

Prêts pour la RGPD ?

Depuis le **25 mai 2018**, le règlement européen n° 2016/679 s'applique à toutes les entreprises européennes.

La **responsabilité des entreprises** s'en trouve renforcée : elles doivent assurer une **protection optimale des données** à chaque instant et être en mesure de la démontrer.

D'importantes **amendes administratives** sont prévues selon la catégorie de l'infraction : **de 2 à 4% du chiffre d'affaires** de l'exercice précédent (RGPD, art. 83).

Que dit la CNIL ?

Guide de la sécurité des données personnelles
Pour aider les professionnels dans la mise en conformité à la loi Informatique et Liberté et au règlement général sur la protection des données, ce guide rappelle les précautions élémentaires qui devraient être mises en œuvre de façon systématique (<https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles>)

5. Sécuriser les postes de travail

(<https://www.cnil.fr/fr/securite-securiser-les-postes-de-travail>)

Prévenir les accès frauduleux, l'exécution de virus

.../... Favoriser le stockage des données des utilisateurs sur un espace de stockage régulièrement sauvegardé accessible via le réseau de l'organisme plutôt que sur les postes de travail .../..., fournir des moyens de synchronisation ou de sauvegarde aux utilisateurs

7. Protéger le réseau informatique interne

(<https://www.cnil.fr/fr/securite-protoger-le-reseau-informatique-interne>)

Limiter les accès Internet en bloquant les services non nécessaires .../... Imposer un VPN pour l'accès à distance .../... Limiter les flux réseau au strict nécessaire en filtrant les flux entrants/sortants sur les équipements

10. Sauvegarder et prévoir la continuité d'activité

(<https://www.cnil.fr/fr/securite-sauvegarder-et-prevoir-la-continuite-dactivite>)

Effectuer des sauvegardes fréquentes des données .../... Stocker les sauvegardes sur un site extérieur.

Que fait ResoSafe pour vous ?

ResoSafe vous propose **Box2Cloud**, son outil de sécurité informatique adapté à la mise en conformité avec RGPD.



• **Véritable serveur de données, Box2Cloud** comprend des paramétrages de sécurité permettant la création de groupes de travail, d'utilisateurs et d'administrateurs.

Complétez votre sécurité informatique avec nos **antivirus** pour postes de travail et serveurs, l'**hébergement des e-mails** dans le Cloud sécurisé et l'**antispam** pour protéger vos boîtes aux lettres des e-mails indésirables ou dangereux.

• **Avec ses options de sécurité** FireWall-Wifi, **VPNClient**, et Filtrage Web, **Box2Cloud** empêche l'accès à des tiers non autorisés à votre réseau local et préserve l'intégrité de vos données. Vos accès VPN vous permettent de travailler de chez vous ou au cours de vos déplacements avec un accès sécurisé à l'aide d'une simple connexion Internet.

• **Sécurisez vos données** avec **Sync2Box**, l'application de copie synchrone de votre poste de travail ou de votre serveur vers **Box2Cloud** et **Sync2Cloud** une véritable sauvegarde cryptée en AES 256 bits, versionnée et stockée dans des Data Center situés en France.

Les utilisateurs des produits ResoSafe ne sont pas exonérés de leurs obligations administratives et documentaires vis-à-vis de la loi Informatique et Liberté et du règlement européen des données personnelles

RGPD : par où commencer

Les 4 actions principales à mener pour entamer votre mise en conformité aux règles de protection des données. Ces actions doivent perdurer dans le temps pour être efficaces.

RGPD

PASSER À L'ACTION

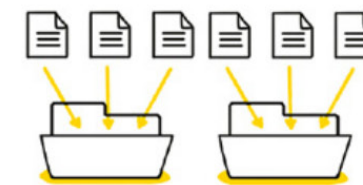
en 4 étapes

1



Constituez un registre de vos traitements de données

2



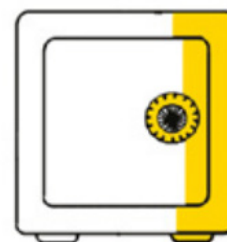
Faites le tri dans vos données

3



Respectez les droits des personnes

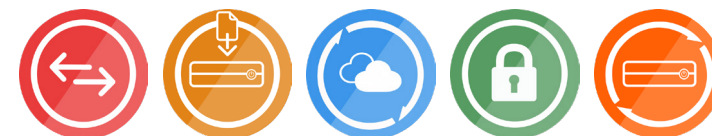
4



Sécurisez vos données

- Synchronisations et sauvegardes
- Partages internes et externes
- Accès à distance sécurisés
- Mobilité
- Numérisation

Pour cette étape, **Box2Cloud** répond à vos besoins de mise en conformité RGPD



1 Constituez un registre de vos traitements de données

Ce document vous permet de recenser tous vos fichiers et d'avoir une vision d'ensemble.

