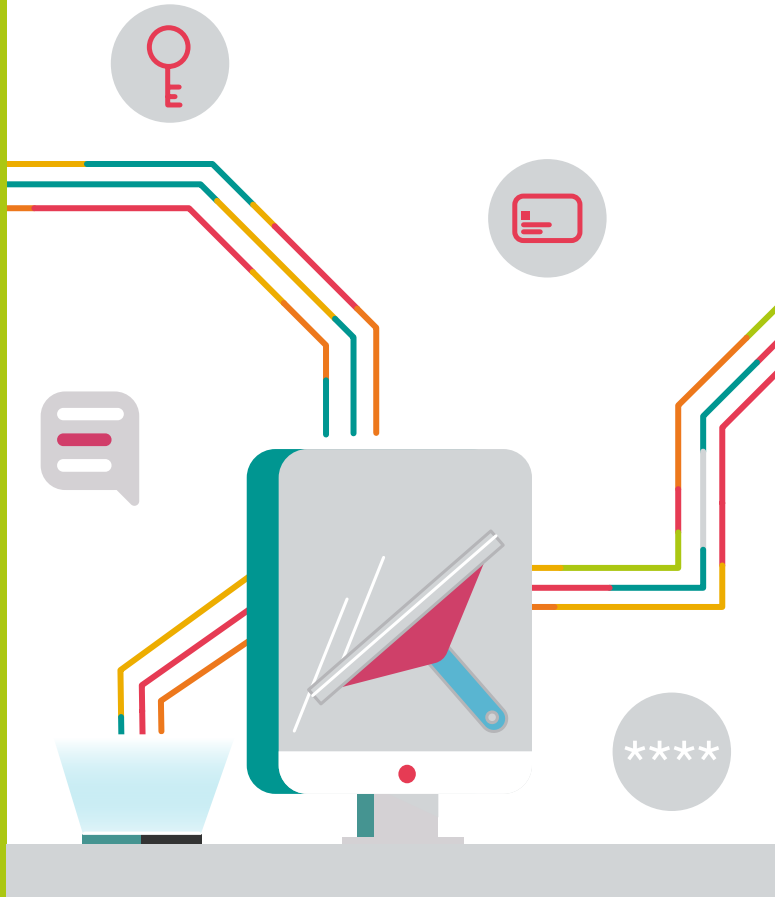
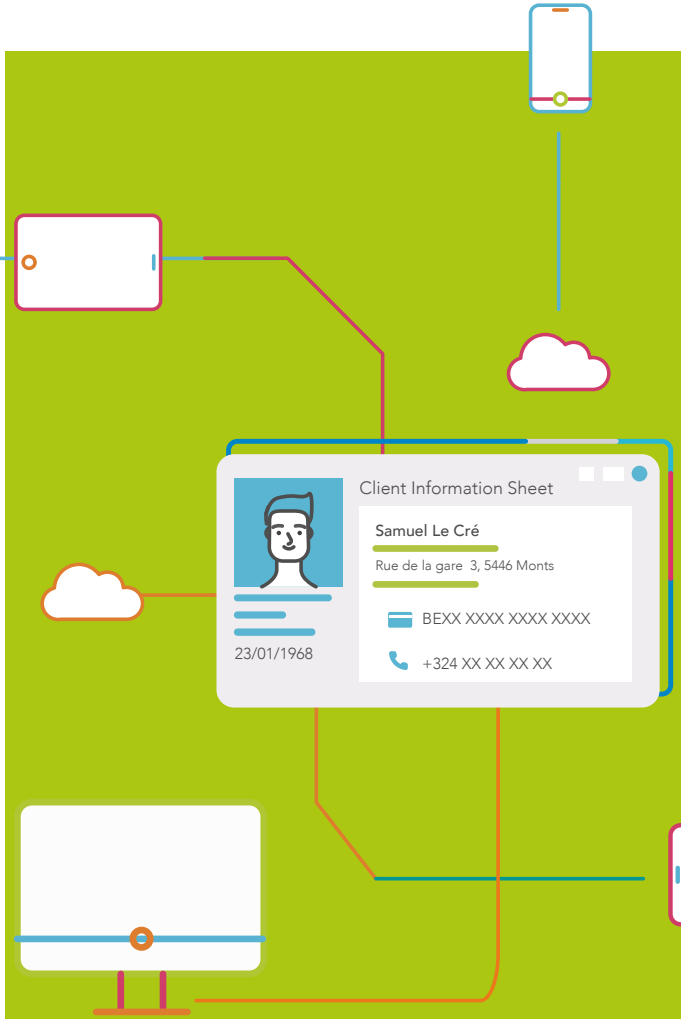
GDPR
DATA CLEAN-UP

