier les patients, les soigner après analyse des symptômes, suivre l'évolution du patient dans le temps…

- Etendue et circonstances du traitement
  Plusieurs centaines de personnes concernées par mois, traitement de données bénéficie aux patients, secret médical, rapport de « dépendance » (?)

- Probabilité et impact d'une violation de la sécurité
  Forte probabilité sur 10 ans, impact élevé sur les personnes concernées

- Coûts de mise en oeuvre des mesures de sécurité envisagées
  A estimer, probablement plusieurs dizaines de milliers de CHF

- Etat des connaissances
  Pas nécessaire d'avoir des technologies avant-gardistes

Exemple

Données RH

- Nature et finalité du traitement
  Traitement automatisé, buts d'évaluer les performances, gérer les absences, payer les salaires…
- Etendue et circonstances du traitement
  Plusieurs dizaines de personnes concernées par mois, traitement de données bénéficie aux employés ET à l'employeur, lien hiérarchique
- Probabilité et impact d'une violation de la sécurité
  Forte probabilité sur 10 ans, impact élevé sur les personnes concernées (personnel et professionnel)
- Coûts de mise en oeuvre des mesures de sécurité envisagées
  A estimer, probablement plusieurs dizaines de milliers de CHF
- Etat des connaissances
  Pas nécessaire d'avoir des technologies avant-gardistes

Quelles mesures de sécurité ?

pour les données médicales et RH

- Renforcement général des systèmes (need-to-know, least priviledge, désactivation des fonctionnalités non nécessaires, antivirus, firewall, journalisation des actions, sauvegardes quotidiennes, règles de mot de passe)
- Chiffrement des communications (emails notamment, VPN)
- Cloud utilisé ? Mesures juridiques impératives, voire techniques si possible
- Comptes privilégiés ? Mise au rebut de matériel ?
- Sensibilisation et formation

Et si une violation se produit ?

Violation de la sécurité

Quatre conditions cumulatives

- concrétisation d’un événement redouté (connu et anticipé, ou non) ayant des effets sur la sécurité
- entraînant, de manière accidentelle ou illicite
- la destruction, la perte, l’altération, la divulgation non autorisée ou l’accès
- à des données personnelles transmises, conservées ou traitées d’une autre manière.

Violation de la sécurité

Eléments sans importance

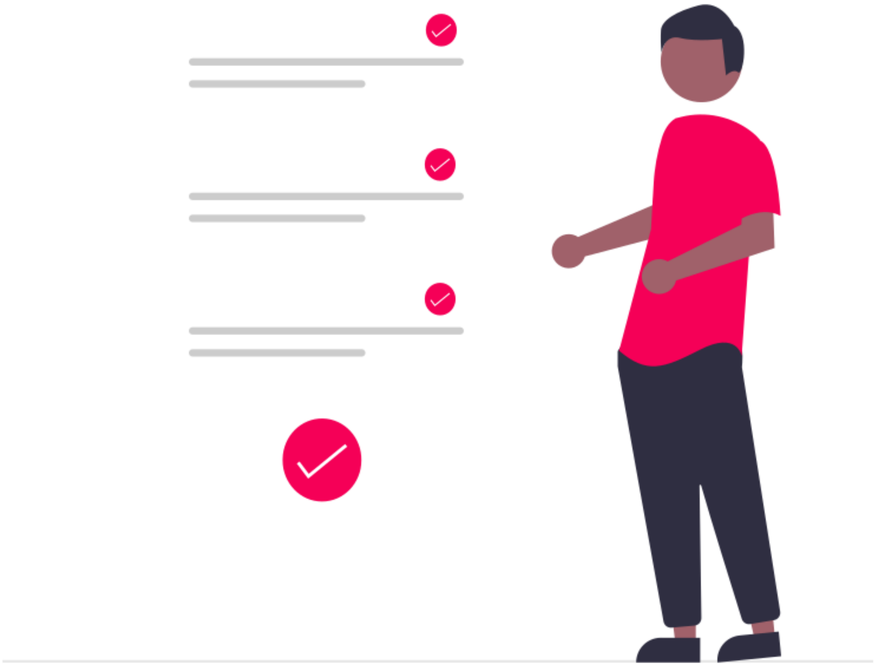
- origine humaine ou informatique
- par un collaborateur ou un tiers
- intentionnelle ou accidentelle
- grande ou faible ampleur
- conséquences concrètes lors de la survenance

Violation de la sécurité

Vous êtes-vous préparés ?

Notamment

- Qui est responsable stratégiquement dans l'entreprise ?
- Procédures en cas de violation ?
- Qui gère la violation ? Liste de prestataires externes ?
- Différencier un incident d'une violation ?
- Personnes de contact ?

