PROTECTION DES DONNÉES PERSONNELLES : RISQUES ENCOURUS ET ASSURANCE

TPE, PME, collectivités territoriales : vous êtes concernées par le RGPD !

Fédération Française de l'Assurance

01 DONNÉES PERSONNELLES ET RGPD : NOTIONS CLÉS

02 VIOLATION DES DONNÉES PERSONNELLES : VOTRE RESPONSABILITÉ

03 PROTECTION DES DONNÉES PERSONNELLES : PRÉVENTION ET ASSURANCE

Les TPE-PME et collectivités territoriales face aux risques d'atteinte aux données personnelles

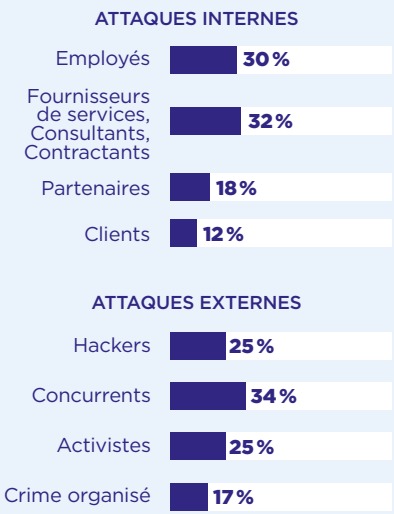
Les cyber attaques en France en 2017

79%
des entreprises ont déclaré au moins 1 attaque

77%
des attaques concernent des PME

Source Baromètre CESIN / Opinion Way janvier 2018

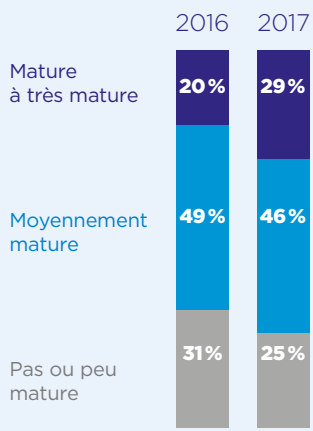
Origine des attaques



Source: PwC, Enquête Global State of Information Security Survey (GSISS) 2017. Un répondant peut citer plusieurs sources d'incidents.

Maturité numérique

La maturité numérique des collectivités locales progresse



Source: MARKESS - Observatoire des compétences et de la maturité numérique des collectivités locales - 2017: http://blog.markess.com

01

DONNÉES PERSONNELLES ET RGPD : **NOTIONS CLÉS**

NOTIONS CLÉS

Une donnée personnelle, c'est quoi ?

> Toute information se rapportant à une personne physique identifiée ou identifiable est une donnée personnelle.

Une personne peut être identifiée :

- **directement :** par exemple par son nom et son prénom
- **indirectement :** par un identifiant (n° de client, n° de téléphone), une donnée biométrique (caractéristique physique ou biologique comme l'ADN, le contour de la main, les empreintes digitales...), des éléments spécifiques à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image…

Source : MEDEF, "Guide pratique sur la protection des données personnelles"

NOTIONS CLÉS

En quoi consiste le traitement des données personnelles ?

On entend par traitement toute opération ou tout ensemble d'opérations automatisées ou non, appliqué à des données personnelles, quel que soit le procédé utilisé, notamment :

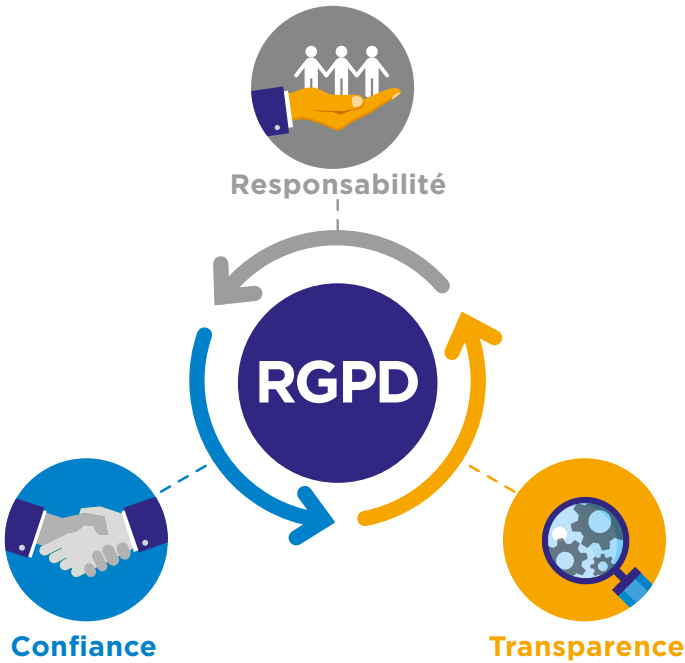
- Collecte
- Enregistrement
- Organisation
- Conservation
- Adaptation
- Modification
- Extraction
- Consultation
- Utilisation
- Communication par transmission, diffusion ou toute forme de mise à disposition