Identifiez les activités principales de votre entreprise qui nécessitent la collecte et le traitement des données.

Exemples : recrutement, gestion de la paye, formation, gestion des badges et des accès, statistiques gestion des clients prospects, etc.



Appuyez-vous sur **le modèle de registre**.

Dans votre registre, créez une fiche pour chaque activité recensée, en précisant :

- **L'objectif poursuivi** (la finalité - exemple : la fidélisation client) ;
- **Les catégories de données utilisées** (exemple pour la paie : nom, prénom, date de naissance, salaire, etc.) ;
- **Qui a accès aux données** (le destinataire - exemple : service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs) ;
- **La durée de conservation de ces données** (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive).

Le registre est placé sous la responsabilité du dirigeant de l'entreprise.

En constituant votre registre, vous aurez une vision d'ensemble sur vos traitements de données.



2 Faites le tri dans vos données

La constitution du registre vous permet de vous interroger sur les données dont votre entreprise a réellement besoin.

Pour chaque fiche de registre créée, vérifiez que :

- les données que vous traitez sont nécessaires à vos activités (par exemple, il n'est pas utile de savoir si vos salariés ont des enfants, si vous n'offrez aucun service ou rémunération attachée à cette caractéristique) ;
- vous ne traitez aucune donnée dite « sensible » ou, si c'est le cas, que vous avez bien le droit de les traiter (voir la fiche « Traitements de données à risque : êtes-vous concerné ? ») ;
- seules les personnes habilitées ont accès aux données dont elles ont besoin ;
- vous ne conservez pas vos données au-delà de ce qui est nécessaire.

3 Respectez les droits des personnes

Le RGPD renforce l'obligation d'information et de transparence à l'égard des personnes dont vous traitez les données (clients, collaborateurs, etc.).

Informez les personnes

A chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information.

Vérifiez que l'information comporte les éléments suivants :

- pourquoi vous collectez les données (« la finalité » ; par exemple pour gérer l'achat en ligne du consommateur) ;
- ce qui vous autorise à traiter ces données (le « fondement juridique » : il peut s'agir du consentement de la personne concernée, de l'exécution d'un contrat, du respect d'une obligation légale qui s'impose à vous, de votre « intérêt légitime ») ;
- Qui a accès aux données (indiquez des catégories : les services internes compétents, un prestataire, etc.) ;
- Combien de temps vous les conservez (exemple : « 5 ans après la fin de la relation contractuelle ») ;
- Les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (via leur espace personnel sur votre site internet, par un message sur une adresse email dédiée, par un courrier postal à un service identifié) ;
- Si vous transférez des données hors de l'UE (précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données).

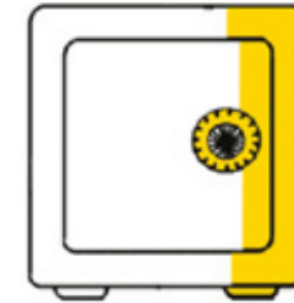


4 Sécurisez vos données

Si le risque zéro n'existe pas en informatique, vous devez prendre les mesures nécessaires pour garantir au mieux la sécurité des données. Vous êtes en effet tenu à une obligation légale d'assurer la sécurité des données personnelles que vous détenez.

Vous garantisiez ainsi l'intégrité de votre patrimoine de données en minimisant les risques de pertes de données ou de piratage.

Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas de d'incident.



Les failles de sécurité ont également des conséquences pour ceux qui vous ont confié des données personnelles : Ayez à l'esprit les conséquences pour les personnes de la perte, la divulgation, la modification non souhaitée de leurs données, et prenez les mesures nécessaires pour minimiser ces risques.

“ **Exemple** : vous êtes restaurateur et vous livrez à domicile. Vos clients vous communiquent leur adresse précise et le code d'entrée de leur immeuble. Si ces informations sont piratées ou perdues, elles peuvent être utilisées pour s'introduire frauduleusement au domicile de votre client. Conséquence désastreuse pour vos clients, mais aussi pour vous ! ”

BONNE PRATIQUE

Pour évaluer le niveau de sécurité des données personnelles dans votre entreprise, voici quelques questions à se poser :

- Les comptes utilisateurs internes et externes sont-ils protégés par des mots de passe d'une complexité suffisante ?
- Les accès aux locaux sont-ils sécurisés ?
- Des profils distincts sont-ils créés selon les besoins des utilisateurs pour accéder aux données ?
- Avez-vous mis en place une procédure de sauvegarde et de récupération des données en cas d'incident ?

Signalez à la CNIL les violations de données personnelles

Votre entreprise a subi une violation de données (des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées ou vous avez constaté un accès non autorisé à des données) ?

Vous devez **la signaler à la CNIL** dans les 72 heures si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées. Cette notification s'effectue en ligne sur le site internet de la CNIL.