CONTRIBUEZ À LA PROTECTION DES DONNÉES. IL EST TEMPS DE FAIRE LE MÉNAGE !



CYBER SECURITY COALITION.be



Dans cette brochure, nous vous montrerons comment trier les données à caractère personnel que vous sauvegardez durant l'exercice de votre travail – sur votre ordinateur portable, dans vos applications, sur votre GSM ou dans le cloud.

Pourquoi est-il si important d'effectuer un nettoyage ?

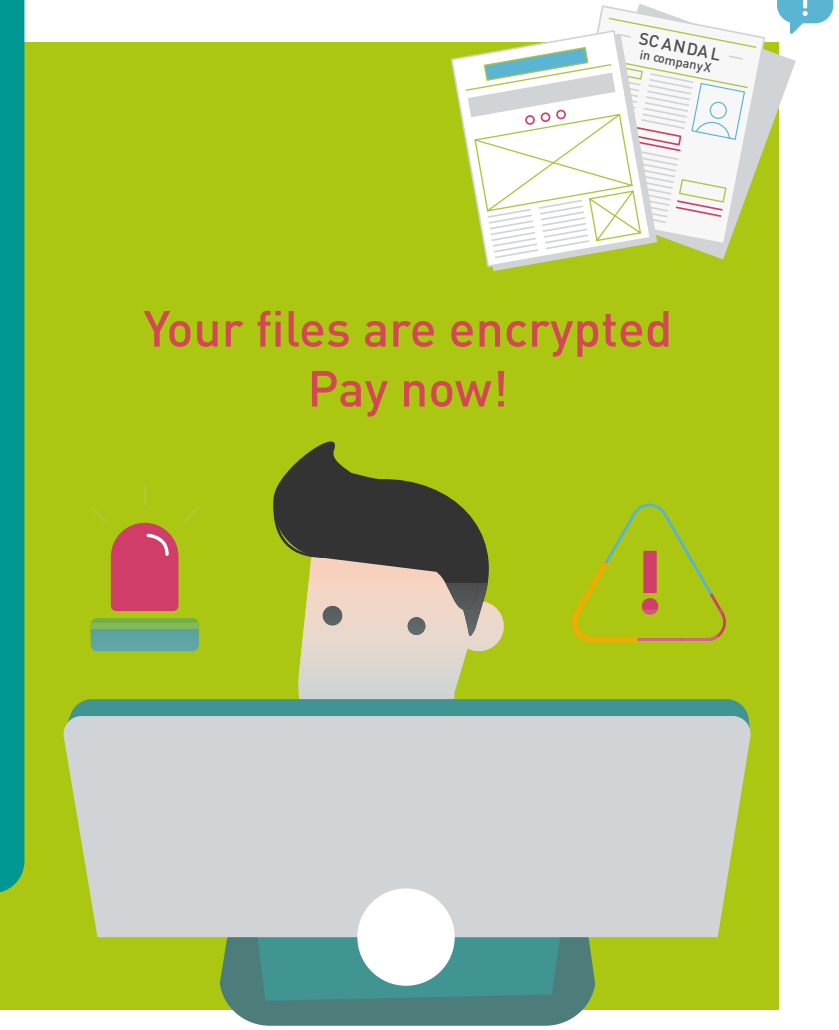
Les données à caractère personnel sont partout
Vous serez surpris de la quantité de données à caractère personnel que vous conservez dans le cadre de votre travail sur divers appareils et dans diverses applications ou apps (par exemple sur votre ordinateur portable, votre smartphone ou tablette à des fins professionnelles, ainsi que sur des clés USB et des disques durs externes). Chaque jour, nous envoyons et conservons des données à caractère personnel dans nos boîtes aux lettres électroniques, sur des applications, dans un cloud, etc.