Un traitement de données personnelles n'est pas nécessairement informatisé et concerne aussi les fichiers papier.

Source : MEDEF, "Guide pratique sur la protection des données personnelles"

NOTIONS CLÉS

Qu'est-ce que le RGPD ?



Au 25 mai 2018 est entré en vigueur le Règlement Général sur la Protection des Données (RGPD) qui harmonise au niveau européen la réglementation sur la protection des données personnelles.

Objectif du RGPD
Le RGPD a pour objectif la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel.

Conséquences du RGPD pour votre activité
Le règlement place les organismes (entreprises, collectivités territoriales…) dans une logique de responsabilisation dans le traitement des données personnelles.

Source : CNIL, "Guide pratique de sensibilisation au RGPD"

NOTIONS CLÉS

Etes-vous concernés par le RGPD ?

Le RGPD concerne tous les organismes, tant publics que privés (associations, collectivités territoriales...) et toutes les entreprises, quels que soient leur taille et leur secteur d'activité.

Si je dispose de données personnelles

On entend par donnée personnelle, toute information permettant d'identifier directement ou indirectement une personne physique

+

si je traite ces données personnelles

On entend par traitement, toute opération sur des données personnelles (collecte, stockage, conservation, utilisation…) y compris les fichiers papier qui sont organisés ou classés

dans le cadre d'une activité professionnelle

+

Si le traitement a lieu sur le territoire de l'UE

OU

Si le responsable du traitement ou le sous-traitant sont établis sur le territoire de l'UE

OU

Si les personnes concernées par le traitement sont situées sur le territoire de l'UE pour les activités d'offre de biens ou de services et de suivi du comportement des personnes

ALORS LE RGPD S'APPLIQUE

Source : MEDEF, "Guide pratique sur la protection des données personnelles"

NOTIONS CLÉS

Quelles sont vos obligations au titre du RGPD ?

Vous devez mettre en place une organisation adaptée à la taille de votre entreprise et à la sensibilité des données personnelles traitées. Vous devez notamment :

Mettre en place une gouvernance et désigner un Délégué à la Protection des données personnelles (DPO), le cas échéant.

Bon à savoir : *Si votre entreprise n'est pas soumise à l'obligation de nommer un DPO, il est recommandé de désigner une personne pilote pour mener le plan de conformité au RGPD.*

Tenir une documentation permettant de démontrer la conformité au RGPD.

Depuis le 25 mai 2018, votre entreprise est soumise à une obligation de sécurité afin de garantir un niveau de sécurité adapté au risque de traitement.

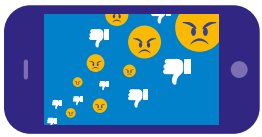
Protéger les données par la mise en œuvre de mesures techniques et organisationnelles.

Prendre en compte les enjeux liés à la protection des données dès la phase de conception du produit ou du service et par défaut *(Privacy by design /Privacy by default)*.

Notifier les violations de données auprès de la CNIL, voire auprès de la personne concernée par la violation de ces données, en cas de risque élevé pour ses droits et libertés.

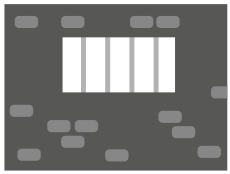
NOTIONS CLÉS

Quels sont les risques encourus en cas de violation du RGPD ?



