10 fiches pratiques pour mieux comprendre le risque numérique

Generali Protection Numérique

GENERALI

Le Règlement général sur la protection des données (RGPD)

Le Règlement Général sur la Protection des Données (RGPD) entrera en vigueur en mai 2018. Il a vocation à donner au citoyen plus de transparence sur l'usage qui est fait de ses données personnelles et l'assurance de leur protection. Mais le RGDP est également un gage de prévention contre le risque numérique pour l'entreprise.

En quoi consiste le RGPD ?

Le Règlement Général sur la Protection des Données (RGPD) du 27 avril 2016 sera applicable à compter du 25 mai 2018. Il renforce les droits des citoyens concernant l'usage que toutes les entreprises européennes (ou qui ont une activité en Europe) font de leurs données personnelles :

- **transparence :** droit de savoir à quoi servent ses données. Elles doivent être traitées de manière loyale et licite ;
- **droit à la portabilité :** les personnes peuvent réclamer qu'une entreprise lui restitue toutes les données qu'elle a récupérées sur elle ;
- **droit à l'effacement :** un individu peut exiger qu'une entreprise supprime de ses bases de données tous les fichiers la concernant ;
- **droit à réparation :** tout individu peut exiger réparation des dommages matériels ou moraux causés par une violation du Règlement.

Le renforcement de ces droits accentue par conséquent les obligations de toutes les entreprises qui collectent, traitent et stockent des données personnelles.

Aujourd'hui, de nombreuses sociétés ne protègent pas assez leur réseau informatique, par manque de moyens ou de prise de conscience des risques numériques. Résultat, **onze incidents de cybersécurité seraient comptabilisés chaque jour en milieu professionnel en France,** d'après le cabinet de conseil PwC.

Face aux menaces numériques (phishing, infiltration sur le réseau informatique, virus…) pouvant entraîner une fuite de données - non seulement celles de vos clients, mais aussi celles de votre entreprise - vous devez renforcer votre niveau de sécurité.

Les mesures élémentaires à mettre en place

Pour être en conformité avec le RGPD, différentes mesures doivent être prises :

- la réalisation d'une **cartographie exhaustive des supports internes** (serveurs, disques durs) **et externes** (Cloud, prestataires informatiques…) stockant les données personnelles ;
- la création d'un **registre des activités de traitement de toutes les données personnelles** récoltées. Il doit préciser la ou les finalités pour lesquelles ces informations sont collectées ou gérées : relation commerciale, gestion RH, vidéo surveillance, habitudes de consommation, géolocalisation de véhicules... mais également leur lieu d'hébergement, leur durée de conservation ou encore les mesures de sécurité dont elles font l'objet ;
- la nomination d'un **Délégué à la Protection des données.** C'est le responsable du traitement des données dans une entreprise.

À noter que cette nomination ainsi que la création d'un registre des activités de traitement des données sont deux mesures obligatoires pour les entreprises de plus de 250 salariés et pour toutes celles dont les activités nécessitent de traiter des données relatives à des secteurs sensibles (santé, données en lien avec les infractions et les condamnations pénales…).

- L'établissement d'une **liste exhaustive de tous les sous-traitants** enregistrant des informations à caractère personnel. La CNIL signale qu'ils sont tenus « de respecter des obligations spécifiques en matière de sécurité et de confidentialité (...). Ils ont notamment une obligation de conseil auprès du responsable de traitement pour la conformité à certaines obligations du règlement (failles, sécurité, destruction des données, contribution aux audits). »

- **La conservation des seules données personnelles nécessaires** à l'activité de l'entreprise. C'est le principe dit de « minimisation » du RGPD. Si l'on prend le cas d'une newsletter envoyée à des prospects ou à des clients, une entreprise ne doit garder qu'une seule donnée « nécessaire » : l'adresse e-mail. Éventuellement, un site de e-commerce peut enregistrer les dates de naissance pour tenir compte des anniversaires et proposer des offres spéciales à ses consommateurs. La durée de conservation doit par ailleurs être précisée et justifiée.
- La mise en place **de moyens d'identification et d'authentification des salariés.** Cela implique d'établir une politique de gestion des mots de passe et de limiter les accès aux dossiers sensibles aux seuls collaborateurs vraiment concernés.
- La mise en place d'une **politique de sauvegarde** assurant la restitution intègre des données.

D'un point de vue technique, les entreprises doivent s'appuyer notamment sur :

- des techniques de chiffrement des données personnelles ;
- l'authentification forte (certificat électronique, carte à puce…) afin de tracer les accès ;
- des procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. Cette mission incombe notamment à des sociétés spécialisées dans la sécurité informatique et qui peuvent être mandatées par votre assureur.

Ces principales mesures doivent être mises en place sous peine de sanctions de la CNIL en cas de contrôle ou après un piratage ayant eu un impact sur la sécurité des données personnelles. Le RGPD prévoit des amendes par paliers selon les fautes commises. Il précise que cette sanction peut atteindre jusqu'à 4 % du chiffre d'affaires annuel.

Ce qu'il ne faut pas faire

Envoyer des mailings sans le consentement explicite des citoyens n'est plus possible. Il faut qu'ils aient manifesté « de façon libre, spécifique, éclairée et univoque » leurs accords.