Un risque réel et élevé

Tout comme les autres données, les données à caractère personnel sont sujettes à la perte, au vol ou à la violation de la confidentialité. Si une organisation perd des données à caractère personnel ou si ces données sont volées, les répercussions peuvent être très graves. Une fuite de données a des conséquences non seulement pour les personnes concernées (en termes de risques), mais aussi pour l'entreprise (image ternie, amendes, perte de clients). En outre, il est légalement obligatoire de supprimer les données à caractère personnel lorsque la finalité du traitement a été atteinte.

Tout le monde est concerné

La responsabilité de la protection des données incombe à votre entreprise ou organisation. Mais en tant que collaborateur, vous pouvez également apporter une contribution importante. En traitant correctement les données à caractère personnel, vous protégez les autres et vous aidez votre organisation à maintenir sa bonne réputation. Traitez les données à caractère personnel des autres comme vous souhaiteriez que les vôtres soient traitées.



Protection des données : une brève introduction

GDPR

Le GDPR (General Data Protection Regulation) est en vigueur depuis le 25 mai 2018. Cette réglementation européenne définit les mesures nécessaires à prendre par l'ensemble des entreprises afin de protéger les données à caractère personnel.

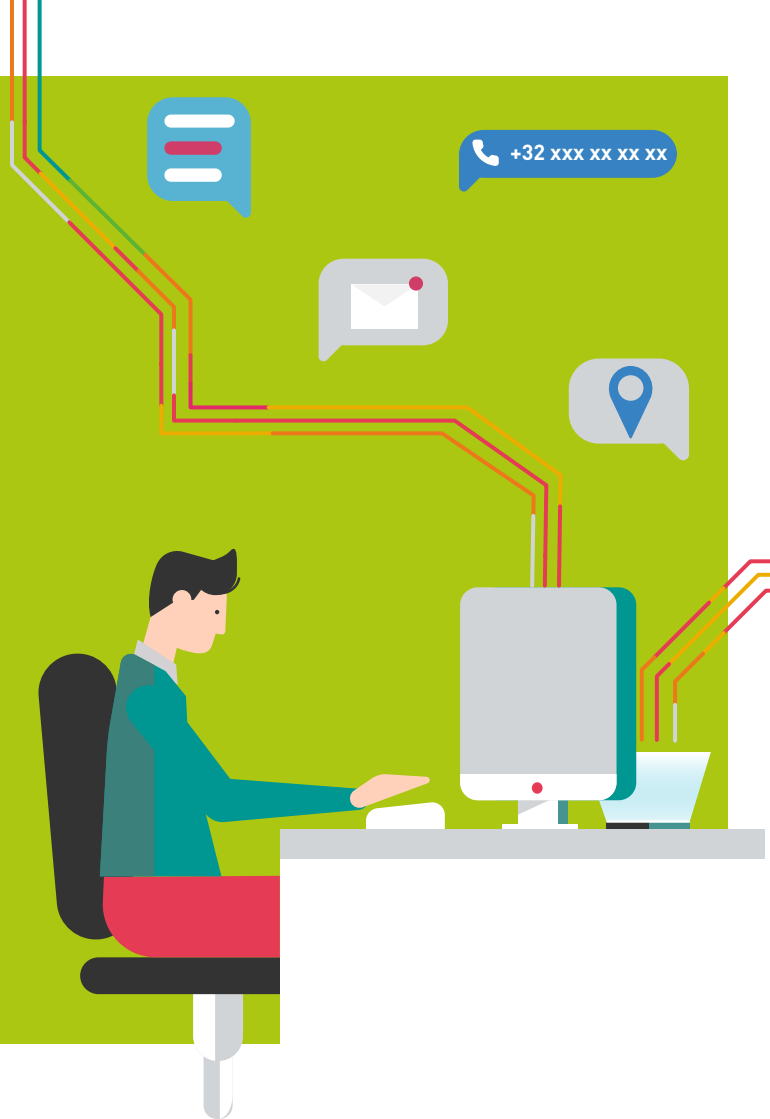
Principes de base

Le GDPR détermine donc la manière dont nous collectons, traitons et conservons les données à caractère personnel de manière légale et sécurisée. Parmi les principes de base, notons que les données à caractère personnel ne peuvent être collectées qu'à des fins spécifiques et légitimes, et que nous ne pouvons pas conserver ces données plus longtemps que nécessaire. En outre, nous devons veiller à ce que les données à caractère personnel soient traitées en toute sécurité.