Atteinte à l'image
et à la réputation
de votre entreprise

Amende administrative en cas d'action de la CNIL ou d'une autorité administrative. Le risque d'une sanction financière peut aller jusqu'à 4% de votre chiffre d'affaires annuel global, ou 20 millions d'euros



Sanctions pénales
Amendes pénales
jusqu'à 300 000 € et
peine d'emprisonnement
jusqu'à 5 ans

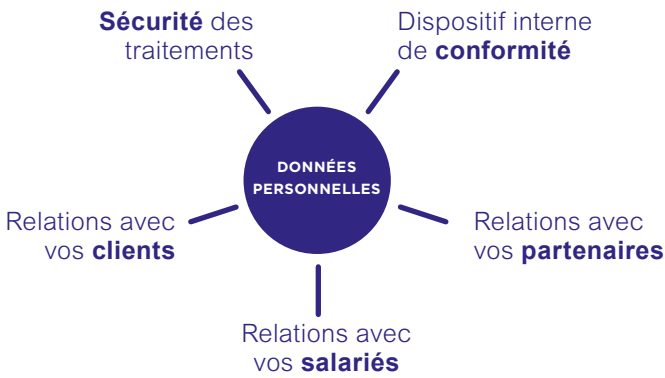
Frais de notification
de la violation des données
personnelles à la CNIL, voire
aux personnes concernées

Responsabilité civile
de l'entreprise en cas de
dommages causés du fait
de la violation des données
personnelles

NOTIONS CLÉS

Enjeux de la protection des données personnelles pour votre activité

Les données personnelles sont au cœur de votre activité :



RGPD : LES 6 AVANTAGES POUR VOTRE ENTREPRISE

1. **Renforcer la confiance**
2. **Améliorer votre efficacité commerciale**
3. **Mieux gérer votre entreprise**
4. **Améliorer la sécurité des données de votre entreprise**
5. **Rassurer vos clients et donneurs d'ordre et ainsi développer votre activité**
6. **Créer de nouveaux services**

Source : CNIL, "Guide pratique de sensibilisation au RGPD"

02

VIOLATION DES DONNÉES PERSONNELLES : **VOTRE RESPONSABILITÉ**

VOTRE RESPONSABILITÉ

Votre responsabilité civile peut être engagée

En cas de violation des données personnelles lors de leur traitement, la responsabilité civile de votre entreprise peut être engagée.

Qui peut engager la responsabilité civile de votre entreprise ?

Toute personne ayant subi un dommage du fait d'une atteinte à ses données personnelles peut engager votre responsabilité civile. Il peut s'agir de vos salariés, clients, administrés, adhérents…

Quand ?

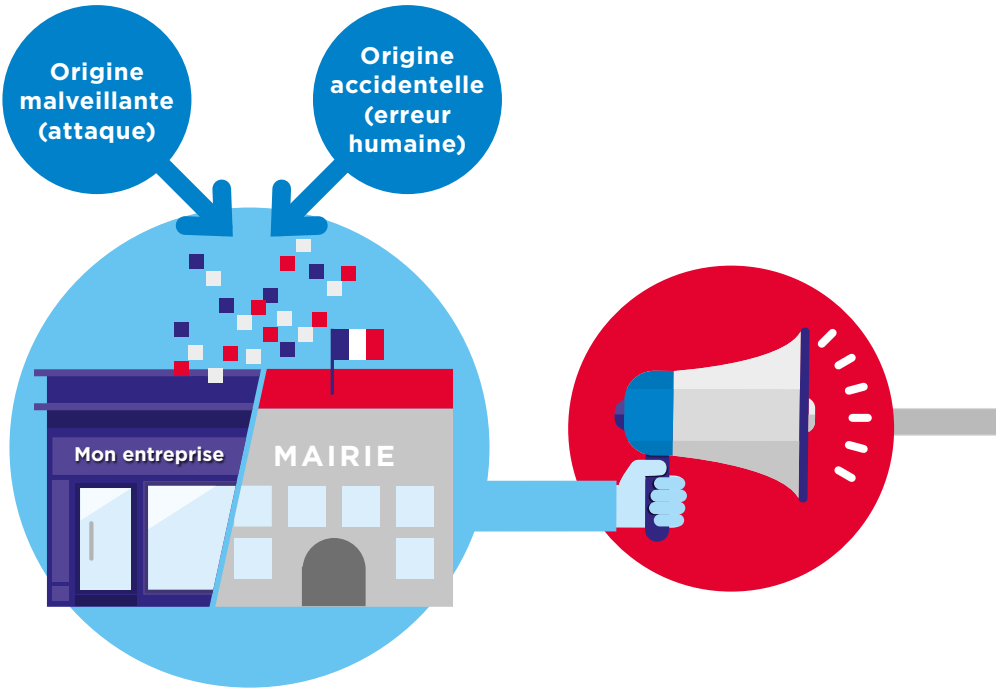
En cas de « violation de leurs données personnelles », c'est-à-dire de « faille de sécurité » entraînant la destruction, la perte, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement.