Par ailleurs, si une personne vous demande des précisions sur le traitement de ses données, il n'est pas possible de pratiquer la politique de l'autruche. Une réponse doit par principe être apportée dans les meilleurs délais et en tout état de cause dans le délai d'un mois à compter de la réception de la demande.

Pour aller plus loin

« Des mécanismes techniques et organisationnels garantissant la confidentialité et l'intégrité des données personnelles doivent être mis en œuvre pour éviter que leur consultation par des tiers non autorisés, des modifications ou encore leur perte porte préjudice aux personnes concernées », explique Sophie Nerbonne, Directrice de la conformité à la CNIL dans une interview publiée dans la Revue des Collectivités Locales (n° 485, en septembre 2017). Parmi ces solutions, il y a notamment un logiciel mis à disposition gratuitement par la CNIL. Il permet de réaliser soit même son analyse d'impact sur la protection des données.

LEXIQUE

Les données personnelles

Il s'agit d'informations permettant d'identifier, directement ou indirectement, une personne : nom, âge, lieu de naissance, numéro de Sécurité sociale… L'arrêt n° 1184 du 3 novembre 2016 de la Cour de cassation précise aussi que « les adresses IP (…) sont des données à caractère personnel, de sorte que leur collecte constitue un traitement de données à caractère personnel ».

Pour vous accompagner dans votre mise en conformité avec le RGPD, découvrez l'offre Generali Protection Numérique

https://www.generali.fr/professionnel/assurance-cyber-risques/

Generali IARD Société anonyme au capital de 94 630 300 euros. Entreprise régie par le Code des assurances - 552 062 663 RCS Paris
Siège social : 2 rue Pillet-Will - 75009 Paris

Informations non contractuelles à caractère publicitaire données à titre purement indicatif et dans un but pédagogique. La compagnie ne saurait être tenue responsable d'un préjudice d'aucune nature lié aux informations fournies. La contractualisation éventuelle avec le partenaire nommé ci-dessus se fait sous votre seule et unique responsabilité et ne saurait engager la responsabilité des sociétés Generali en France. Le choix de contractualiser ou pas avec ce partenaire relève de la gestion de votre entreprise et est sans incidence sur vos contrats d'assurance Generali qui demeure tiers à vos relations.

Sensibilisation des utilisateurs : la première pierre de votre sécurité numérique

Antivirus, pare-feu, sauvegarde…, il existe différentes solutions de sécurité informatique. Et si la meilleure des protections restait la formation des salariés ? En étant capables de déjouer les pièges des cybercriminels, ils assurent la pérennité de votre activité.

L'être humain est souvent présenté comme le maillon faible de la sécurité numérique en entreprise, l'e-mail se révélant être son principal talon d'Achille : « Près de 90 % des clics sur des URL malveillantes ont lieu dans un délai de 24 heures après la remise de l'e-mail. 25 % de ces clics se produisent en seulement 10 minutes et près de 50 % en une heure ». Tirées du rapport annuel « Le facteur humain 2017 » de Proofpoint , une société spécialisée dans la sécurité informatique, ces statistiques témoignent du manque de vigilance des salariés et ainsi de l'importance de leur sensibilisation aux bonnes pratiques.

Quels sont les principaux risques ?

Le plus répandu actuellement est le **ransomware**. Il s'agit d'un virus caché dans une pièce jointe. Dès qu'on l'ouvre, il va chiffrer (ou crypter) tous les documents enregistrés sur le disque dur de l'ordinateur de l'utilisateur, mais aussi tous ceux qui sont partagés avec les autres collaborateurs via le serveur. En quelques secondes, l'activité de l'entreprise est au point mort.

L'autre menace est le **phishing** : un e-mail usurpant l'identité d'une banque ou d'un opérateur télécom vous demande de redonner vos identifiants sous différents prétextes. Les PME sont également ciblées avec de faux courriers d'une administration (impôt, URSSAF…) exigeant un virement pour effectuer une procédure quelconque.

Les cybercriminels profitent aussi de l'actualité professionnelle et notamment de l'instauration du RGPD. Fin novembre 2017, la Commission nationale de l'informatique et des libertés (CNIL) a ainsi publié une alerte sur de fausses mises en demeure administratives envoyées par fax et par téléphone à des entreprises. Comme pour le phishing, ce message insiste sur les sanctions financières encourues si les PME ne répondent pas très rapidement.

Face à ces différentes menaces, les outils de sécurité ne peuvent garantir une protection à 100 %. La cybersécurité n'est pas uniquement une affaire de logiciels ; elle repose aussi et avant tout sur la **sensibilisation des salariés**.

Quels sont les objectifs de cette sensibilisation ?

- Limiter les risques d'un piratage à cause d'une erreur humaine.
- Éviter les fuites ou les pertes de données volontaires ou involontaires.
- Réduire les tentatives d'usurpation d'identité de votre entreprise.

Les mesures élémentaires à mettre en place

Pour être en conformité avec le RGPD, différentes mesures doivent être prises :

- **première mesure : rédiger précisément votre charte informatique**
  Elle doit indiquer les droits et **les devoirs de chacun** en matière de protection des données personnelles (pour être en conformité avec le RGPD), de confidentialité des informations sensibles et d'usage des outils informatiques ;

- **deuxième mesure : mettre en place une politique de sensibilisation**
  Il existe toute une palette d'outils de **communication interne** : newsletter, affichage dans les bureaux et à la cafeteria, mémos...
  Cette politique passe également par des **sessions de formation** : intra-entreprise, e-learning mis à disposition par Generali, tutoriels vidéo… Quelle que soit la solution retenue, il s'agit de rappeler les règles de base en matière de sécurité informatique afin que tout le personnel (y compris la direction) acquière les bons automatismes.