Qu'entendons-nous par « données à caractère personnel » ?
Il s'agit de toutes les données qui identifient une personne ou sur la base desquelles une personne peut être directement ou indirectement identifiée. Le nom, le numéro de téléphone et l'adresse e-mail sont des exemples évidents, mais les informations de paiement, les photos, les évaluations et les données de localisation sont également des données à caractère personnel.

Par ailleurs, il existe une catégorie spécifique de données sensibles qui requiert une attention particulière. Il s'agit par exemple des données relatives à la santé, aux opinions politiques, aux croyances religieuses...

De quelles personnes s'agit-il en l'occurrence ?
Le GDPR s'applique à toutes les données à caractère personnel collectées, traitées et conservées au sein de votre organisation. Il peut s'agir de données provenant de clients, de prospects, de collaborateurs ou de fournisseurs.



Comment procéder ?

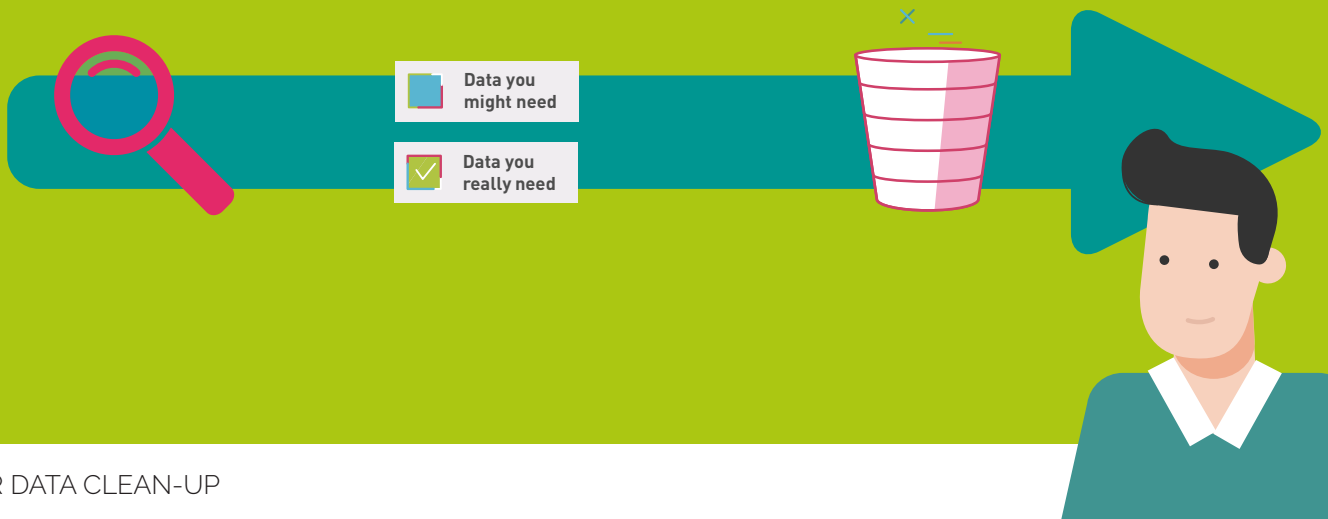
Êtes-vous fin prêt(e) pour le nettoyage des données à caractère personnel ?