L'origine peut être :

- Accidentelle : par exemple divulgation par erreur par un salarié de données, etc.
- Illicite ou malveillante en cas notamment de cyber-attaque ou de comportement mal intentionné.

VOTRE RESPONSABILITÉ

Que faire en cas de violation des données personnelles ?

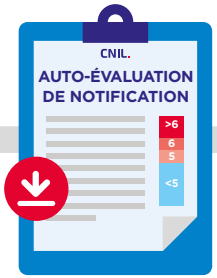


Entreprise ou collectivité, que vous soyez victime d'une attaque malveillante ou d'un accident (erreur, omission) à l'origine d'une atteinte aux données personnelles que vous traitez…

…VOUS AVEZ UNE OBLIGATION DE NOTIFICATION

Commission Nationale Informatique et Libertés (CNIL)

Vous devez informer dans les meilleurs délais l'autorité compétente, la CNIL, en cas de risques pour les droits et libertés des personnes, en utilisant le formulaire téléchargeable sur le site www.cnil.fr.

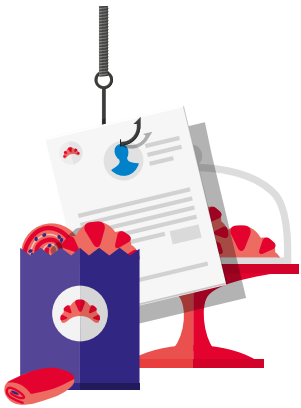


Vous devez aussi informer toute personne concernée de la violation de ses données, en cas de risque élevé pour ses droits. Vous pouvez utiliser l'outil d'auto-évaluation de la CNIL pour estimer si vous êtes tenus de notifier les personnes ou non.

La notification doit être adressée à la personne par tout moyen permettant d'apporter la preuve de l'accomplissement de cette notification (LRAR par voie postale ou courrier électronique, etc.)

VOTRE RESPONSABILITÉ

Exemples de mise en jeu possible de de l'entreprise ou de la collectivité



PME, fabricant de viennoiseries

Des hackers ont lancé une attaque dite de hameçonnage. Un salarié, leurré par un message frauduleux, a permis le vol de données personnelles et confidentielles des salariés de l'entreprise : des données relatives aux salaires.

ORIGINE DE LA VIOLATION

Attaque malveillante
Hameçonnage + erreur humaine

DOMMAGES CONSÉCUTIFS

Atteintes aux données personnelles des salariés de l'entreprise.
Divulgation des données personnelles des salariés comme le salaire

CONSÉQUENCES PÉCUNIAIRES

- Frais de notification de l'atteinte aux salariés
- Préjudice moral subi par les salariés
- Amende administrative et/ou pénale
- Frais de défense
- Impact sur les relations sociales

Éditeurs de logiciels

Le responsable des systèmes d'information d'une société dans l'édition de logiciels et l'infogérance, faisant l'objet d'un licenciement, s'est introduit dans le système informatique de la société et a reformaté les disques durs.
Cette attaque a engendré une perte massive de données dont des données personnelles des clients

ORIGINE DE LA VIOLATION

Malveillance d'un salarié suite à une faille de sécurité

DOMMAGES CONSÉCUTIFS

Les victimes sont des clients de l'entreprise dont les données personnelles ont été volées (exemple : coordonnées bancaires)

CONSÉQUENCES PÉCUNIAIRES

- Frais de notification aux clients concernés
- Atteinte à la réputation de l'entreprise
- Préjudice moral des clients
- Préjudice financier des clients
- Amende pénale et/ou administrative
- Frais de défense

la responsabilité

La mise en jeu de votre responsabilité en cas de violation de données personnelles a de lourdes conséquences financières pour votre entreprise ou votre collectivité

Fleuriste, pratiquant la vente en ligne

Un hacker s'est introduit dans le système informatique d'une TPE et a réussi à modifier l'un des fichiers exécutés lors de la connexion au compte client.
Cette modification a permis au hacker de recevoir le nom d'utilisation (adresse email) et le mot de passe des clients de l'entreprise.