Il faut par exemple que chaque collaborateur sache qu'en cas d'infiltration par un ransomware, le premier réflexe est de débrancher immédiatement le câble Ethernet et de couper la connexion Wi-Fi de l'ordinateur touché afin de limiter au plus vite la propagation du virus à tous les postes de travail ;

- **troisième mesure : organiser des formations spécifiques pour les services RH et comptabilité.**
  Des **formations spécifiques** aux services RH et comptabilité doivent être organisées, car ils sont de plus en plus la cible d'escrocs. Les premiers peuvent être touchés par un CV envoyé par e-mail et qui cache un code malveillant. Ils peuvent aussi être piégés par de faux profils sur les réseaux sociaux.
  Quant aux seconds, ils peuvent être victimes d'une « arnaque au faux Président ». Une personne usurpant l'identité du chef d'entreprise appelle son service comptable pour qu'il effectue immédiatement un virement afin de conclure par exemple un important marché.
  Cette escroquerie peut mettre en péril votre activité. En février 2016, une PME a ainsi été mise en liquidation judiciaire après deux arnaques au Président ayant entraîné le détournement d'environ 1,6 million d'euros.

Ce qu'il ne faut pas faire

Indépendamment de la taille ou du secteur d'activité de votre entreprise, ne restez surtout pas indifférent à sa sécurité numérique. **Toutes les PME peuvent être un jour ou l'autre victimes d'un piratage ou d'une perte de données.**

La sécurité informatique ne concerne pas uniquement les ordinateurs. **Les connexions via un smartphone peuvent aussi être à l'origine d'une attaque informatique.** Le rapport de Proofpoint révèle que 42 % des clics sur des URL frauduleuses ont été effectués depuis des terminaux mobiles.

Enfin, **ne pas faire de sauvegardes de ses données critiques est une erreur majeure.** C'est l'une des meilleures parades contre les ransomware. Payer la rançon exigée par le pirate ne garantit pas que vous pourrez récupérer vos fichiers pris en otage. Il est préférable de formater le disque dur du PC infecté et de faire une restauration de données.

Testez votre niveau de sécurité !

L'ANSSI (Agence nationale de la sécurité des systèmes d'information) a mis en place un MOOC (Massive Open Online Course). Il s'agit de cours en ligne, gratuits et accessibles à tous. Différents modules thématiques sont disponibles.

LEXIQUE

Les bons réflexes à faire passer

- Mettre à jour tous les ordinateurs et les appareils mobiles
- Utiliser des mots de passe « forts », c'est-à-dire comprenant au minimum 8 caractères, des majuscules, des chiffres et des caractères spéciaux, et dont le sens n'est pas transparent. Exemple de mot de passe « fort »: L54*45Rge.
- Contrôler les accès utilisateurs aux dossiers sensibles
- Sauvegarder ses informations confidentielles
- Multiplier les petites sessions de rappel aux bonnes pratiques en matière de sécurité informatique

Pour vous accompagner dans la formation de vos salariés, découvrez l'offre Generali Protection Numérique
https://www.generali.fr/professionnel/assurance-cyber-risques/

Generali IARD. Société anonyme au capital de 94 630 300 euros. Entreprise régie par le Code des assurances - 552 062 663 RCS Paris
Siège social : 2 rue Pillet-Will - 75009 Paris

Informations non contractuelles à caractère publicitaire données à titre purement indicatif et dans un but pédagogique. La compagnie ne saurait être tenue responsable d'un préjudice d'aucune nature lié aux informations fournies. La contractualisation éventuelle avec le partenaire nommé ci-dessus se fait sous votre seule et unique responsabilité et ne saurait engager la responsabilité des sociétés Generali en France. Le choix de contractualiser ou pas avec ce partenaire relève de la gestion de votre entreprise et est sans incidence sur vos contrats d'assurance Generali qui demeure tiers à vos relations.

L'authentification des utilisateurs : un indispensable de votre sécurité informatique

Ordinateurs, smartphones, télétravail, Cloud… Ce sont autant de « portes ouvertes » dans votre réseau informatique qui peuvent être à l'origine d'une fuite de données ou d'une infection par un virus. L'authentification des utilisateurs est indispensable.

Pour accéder à leur messagerie ou à des documents de travail, certains salariés utilisent leur tablette et le Wi-Fi, d'autres téléchargent des dossiers depuis leur ordinateur de bureau et une connexion Ethernet. Quels dossiers ont-ils ouverts ? Ont-ils réellement besoin d'accéder à ces fichiers pour leur travail ? Est-ce que le compte de l'intérimaire qui a fini sa mission est bloqué ?

Toutes ces questions doivent avoir des réponses précises et justifiées. Chaque collaborateur doit être doté d'un identifiant qui lui est propre et doit s'authentifier avant toute utilisation des moyens informatiques.

L'authentification des salariés et le traçage des accès sont indispensables, car :

- ils permettent d'avoir une **vision globale de son réseau** et de ses équipements informatiques ;
- ils renforcent la **sécurité des données** à caractère personnel afin d'être en conformité avec le RGPD ;
- ils constituent des **preuves en cas de fraude interne**.