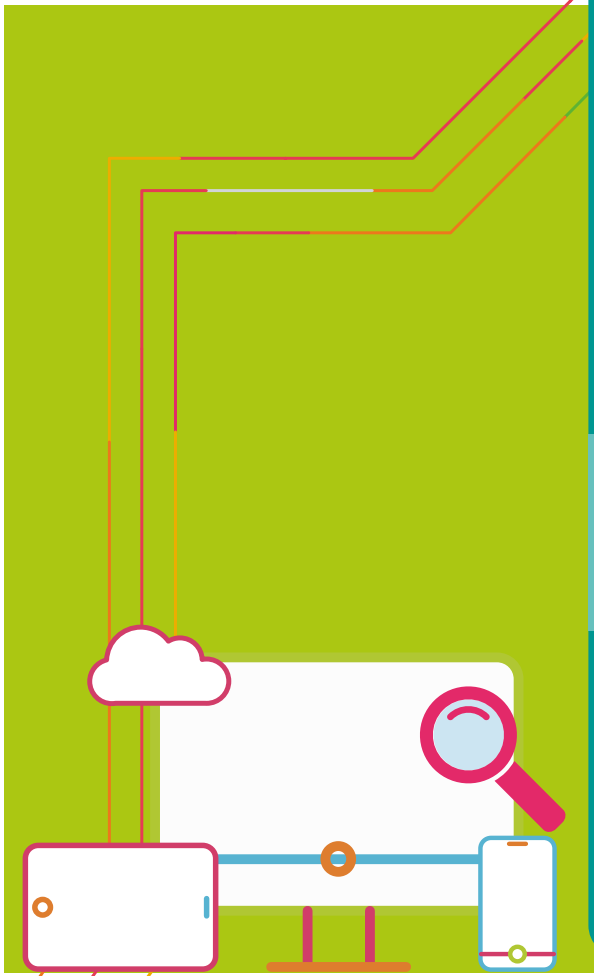
Grâce à notre plan par étapes, vous pouvez commencer dès maintenant !

Étape 1
identification et localisation

Étape 2
connaissance des délais de conservation

Étape 3
passage à l'action





Étape 1 : identification et localisation

Avant d'entamer le processus de nettoyage, il est important que vous réfléchissiez aux données à caractère personnel que vous conservez dans le cadre de votre travail et à l'emplacement où vous les conservez.

- **Identifiez les données à caractère personnel** que vous conservez. Il peut s'agir de données provenant de clients, de fournisseurs, de collègues, de candidats à un poste... Pensez aux données à caractère personnel évidentes, telles que les noms, les adresses e-mail et les numéros de téléphone, mais n'oubliez pas que les photos, les adresses IP... qui sont également considérées comme des données à caractère personnel. Selon le secteur dans lequel votre organisation opère, vous conservez peut-être aussi des données sensibles telles que des informations médicales.

  – Le **registre de traitement** des données à caractère personnel de votre organisation peut vous y aider. Il répertorie toutes les activités liées au traitement des données au sein de votre organisation. Ce document est obligatoire pour les entreprises de plus de 250 employés ou ayant un traitement à risque pour les personnes concernées.

- **Localisez l'endroit où vous conservez ces données à caractère personnel.** La plupart des organisations utilisent des systèmes de conservation des données hébergés **localement ou dans le cloud**. Pensez à l'espace disque central, au système CRM, à l'intranet, au wiki ou à toute autre plateforme de collaboration en ligne, etc. N'oubliez pas votre boîte e-mail professionnelle et pensez aux autres applications que vous utilisez dans le cadre de votre travail. Vous pouvez conserver vos données à caractère personnel **localement sur vos appareils** professionnels, par exemple sur votre ordinateur portable, votre smartphone, votre clé USB ou disque dur externe.

- Vérifiez si vous conservez également ces données à caractère personnel dans **d'autres systèmes ou appareils**. Vous arrive-t-il d'exporter des documents à partir d'une application ou de faire des copies de documents contenant des données à caractère personnel ? Où et comment conservez-vous vos sauvegardes ?

! **Évitez la duplication des données à caractère personnel**. Cela accroît en effet le risque d'incidents tels que l'accès non autorisé par des tiers.

- Renseignez-vous sur les règles de votre organisation pour savoir ce qui est autorisé en matière de duplication des données à caractère personnel (politique de conservation des données à caractère personnel, politique Bring Your Own Device, ...).
- Les données dupliquées pour des raisons de facilité d'utilisation doivent être supprimées immédiatement après leur utilisation, car la période de conservation ne concerne que le fichier original.