ORIGINE DE LA VIOLATION

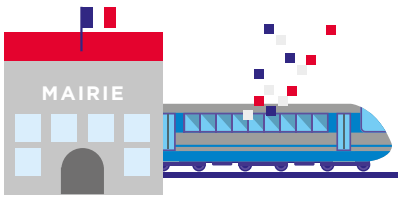
Attaque malveillante par un hacker
Intrusion suite à une faille de sécurité

DOMMAGES CONSÉCUTIFS

Les victimes sont les clients de l'entreprise dont les données personnelles ont été usurpées

CONSÉQUENCES PÉCUNIAIRES

- Frais de notification de l'atteinte aux clients impactés
- Préjudice moral des clients
- Pertes financières
- Atteinte à la réputation de l'entreprise
- Amende pénale et/ou administrative
- Frais de défense



Une collectivité territoriale

Un ordinateur portable, non protégé, oublié dans un train par un agent de la mairie a été dérobé.
Cet ordinateur contenait une base de données personnelles des habitants de la ville (registre d'état civil…)

ORIGINE DE LA VIOLATION

Erreur humaine : omission

DOMMAGES CONSÉCUTIFS

Les victimes sont les habitants de la commune
Atteinte à l'intégrité et la confidentialité des données du registre de l'état civil.

CONSÉQUENCES PÉCUNIAIRES

- Frais de notification
- Atteinte à la réputation de la collectivité territoriale
- Préjudice moral des habitants
- Amende administrative et/ou pénale
- Frais de défense

03

PROTECTION DES DONNÉES PERSONNELLES : **PRÉVENTION ET ASSURANCE**

Assurer la sécurité du traitement des données personnelles

Pour améliorer la connaissance sur les traitements de données personnelles, vous devez penser à :

CARTOGRAPHIE DES TRAITEMENTS

Recenser les traitements de données à caractère personnel, automatisés ou non

CARTOGRAPHIE DES RISQUES

Apprécier les risques engendrés par chaque traitement

- Accès illégitime
- Modification non désirée des données
- Disparition des données

Identifier les sources ou menaces de risques

- Sources humaines interne ou externe
- Source accidentelle ou malveillante
- Sources non humaines

LES QUESTIONS À SE POSER POUR CHAQUE TRAITEMENT DE DONNÉES PERSONNELLES

Qui ?

- **Identifiez les responsables des services opérationnels traitant les données.**
- **Établissez la liste de vos sous-traitants**

Quoi ?

- **Identifiez les catégories de données traitées**
- **Identifiez les données susceptibles de soulever des risques en raison de leur sensibilité (exemples : données relatives à la santé…)**

Pourquoi ?

- **Indiquez la ou les finalités pour lesquelles vous collectez ces données (exemple : gestion RH, relation commerciale…)**

Où ?

- **Déterminez les lieux où sont stockées les données**
- **Indiquez le pays vers lesquels les données sont éventuellement transférées**

Combien de temps ?

- **Indiquez le temps de conservation des données**

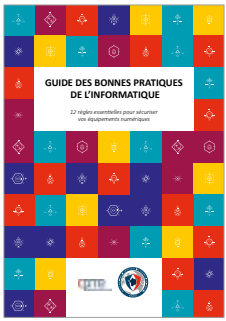
Comment ?

- **Précisez les mesures de sécurité mises en œuvre pour minimiser les risques (voir la cartographie des risques en page précédente)**

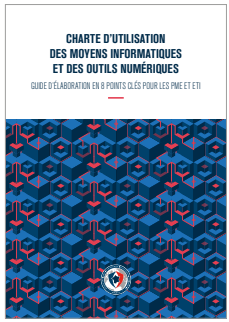
Source : CNIL, “Guide pratique de sensibilisation au RGPD”

Évaluer le niveau de sécurité et mettre en place des mesures de prévention

La prévention des incidents et des attaques informatiques relève souvent de réflexes simples qui concourent à une protection globale de l'entreprise.
Les outils suivants sont à votre disposition pour évaluer votre niveau de sécurité et mettre en œuvre des mesures de prévention adaptées.