Authentification des utilisateurs : les principales mesures à prendre

- **Première mesure : répartir les salariés par métier**
  La constitution de groupes de travail par métiers (ou par profils d'habilitation pour télécharger ou modifier des documents par exemple) évite que tous les salariés ouvrent des fichiers sensibles. Un commercial peut utiliser le logiciel permettant de faire des devis, mais il n'a pas besoin de consulter la comptabilité et les données financières de l'entreprise.

- **Seconde mesure : renforcer l'authentification**
  Les salariés doivent avoir un identifiant et un mot de passe différents pour chaque usage (accès à Office 365, aux réseaux sociaux, aux dossiers partagés sur le serveur ou dans le Cloud…). Pour améliorer cette authentification, le responsable informatique doit mettre en place des procédures techniques imposant des mots de passe « forts » avec l'utilisation d'au moins 8 caractères (lettres en majuscule et en minuscule, chiffres et symboles).

- **Troisième mesure : la signature d'un engagement de confidentialité**
  Elle peut être indiquée dans la charte informatique ou dans une clause des contrats de travail. Ces documents doivent aussi rappeler que les salariés ne doivent communiquer leurs mots de passe à quiconque.

- **Quatrième mesure : supprimer les comptes anonymes et génériques (admin, user, contact...)**
  Chaque personne doit être identifiée nommément afin de pouvoir relier une action sur le système informatique à un utilisateur. Cette mesure permet aussi de bloquer les connexions anonymes pouvant être à l'origine d'une tentative d'infiltration.

Ce qu'il ne faut pas faire

- **Multiplier les comptes « administrateur »**
  Seul le responsable informatique doit avoir ce profil afin d'assurer la maintenance (gestion des groupes utilisateurs, installation ou suppression de logiciels…) et la mise à jour (téléchargement des correctifs de sécurité) du parc informatique et du réseau.

- **Laisser visibles tous ses mots de passe**
  Lors des formations de sensibilisation, la Direction de l'entreprise doit rappeler aux collaborateurs qu'ils ne doivent pas conserver leurs mots de passe sur des post-its collés sur l'écran du PC ou une feuille mise dans un tiroir.
- **Ne jamais changer tous ses mots de passe**
  Régulièrement (tous les six mois par exemple), il est recommandé de modifier tous les mots de passe des salariés. Cette opération doit être aussi l'occasion de vérifier si des comptes sont toujours actifs alors qu'une personne a démissionné ou que l'intérimaire a terminé sa mission.
- **Sauvegarder sans chiffrement les identifiants et mots de passe**
  Ces données sont une cible privilégiée par les attaquants désireux d'accéder à votre réseau. Le responsable informatique doit protéger cette base de données par des solutions de chiffrement afin de disposer d'accès aussi « sécurisés » qu'un coffre-fort.

Pour aller plus loin

Si certaines authentifications envisagées ont recours à des **dispositifs biométriques**, il est nécessaire d'effectuer une demande d'autorisation auprès de la CNIL (Commission nationale de l'informatique et des libertés).

Concernant **des dispositifs basés sur l'empreinte digitale**, il convient de se référer au Guide de la CNIL.

L'ANSSI (Agence nationale de la sécurité des systèmes d'information) publie une **liste de logiciels certifiés** et permettant de renforcer l'authentification des utilisateurs.

Generali vous propose une offre alliant prévention, protection et accompagnement contre les cyber risques. Découvrez l'offre Generali Protection Numérique !

LEXIQUE

Lexique : Les authentifications biométriques

Il s'agit de technologies permettant d'identifier de manière unique une personne grâce à une ou plusieurs caractéristiques biologiques, telles que l'empreinte digitale, le visage, la morphologie de la main, la voix…

La biométrie remplit deux fonctions distinctes :
• l'identification répond à la question **« Qui êtes-vous ? »**. Dans ce cas, la personne est identifiée parmi d'autres (vérification) ;
• l'authentification répond à la question : **« Êtes-vous bien celui que vous prétendez être ? »**. Dans ce cas, elle certifie l'identité d'une personne en comparant les données qu'elle va présenter avec celles préenregistrées de la personne qu'elle prétend être.

Generali IARD. Société anonyme au capital de 94 630 300 euros. Entreprise régie par le Code des assurances - 552 062 663 RCS Paris
Siège social : 2 rue Pillet-Will - 75009 Paris

Informations non contractuelles à caractère publicitaire données à titre purement indicatif et dans un but pédagogique. La compagnie ne saurait être tenue responsable d'un préjudice d'aucune nature lié aux informations fournies. La contractualisation éventuelle avec le partenaire nommé ci-dessus se fait sous votre seule et unique responsabilité et ne saurait engager la responsabilité des sociétés Generali en France. Le choix de contractualiser ou pas avec ce partenaire relève de la gestion de votre entreprise et est sans incidence sur vos contrats d'assurance Generali qui demeure tiers à vos relations.

La sauvegarde des données pour assurer la pérennité de votre activité

Imaginez une journée sans pouvoir accéder à votre fichier clients, votre comptabilité ou vos documents administratifs. C'est impossible, car vous êtes dépendant de toutes ces données ! Or, le pire peut vous arriver si vous n'avez pas mis en place des sauvegardes de vos données informatiques.