  – Exemple : Un collaborateur exporte les adresses e-mail de clients à partir du système central de gestion de la relation client (CRM) vers un fichier Excel, pour ensuite télécharger cette liste dans un programme d'e-mail marketing. Une fois cette action terminée, il doit supprimer la liste exportée.

- Vérifiez également si vous conservez des données à caractère personnel à usage professionnel sur vos **appareils personnels autorisés pour un usage professionnel**. Vous devez également effectuer un nettoyage des données sur ces appareils !

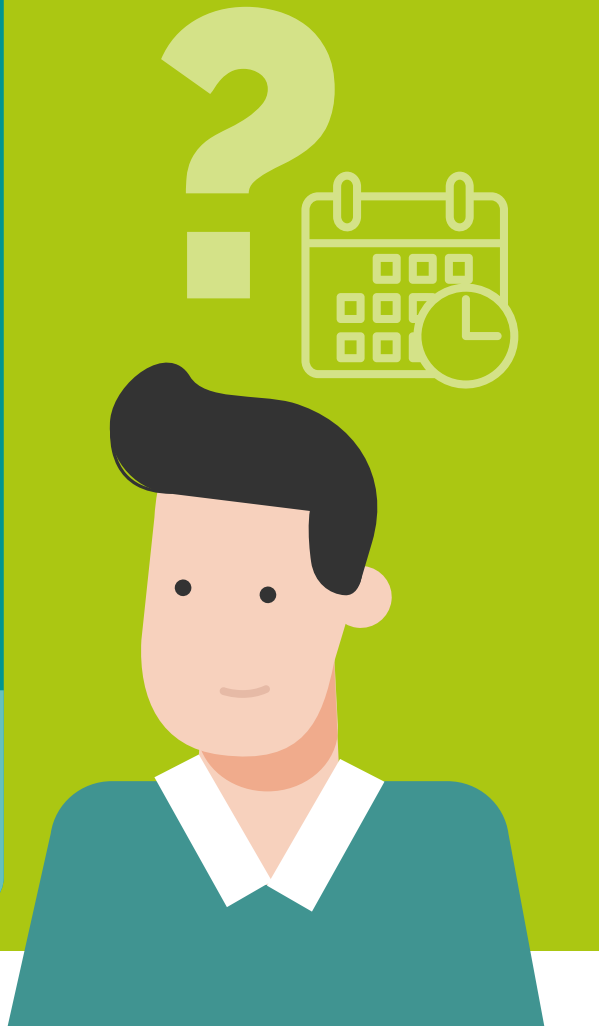
Étape 2 : connaissance des délais de conservation

Maintenant que vous avez identifié les données à caractère personnel que vous avez conservées, il est important de savoir combien de temps vous pouvez les conserver. En règle générale, vous ne pouvez conserver des données à caractère personnel que pour une durée strictement nécessaire. Mais quelle est cette durée ? Certains délais de conservation ont été fixés par la loi, d'autres par votre organisation. Dès que vous connaîtrez les délais de conservation en vigueur, vous saurez quelles données à caractère personnel vous pourrez définitivement supprimer au cours de l'étape suivante.

Délais de conservation au sein de votre organisation ou entreprise
Renseignez-vous sur les délais de conservation fixés par votre organisation pour tout traitement de données à caractère personnel.

- Chaque opération de traitement a une durée déterminée ou doit au moins répondre à certains critères qui déterminent quand l'objectif a été atteint.
- Les organisations doivent régulièrement revoir leurs délais de conservation. La fin d'une période de conservation des données peut être provoquée par certains événements.