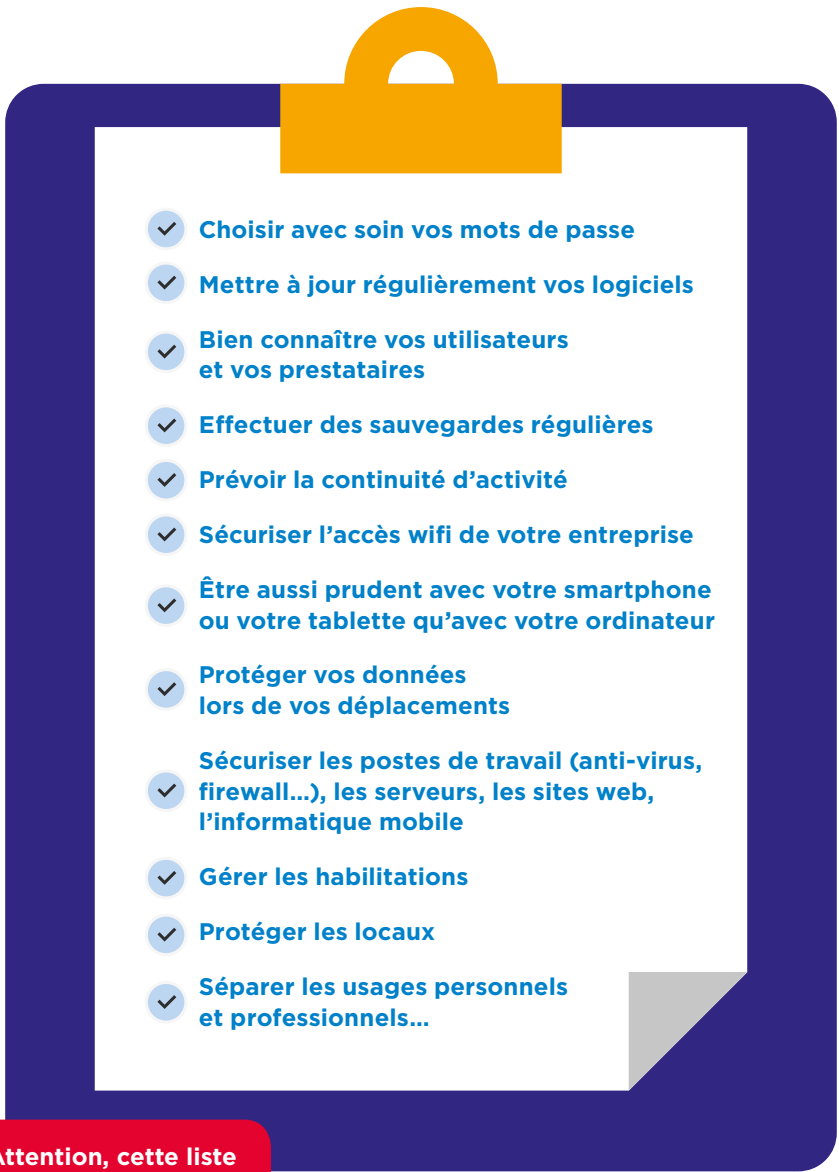
« Guide des bonnes pratiques de l'informatique »
Douze règles essentielles pour la sécurité des systèmes d'information des petites et moyennes entreprises.
—
CPME/ANSSI



« Charte d'utilisation des moyens informatiques et des outils numériques »
Huit points clés pour accompagner la transition numérique des entreprises face à l'augmentation croissante de la menace.
—
ANSSI

Cours en ligne de Cybersécurité pour tous
Mooc pour s'initier à la cybersécurité, approfondir ses connaissances et agir efficacement sur la protection de vos outils numérique.
—
ANSSI

AVEZ-VOUS NOTAMMENT PENSÉ À PRENDRE TOUTES LES MESURES NÉCESSAIRES ?



- Choisir avec soin vos mots de passe
- Mettre à jour régulièrement vos logiciels
- Bien connaître vos utilisateurs et vos prestataires
- Effectuer des sauvegardes régulières
- Prévoir la continuité d'activité
- Sécuriser l'accès wifi de votre entreprise
- Être aussi prudent avec votre smartphone ou votre tablette qu'avec votre ordinateur
- Protéger vos données lors de vos déplacements
- Sécuriser les postes de travail (anti-virus, firewall…), les serveurs, les sites web, l'informatique mobile
- Gérer les habilitations
- Protéger les locaux
- Séparer les usages personnels et professionnels…

Attention, cette liste n'est pas exhaustive !