Rien n'est éternel. Du jour au lendemain, vos disques durs peuvent tomber en panne. Sans toujours prévenir par des signes particuliers (bruit suspect, accès plus lent aux fichiers...), ces pièces mécaniques peuvent « lâcher ». Et la récupération des données qu'ils contenaient n'est pas toujours possible. 80 % des entreprises non ou mal équipées déposent le bilan après un sinistre informatique .

Outre les pannes matérielles, les sauvegardes représentent l'un des facteurs-clés de la pérennité de votre entreprise :

- Elles permettent **de récupérer des données effacées ou détruites** par erreur, ou volontairement, par des salariés ;
- Elles **évitent de payer une rançon** exigée par des pirates qui ont pris en otage tous vos fichiers avec un virus de type ransomware. Le formatage du disque dur du poste de travail infecté et la restauration des données sont en effet la seule solution véritablement efficace contre ce type d'attaque ;
- Elles facilitent le **redémarrage de votre activité après un dégât des eaux ou un incendie.**

À l'heure de l'essor de l'Internet des objets (IoT), les données se multiplient au sein de l'entreprise constituant un véritable patrimoine informatif. Et pourtant, sauvegarder ces données n'est pas toujours un réflexe : 35 % des entreprises n'ont pas établi de règles en matière de conservation des données liées à l'IoT .

Sauvegarde des données : les principales mesures à prendre

Pour être en conformité avec le RGPD, différentes mesures doivent être prises :

- **Première étape : identifier et classer toutes vos données**
  Toutes vos données sont importantes. Mais certaines présentent une importance capitale : brevets, fichiers clients et prospects, factures, documents administratifs et tous ceux intégrant des données à caractère personnel.
  Après avoir repéré leur **lieu exact de stockage** (serveur, Cloud, prestataire local, etc.), il est indispensable de les **classifier par ordre d'importance selon une échelle de 1 à 5**, 1 étant « insignifiant » et 5 « catastrophique ».
  Toutes celles qui ont 4 au minimum doivent bénéficier d'une sécurité renforcée : authentification et surveillance des accès, chiffrement, sauvegardes régulières…

- **Seconde étape : programmer des sauvegardes**
  Il est important d'effectuer des sauvegardes fréquentes pour éviter la perte d'information. Selon le volume d'informations à protéger, il peut être opportun de prévoir des **sauvegardes incrémentales à une fréquence quotidienne** et des **sauvegardes complètes à une fréquence moindre** (hebdomadaire ou bimensuelle).

À SAVOIR

Il y a trois types de sauvegardes :

- complète : toutes vos données sont copiées indépendamment des modifications depuis la précédente sauvegarde ;
- différentielle : elle permet de conserver toutes les modifications depuis la sauvegarde complète, quel que soit le type de modification ;
- incrémentale : elle permet de conserver toutes les modifications depuis la précédente sauvegarde. Ce qui signifie que la préservation des données est effectuée depuis les sauvegardes incrémentales précédentes.

- **Troisième étape : des tests de restauration**
  Trop souvent négligée, cette pratique est pourtant essentielle. Tous les mois (ou plus souvent si votre activité est importante), vous devrez vérifier que les données restaurées sont utilisables en l'état.

Ce qu'il ne faut pas faire

- **Conserver les sauvegardes dans votre entreprise**
  C'est bien connu, il ne faut pas mettre tous ses œufs dans le même panier. Cette règle de bons sens s'applique aussi à vos sauvegardes. Imaginez un incendie dans vos locaux ; vos sauvegardes ont certainement brûlé sauf si vous les avez mises dans un coffre ignifugé et étanche. Pensez donc à héberger vos données dans le Cloud ou chez un prestataire informatique local.
- **Sauvegarder sur un DVD ou des clés USB**
  Ces supports sont fragiles, ils ne sont pas éternels et vous pouvez les égarer facilement. L'usage des clés USB est par ailleurs fortement déconseillé, car elles peuvent contenir des virus informatiques et infecter vos postes de travail.
- **Ne pas lire les Conditions générales de service**
  Avant d'effectuer des sauvegardes sur des plateformes sur Internet (dans le Cloud) ou chez un prestataire informatique local, vérifiez les clauses du contrat concernant les procédures de sécurité mises en place. Soyez attentif aussi à la présence d'une clause de réversibilité. Elle doit indiquer précisément comment et sous quel format vous pourrez récupérer vos fichiers si vous souhaitez changer de fournisseur.

Pour aller plus loin

Parlez-en à votre prestataire informatique. Celui-ci pourra vous conseiller différentes solutions adaptées à vos besoins et moyens.

Il doit notamment vous proposer **d'installer un NAS**. Ce n'est pas un achat superflu.

Le « Network Attached Storage » ou « Espace de stockage lié au réseau », est un petit boîtier (un mini-PC) qui enferme deux disques durs (voire plus pour les gros modèles). Ils sont synchronisés entre eux en temps réel (le disque B est le miroir du disque A).

C'est le principe de la technologie appelée RAID (acronyme de Redundant Array of Independent Disks). Elle assure une parfaite sauvegarde et limite les impacts d'une panne. Si l'un des deux supports tombe en panne, vous pouvez récupérer immédiatement les données sur le second. Très facile à installer et à configurer via une interface web, le NAS représente un bon investissement en matière de protection de données.