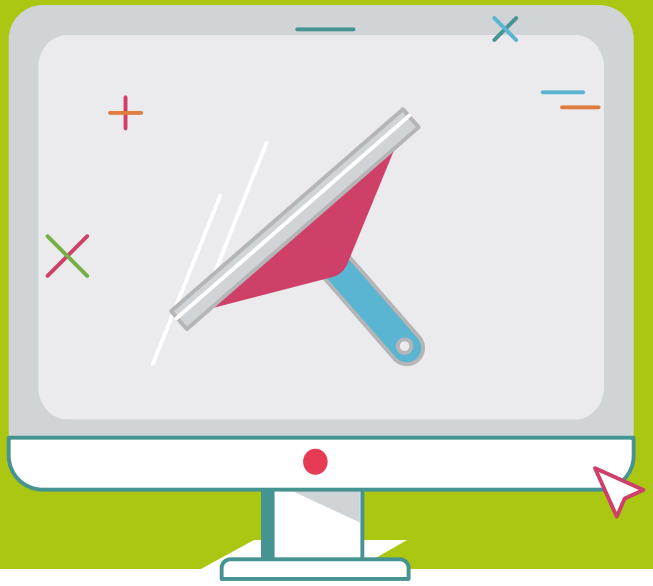
  – Exemple : une organisation doit supprimer les données à caractère personnel d'un candidat dès qu'il apparaît clairement que cette personne ne sera pas engagée. Si l'organisation souhaite toutefois conserver le CV du candidat, par exemple pour créer une réserve de recrutement, elle doit en informer le candidat et lui donner la possibilité de s'y opposer.



- Certains délais de conservation sont basés sur des obligations légales et ont été fixés par **la législation belge**.

Où puis-je trouver ces informations ?
Les informations relatives aux délais de conservation fixés par votre organisation figurent dans la **déclaration de confidentialité ou dans le règlement de protection des données à caractère personnel de votre organisation.** Veuillez contacter le responsable du traitement des données ou le DPO (Data Protection Officer) de votre organisation pour obtenir des explications à ce sujet.

N'oubliez pas !
- Si vous n'avez pas d'obligation légale, veuillez conserver **uniquement les données à caractère personnel qui sont réellement nécessaires à l'accomplissement de votre travail** et vous assurer que cette tâche s'inscrit dans le cadre des finalités définies. En cas de doute, demandez conseil au (à la) responsable du traitement/DPO de votre organisation.
- Ne conservez pas de copies inutiles de données à caractère personnel.



Étape 3 : passage à l'action

Maintenant que vous connaissez les délais de conservation des données, vous pouvez vous y mettre. Au cours de cette étape, vous allez supprimer ou conserver en toute sécurité les données à caractère personnel.

Supprimez toutes les données à caractère personnel dont la durée de conservation a expiré, ou qui ne sont plus nécessaires à l'exécution de votre travail.

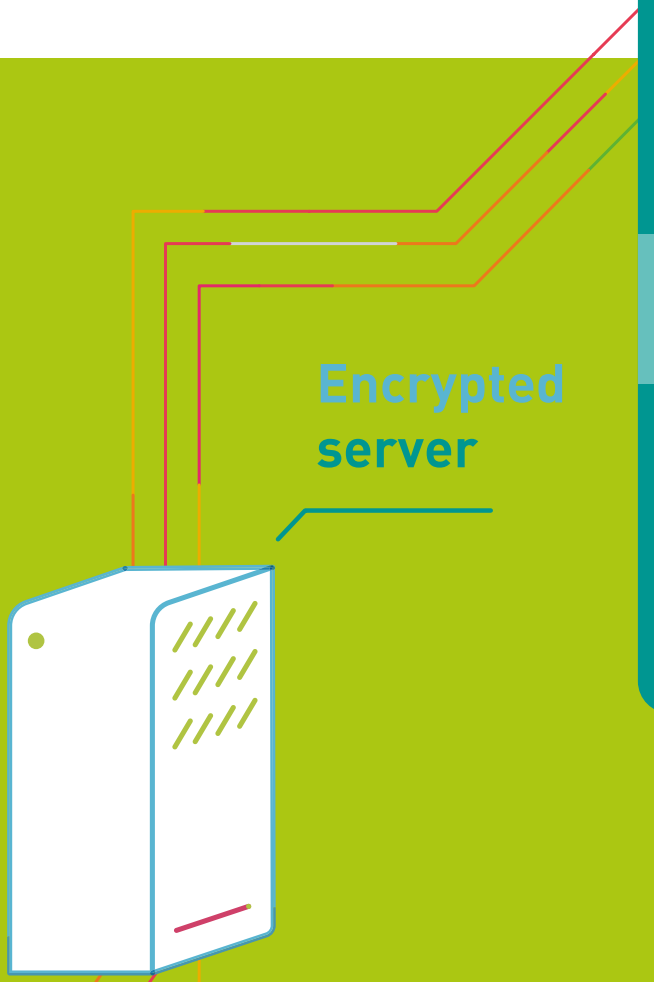
- Si votre organisation dispose de systèmes informatiques centralisés, votre département informatique a peut-être déjà mis en œuvre des **tâches d'archivage et/ou de suppression automatique** afin de respecter les délais de conservation.