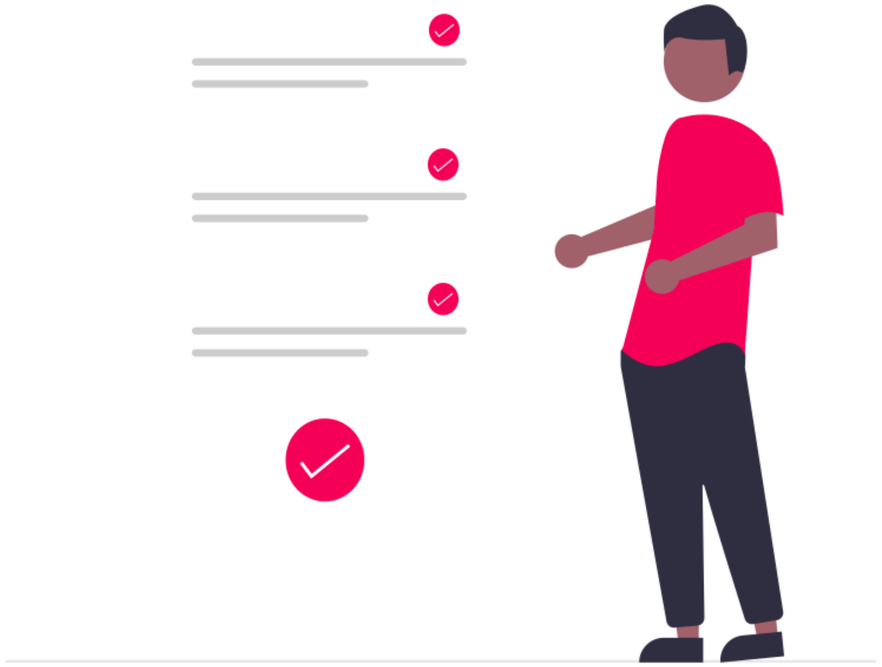


Violation de la sécurité

L’avez-vous détectée/analysée ?

Notamment

- Vecteur d’attaque ?
- Vulnérabilité ?
- Quels comptes utilisées ?
- Informations/données volées et par quel moyen ?

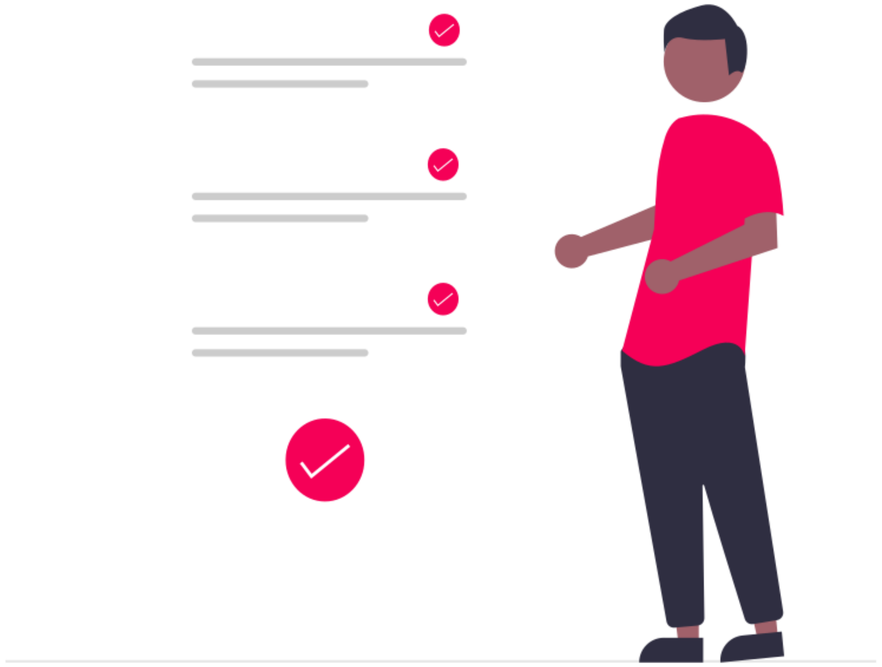


Violation de la sécurité

Quel est son impact ?

Notamment

- Impact opérationnel ?
- Impact sur les informations/ données ?
- Effort de récupération (retour à la normale) ?