LEXIQUE

Vos obligations

L'article 34 de la loi du 6 janvier 1978 du Code pénal précise que « le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

Prévention, protection, accompagnement, découvrez découvrez l'offre Generali Protection Numérique
https://www.generali.fr/professionnel/assurance-cyber-risques/

Generali IARD. Société anonyme au capital de 94 630 300 euros. Entreprise régie par le Code des assurances - 552 062 663 RCS Paris
Siège social : 2 rue Pillet-Will - 75009 Paris

Informations non contractuelles à caractère publicitaire données à titre purement indicatif et dans un but pédagogique. La compagnie ne saurait être tenue responsable d'un préjudice d'aucune nature lié aux informations fournies. La contractualisation éventuelle avec le partenaire nommé ci-dessus se fait sous votre seule et unique responsabilité et ne saurait engager la responsabilité des sociétés Generali en France. Le choix de contractualiser ou pas avec ce partenaire relève de la gestion de votre entreprise et est sans incidence sur vos contrats d'assurance Generali qui demeure tiers à vos relations.

Garantissez la sécurité de vos postes de travail

Connecté en permanence à Internet, votre ordinateur peut être infecté à tout moment par un virus. Les risques ? Vol de données confidentielles, paralysie de toute l'activité, usurpation d'identité. Installer un antivirus et un pare-feu est indispensable.

Êtes-vous prêt à faire entrer chez vous un inconnu ? Tout le monde se pose cette question… sauf lorsqu'il s'agit d'Internet. En n'installant pas un **pare-feu** sur votre ordinateur, c'est comme si vous répondiez par « oui » à cette question.

Appelé aussi firewall en anglais, ce programme joue le même rôle que le physionomiste d'une discothèque interdisant l'accès aux personnes ayant un comportement agressif ou suspect.

Rapporté au réseau informatique, ce logiciel filtre les connexions entrantes (pour bloquer l'installation d'un programme malveillant) mais également sortantes (pour éviter des fuites de données par exemple).

Quant à l'antivirus, c'est la vigie de votre ordinateur. Il vérifie « l'identité » des logiciels et des fichiers que vous souhaitez installer ou ouvrir. Dès qu'il repère un code malveillant, il le met en quarantaine ou le supprime selon ses réglages.

Mais **« 90 % des PME n'ont aucun outil pour lutter contre la cybercriminalité »,** assure Michel Van Den Berghe, directeur général d'Orange Cyberdefense . Or, l'installation de ces deux outils de sécurité est indispensable. Sans eux, vous serez rapidement infectés par une pièce jointe cachant un virus comme les ransomware (ou rançongiciels) qui chiffrent toutes les données de votre réseau informatique. Selon une étude d'Avast, un éditeur d'antivirus, **20 000 ordinateurs sont infectés tous les mois en France par ce type de virus.**

Si aucune sauvegarde n'a été mise en place au préalable, la situation devient cauchemardesque : l'entreprise perd toutes ses données.

Autre menace : l'installation à votre insu d'un **keylogger.** Il s'agit d'un **logiciel espion enregistrant toutes les données que vous tapez** : mots de passe, identifiants, numéro de carte bancaire… Une fois récupérées, toutes ces informations sont revendues incognito sur le marché noir. D'où l'intérêt d'avoir un pare-feu filtrant ses flux sortants !

Des **symptômes pouvant indiquer la présence de codes malveillants** doivent vous alerter :

- ralentissement de l'ordinateur ou de la connexion ;
- ouvertures régulières de fenêtres de pop-up et de publicités ;
- surconsommation des ressources : réduction de l'espace libre sur le disque dur ou surcharge du processeur ;
- l'antivirus ou le pare-feu est désactivé sans votre intervention ;
- les mises à jour du système d'exploitation (Windows), de l'antivirus ou du pare-feu échouent constamment, etc.

La sécurité des postes de travail : les principales mesures à prendre

Le renforcement de ces droits accentue par conséquent les obligations de toutes les entreprises qui collectent, traitent et stockent des données personnelles.

Aujourd'hui, de nombreuses sociétés ne protègent pas assez leur réseau informatique, par manque de moyens ou de prise de conscience des risques numériques. Résultat, **onze incidents de cybersécurité seraient comptabilisés chaque jour en milieu professionnel en France,** d'après le cabinet de conseil PwC.

Face aux menaces numériques (phishing, infiltration sur le réseau informatique, virus…) pouvant entraîner une fuite de données - non seulement celles de vos clients, mais aussi celles de votre entreprise - vous devez renforcer votre niveau de sécurité.

Les mesures élémentaires à mettre en place

- **Première mesure : installer un antivirus et un pare-feu**
  L'installation de ces deux logiciels sur chacun de vos postes de travail renforce votre niveau de protection.
  Ne choisissez pas des solutions gratuites. Optez plutôt pour une suite payante regroupant notamment un antivirus, un pare-feu et un antispam. Proposés par le même éditeur, ces outils s'intègrent parfaitement et n'entraînent pas de bugs.

- **Seconde mesure : bien configurer vos antivirus, anti spam et pare-feu**
  Activez leur mise à jour automatique afin qu'ils intègrent les dernières variantes des programmes malveillants ou des adresses URL suspectes. Réglez également l'antivirus de façon à ce qu'il scanne tout le contenu d'une clé USB ou d'un disque dur externe dès qu'il est inséré dans un poste de travail. Ce logiciel doit aussi analyser toutes les pièces jointes avant leur ouverture.