  – Exemple : les images vidéo peuvent être conservées pour une durée de un mois maximum. Le système reconnait automatiquement les dates et supprime les images de plus d'un mois.

- Si les systèmes que vous utilisez ne permettent pas la suppression automatique, vérifiez s'il existe une **procédure manuelle** que vous pouvez appliquer régulièrement.
- Veillez à ce que les **données à caractère personnel dupliquées** soient supprimées, sauf si elles doivent faire office de sauvegarde pour l'organisation.
- N'oubliez pas de supprimer également les données à caractère personnel conservées sur vos **appareils personnels**.

Dans certains cas spécifiques, vous pouvez archiver des données à caractère personnel.

- Dans certains cas, vous pouvez encore avoir besoin de conserver certaines données à caractère personnel, même si vous n'en avez plus besoin pour effectuer votre travail. Songez par exemple aux données qui pourraient s'avérer nécessaires en cas de plainte (procédure judiciaire) ou de justification comptable. **Veillez à archiver ces données à caractère personnel en toute sécurité et à restreindre spécifiquement leur accès**. En cas de doute, demandez conseil au DPO de votre organisation.



Conservez les données à caractère personnel qui sont encore nécessaires de manière sécurisée.

- Tout d'abord, **l'accès aux données à caractère personnel doit être limité** aux personnes qui ont besoin de ces données dans le cadre de leur travail.
  - Exemple : rendre les contrats de travail uniquement accessibles au département des ressources humaines en les conservant à un endroit spécifique, protégé.
- Pour empêcher les personnes non autorisées d'accéder à vos appareils ou outils en cas de perte/vol, vous devez restreindre l'accès à vos appareils ou outils. Notamment grâce à l'utilisation d'un **mot de passe sûr** (élaboré).
- Si vous souhaitez conserver ces données au-delà de la période de conservation nécessaire, par exemple à des fins statistiques ou de test, il est nécessaire de les **anonymiser**.

Conseils pratiques

Le nettoyage des données à caractère personnel nécessite du temps et des efforts. Voici encore quelques conseils utiles :

- **Procédez de manière systématique et régulière.** Suivez le plan en trois étapes et prévoyez suffisamment de temps pour chaque étape.
- **Collaborez avec vos collègues**. Si vous travaillez dans une grande entreprise, vous pouvez également organiser le nettoyage des données avec les collègues de votre département.
- **Commencez par un appareil ou outil**. Par exemple, commencez à nettoyer votre boîte à e-mails professionnelle.
- **Nettoyez également vos appareils personnels**. Par exemple, si vous utilisez votre smartphone personnel à des fins professionnelles, supprimez les anciennes photos professionnelles et les données à caractère personnel que vous avez partagées sur les applications de messagerie, etc.
- **Utilisez des mots de passe sûrs**. Protégez les données à caractère personnel dont vous avez encore besoin à l'aide de mots de passe sûrs.
- **Évitez d'utiliser des clés USB ou disques durs externes pour conserver des données à caractère personnel**. Si vous en utilisez toutefois, assurez-vous toujours que les données sont cryptées.
- **Si vos appareils professionnels contiennent également des fichiers à caractère privé**, vous devez effectuer vous-même (et dans votre propre intérêt) un nettoyage des données, par exemple dans « Mes documents » ou « Mes images », surtout si vous y conservez des données sensibles.

Liste de sites Web intéressants

autoriteprotectiondonnees.be

edpb.europa.eu

Safeonweb.be

CYBER SECURITY
COALITION.be

www.cybersecuritycoalition.be

Cette brochure a été réalisée grâce à la coopération de Belnet, de la STIB, du Conseil Supérieur des Indépendants et des PME et d'AG Insurance.