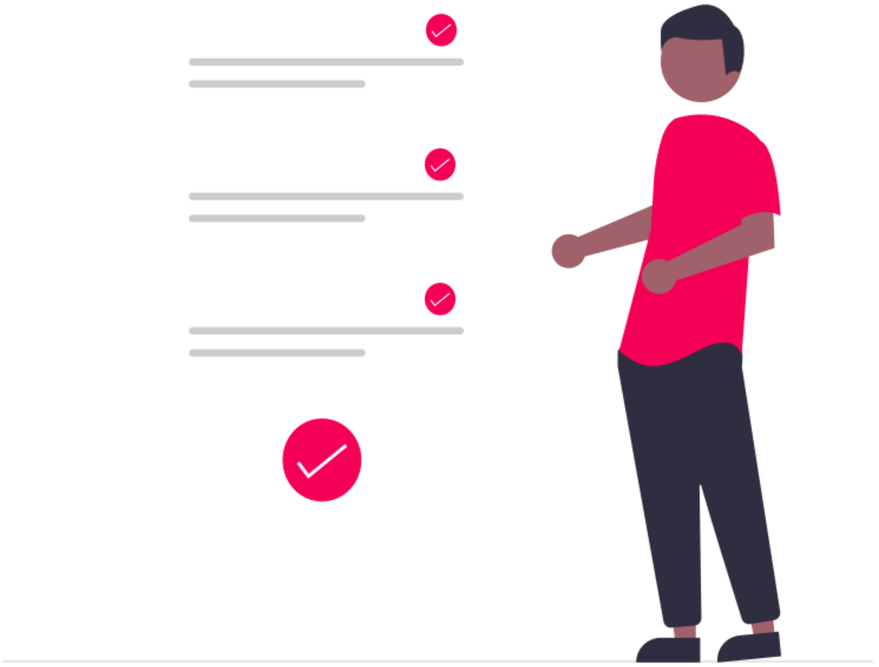


Violation de la sécurité

Comment y répondre ?

Notamment

- Empêcher que la situation empire
- Limiter les dégâts immédiats
- Mobilisation de ressources (internes ou externes)



Violation de la sécurité

Faut-il notifier ?

- Le responsable du traitement ?
- Le PFPDT ?
- Les personnes concernées ?

Violation de la sécurité

Faut-il notifier le responsable du traitement ?

- Le sous-traitant (ultérieur) doit annoncer la violation dans les meilleurs délais après en avoir pris connaissance
- Connaissance = moment où le sous-traitant a un degré raisonnable de certitude qu'un incident de sécurité s'est produit et a conduit à la compromission de données personnelles
- Délai fixé contractuellement

Violation de la sécurité

Faut-il notifier le PFPDT ?

- Lorsque la violation entraîne vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée
- Comment déterminer ce risque élevé ?
- « Dans les meilleurs délais »

Violation de la sécurité

Faut-il notifier le PFPDT ?

- Type de violation
- Nature, sensibilité et quantité de données
- Facilité d’identification
- Gravité des conséquences
- Type et nombre de personnes concernées
- Type de responsable du traitement

Violation de la sécurité

Faut-il notifier les personnes ?

- Lorsque c’est nécessaire à leur protection ou si le PFPDT l’exige
- Si la personne concernée peut prendre elle-même des dispositions pour se protéger des effets négatifs (effectifs ou potentiels)
- Notifier par quel moyen ?

Violation de la sécurité

Exemples de cas de notification au PFPDT et aux personnes

- Attaque par ransomware d'un hôpital, données sauvegardées correctement, aucune fuite ni vol de données
- Attaque par ransomware, données mal ou pas sauvegardées correctement, avec fuite ou vol de données
- Vol de données relatives à des candidatures à des emplois depuis un site web
- Attaque par utilisation d'identifiants volés (credential stuffing) pour accéder à un e-banking
- Vol de matériel informatique contenant des données non chiffrées
- Vol de documents papier contenant des données sensibles

Violation de la sécurité

Limites à l’information des personnes concernées

Notamment

- Intérêts prépondérants d’un tiers
- Devoir légal de garder le secret
- Information impossible à fournir ou exige des efforts disproportionnés

Violation de la sécurité

Contenu de la notification

Au PFPDT

- Art. 15 OPDo (+ formulaire en ligne sur le site du PFPDT)

Aux personnes concernées

- idem, dans un langage simple et compréhensible

Et si on dissimulait tout sous le tapis, ni vu ni connu ?

Conclusion

Conclusion

Le principe de sécurité exige de l'entreprise de prendre des mesures de sécurité en fonction de certains critères.

Analyser ces critères n'est pas aisé mais permet d'établir des priorités, de consacrer le temps et l'argent qu'il faut (sans exagérer, ni sous-estimer).

Toute violation ne doit pas être annoncée, mais lorsqu'elle doit l'être, on ne peut pas attendre, d'où l'importance d'être préparé et de savoir quoi faire.

La question n'est pas de savoir si la violation se produira, mais quand.