- **Troisième mesure : faites des analyses complètes**
  Beaucoup plus longues qu'un scan rapide, les analyses complètes doivent être réalisées régulièrement, car elles traquent les virus dans les moindres recoins de vos disques durs. Cette analyse pouvant durer plusieurs heures, lancez-la le soir en laissant allumé votre PC (mais en verrouillant la session par un mot de passe !) pour éviter qu'une personne n'accède à vos fichiers.

- **Quatrième mesure : sécuriser votre PC**
  Utilisez un mot de passe « fort » comprenant au moins 8 caractères mêlant majuscules, minuscules et caractères spéciaux (évitez les noms, dates de naissance, et tout terme du dictionnaire) pour ouvrir votre session. Changez-le tous les six mois. Enfin, configurez Windows pour qu'il télécharge automatiquement ses mises à jour. Faites de même avec tous les logiciels installés sur chacun des postes de travail.

- **Cinquième mesure : faites référence à votre charte informatique**
  Précisez dans ce document les devoirs de vos salariés en matière de sécurité informatique : ne pas ouvrir d'email suspect, ne pas installer de version pirate de logiciels, ne communiquer ses identifiants à quiconque… Ces règles de base doivent être rappelées lors de sessions de sensibilisation.

Ce qu'il ne faut pas faire

- **Pré-enregistrer ses mots de passe dans les navigateurs**
  La facilité d'usage n'a jamais fait bon ménage avec la sécurité informatique. Configurer son navigateur Web pour qu'il enregistre tous vos identifiants et mots de passe est pratique pour ouvrir plus rapidement son compte sur un réseau social ou sa messagerie en ligne. Mais si un pirate accède à votre ordinateur, il peut récupérer toutes vos précieuses données.

- **Ne pas verrouiller sa session**
  Vous devez régler votre système d'exploitation de façon à ce que votre session soit verrouillée au bout de quelques minutes. Pour accéder de nouveau à vos fichiers, vous devrez retaper votre mot de passe. Cela évitera qu'une personne mal intentionnée puisse consulter vos documents en votre absence.

- **Utiliser un compte « administrateur »**
  Ce type de compte permet de tout faire sur un poste de travail et notamment d'installer ou de supprimer un programme. Seul le responsable informatique doit en posséder un. Tous les autres salariés doivent avoir un compte « utilisateur ».

Pour aller plus loin

Pour repérer les virus, ce logiciel applique deux principales méthodes :

- **il vérifie la « signature »** (en quelque sorte l'ADN) des programmes et des fichiers fonctionnant sur le PC. Si une signature correspond à celle d'un code malveillant, celui-ci est mis en quarantaine ou supprimé selon la configuration préalablement établie. La mise en quarantaine est conseillée, car les antivirus peuvent parfois afficher de fausses alertes en pointant du doigt un programme légitime ;

- **il étudie le comportement** des logiciels pour repérer des actions douteuses (tentatives d'ouverture en lecture/écriture de fichiers exécutables, écriture sur une partition...). Là aussi, il les bloque ou les supprime.

ANNEXE

Deux techniques simples pour choisir vos mots de passe :

- la méthode phonétique : « J'ai acheté 5 CD pour cent euros cet après-midi » : ght5CD%E7am ;
- la méthode des premières lettres : « 1 Chef d'Entreprise averti en vaut 2 » : 1Cd'Eaev2.

Pour vous accompagner dans la protection de vos postes de travail, découvrez l'offre Generali Protection Numérique

https://www.generali.fr/professionnel/assurance-cyber-risques/

Generali IARD. Société anonyme au capital de 94 630 300 euros. Entreprise régie par le Code des assurances - 552 062 663 RCS Paris
Siège social : 2 rue Pillet-Will - 75009 Paris

Informations non contractuelles à caractère publicitaire données à titre purement indicatif et dans un but pédagogique. La compagnie ne saurait être tenue responsable d'un préjudice d'aucune nature lié aux informations fournies. La contractualisation éventuelle avec le partenaire nommé ci-dessus se fait sous votre seule et unique responsabilité et ne saurait engager la responsabilité des sociétés Generali en France. Le choix de contractualiser ou pas avec ce partenaire relève de la gestion de votre entreprise et est sans incidence sur vos contrats d'assurance Generali qui demeure tiers à vos relations.

La sécurité de votre site web

Pour développer vos parts de marché, vous avez décidé de créer un site vitrine ou de e-commerce. L'ergonomie des pages web et la gestion des stocks sont indispensables pour satisfaire vos clients. Mais leur fonctionnement optimal pourrait être menacé si vous avez négligé la sécurité informatique.

Quelle que soit la solution retenue (site vitrine ou de e-commerce), il est primordial de renforcer la protection de votre site contre diverses menaces numériques. Or, beaucoup de sites web professionnels présentent d'importantes vulnérabilités. En auditant le niveau de sécurité de ses clients français entre juin 2016 et juin 2017, Wavestone, un cabinet spécialisé dans la transformation digitale des entreprises, a constaté que la moitié des sites était affectée par « au moins une faille grave ». Une faille « grave » permet d'accéder à l'ensemble du contenu du site et/ou de compromettre les serveurs. Profiter d'une faiblesse de sécurité sur un site c'est comme si un cambrioleur passait par une fenêtre laissée ouverte.

Quels sont les risques ?