Le sous-traitant, un maillon clé

Si vous faites appel à un sous-traitant chargé de gérer pour votre compte le traitement des données personnelles de votre entreprise, vous devez notamment :

- **Sélectionner votre sous-traitant** en choisissant un prestataire qui assure un niveau de protection suffisant aux données qui lui sont confiées.
- **Contractualiser votre relation** avec votre sous-traitant. C'est obligatoire !
- **Évaluer le niveau de risque** de votre sous-traitant.
- **Négocier les clauses** contractuelles adaptées au niveau de risque.
- **Prévoir un mécanisme de contrôle** et d'audit de votre sous-traitant.

L'une des nouveautés majeures du RGPD est d'imputer une part de responsabilité au sous-traitant en créant une co-responsabilité entre vous et lui en cas de violation des données personnelles. Vous pourrez, le cas échéant, exercer un recours à l'encontre de votre sous-traitant.

Le rôle de l'assurance

Face au risque de mise en jeu de votre responsabilité civile en cas de violation des données personnelles que vous traitez, votre assureur peut vous accompagner dans le cadre d'une garantie d'assurance CYBER.

Quels sont les frais généralement assurables ?

- **Frais de notification** à la CNIL et aux personne concernées suite à une violation des données personnelles
- **Frais de gestion de crise comme :**
  - Frais de communication
  - Frais de préservation de la réputation et de l'image de l'entreprise
- **Conséquences pécuniaires de votre responsabilité civile :** dommages corporels, matériels et immatériel (perte financière) et le préjudice moral du fait de la violation des données personnelles
- **Frais de défense – Conseil juridique**
- **Prise en charge de prestations de services :**
  - Frais d'expertise et d'assistance informatique
  - Frais de mise en place d'une plateforme téléphonique
  - Frais de reconstitution des données en présence de sauvegardes informatiques disponibles et exploitables
  - Frais liés à la prestation de nettoyage

Quels sont les frais inassurables ?

- Les sanctions pénales
- Les conséquences de la collecte illicite de votre part, de données tiers ou de données personnelles ou confidentielles.

ACTIONS À MENER

Dès à présent :

- **Pensez à vérifier que vous avez bien souscrit une garantie d'assurance CYBER**
- **Vérifiez l'étendue et le montant de garantie de votre contrat (montant d'intervention maximum)**

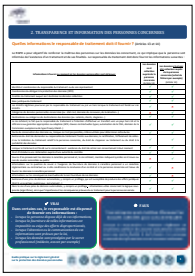
En cas d'incident ou d'acte de malveillance occasionnant une violation des données personnelles :

- **Contactez sans délai votre partenaire assureur, il saura vous conseiller et vous accompagner**
- **En tout état de cause, informez-le avant toute décision qui pourrait avoir un impact sur les conséquences de cet incident et sur la gestion de votre dossier de déclaration de sinistre**

POUR EN SAVOIR PLUS

Fédération Française des Assureurs
Guide pratique
« Anticiper et minimiser l'impact d'un cyber risque sur votre entreprise »

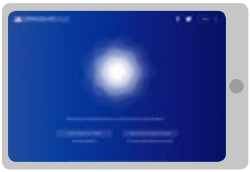
CNIL
Guide pratique de sensibilisation des entreprises au RPDG pour les TPE et PME



MEDEF
Guide pratique sur la Protection des Données personnelles

CPME / ANSSI
« Guide des bonnes pratiques de l'informatique »

CNIL
Guide du sous-traitant RGPD



Cybermalveillance.gouv.fr
Dispositif d'assistance aux victimes d'actes de cybermalveillance

➜ Des fiches réflexes par thématiques :
- Rançongiciel
- Le déni de service
- L'arnaque au faux support technique
- La défiguration

➜ Kit de sensibilisation à destination des collaborateurs

cyberveille-sante.gouv.fr
Fiches réflexes

Agence nationale de la Sécurité des systèmes d'information (ANSSI)
Cartographie du système d'information à l'usage de la sécurité numérique

06/2018 - Conception graphique : Vanessa Vansteelandt - Illustrations : Vansteelandt, Shutterstock

26, boulevard Haussmann
75311 Paris Cedex 09

Rue Montoyer 51
1000 Bruxelles

ffa-assurance.fr
@FFA_assurance