- **Première menace : la prise de contrôle de votre site**
  En accédant aux coulisses de votre boutique en ligne ou de votre site vitrine, une personne malhonnête peut devenir administrateur à votre place. Elle peut alors tout faire : télécharger votre fichier clients et leurs identifiants, récupérer des informations sur vos pratiques commerciales, supprimer des plug-in (ou extensions en français) permettant de gérer les paniers, la facturation, les mailings…
- **Deuxième menace : l'atteinte à votre réputation**
  Mal sécurisé, votre site peut présenter une faille qui pourrait permettre à une personne malveillante de « défigurer » votre page d'accueil en remplaçant les photos de vos produits par des images osées ou des messages illicites (racistes, injurieux…). Visible par tout le monde, cet acte porte directement atteinte à votre notoriété et à votre crédibilité vis-à-vis de vos clients, mais aussi de vos partenaires et actionnaires.
- **Troisième menace : l'indisponibilité de votre site**
  Pas assez bien protégé, votre site peut être victime d'une **attaque DoS** (Denial of Service attack ou attaque par déni de service). Après avoir pris le contrôle de milliers d'ordinateurs à l'insu de leur propriétaire, un pirate peut les configurer de façon à ce qu'ils se connectent en même temps à votre site. Croulant sous les requêtes simultanées, ce dernier devient en quelques secondes inaccessible pour tous les internautes. C'est comme un compteur électrique qui « disjoncte » à cause d'une trop forte demande.
- **Quatrième menace : l'usurpation d'identité numérique**
  Cet acte malveillant est appelé **« Cybersquat »**. Il consiste à déposer un nom de domaine en usurpant le nom de votre PME ou de vos marques en modifiant quelques lettres. Par exemple elyseee.fr. Les noms de domaine ne coûtant pas très chers, pensez à réserver (et à renouveler chaque année) des variantes en .fr et .com.

La sécurité du site web : les mesures élémentaires à mettre en place

- **Installer toutes les mises à jour**
  Comme pour un ordinateur, vous devez **mettre à jour toutes les extensions installées sur votre site et la version de son CMS.** Un « Content Management System » est une solution « packagée » permettant de créer un site et d'y ajouter des pages web et des rubriques. Les CMS les plus connus sont Drupal, Wordpress et Magento. Ces mises à jour limitent ainsi les vulnérabilités.
- **Limiter les accès**
  Assurez-vous que les rubriques et les fichiers de votre site ne sont accessibles qu'aux seules **personnes habilitées.** Veillez aussi à ce qu'elles ne donnent pas leurs identifiants et mots de passe à n'importe qui.

- **Bloquer les tentatives malveillantes**
  Un **« captcha »** est un terme étrange, mais sa fonction est pratique. Lorsqu'une personne veut se connecter à votre site (en tant qu'utilisateur ou client), elle doit taper son identifiant et mot de passe, mais également **répondre à la petite question qui apparaît.** C'est un captcha, acronyme de « Completely Automated Public Turing test to Tell Computers and Humans Apart » ou « Test public de Turing complètement automatique ayant pour but de différencier les humains des ordinateurs »). Cette question peut par exemple demander de cliquer sur tous les carrés représentant un bus dans une image quadrillée. Cette technique permet de bloquer les logiciels-robots incapables de répondre à ce type de requête. C'est une parade efficace contre les tentatives répétées qui pourraient empêcher l'accès à votre site comme une attaque DoS (vérifiez d'ailleurs que votre hébergeur propose bien cette protection).

Ce qu'il ne faut pas faire

- **Utiliser des mots de passe « faibles »**
  L'étude de Wavestone montre que dans **45 % des cas les mécanismes d'authentification ne sont pas suffisamment robustes.** Les mots de passe n'étaient pas assez complexes (avec minimum 8 caractères et comprenant majuscules, minuscules et caractères spéciaux) et les tentatives d'accès à répétition n'étaient pas bloquées.

- **Ne jamais sauvegarder son site**
  Même si votre site est hébergé chez un prestataire informatique ou un fournisseur dans le Cloud, **faites chaque semaine une sauvegarde locale.** Cette précaution permet d'avoir toujours une copie exacte de son site et de l'intégralité de son contenu.

ANNEXE

Lexique : le HTTPS

Le **HTTP** (Hyper Text Transfert Protocol) est un protocole permettant de se connecter à un site web. Le HTTPS (le petit cadenas affiché dans le navigateur web) joue le rôle d'un fourgon blindé : il assure la sécurité du transport des billets

Rapporté à Internet, le **HTTPS protège l'intégrité ainsi que la confidentialité des flux** entre le PC du client et votre site. Ces flux sont sécurisés via le protocole Transport Layer Security (TLS), qui intègre trois niveaux clés :

- **le chiffrement** des échanges (les flux sont codés) ;
- **l'intégrité** des données (elles ne peuvent être ni modifiées, ni corrompues durant leur transfert) ;
- **l'authentification** (les internautes communiquent avec le bon site Web).

Pour inciter les entreprises à migrer leur site vers le HTTPS, Google a décidé de référencer en priorité ces sites. Si vous souhaitez être vu par de nombreuses personnes, voici donc un argument supplémentaire.

Vous souhaitez vous prémunir contre toute cyberattaque ? consultez l'offre Generali Protection Numérique
https://www.generali.fr/professionnel/assurance-cyber-risques/

Generali IARD. Société anonyme au capital de 94 630 300 euros. Entreprise régie par le Code des assurances - 552 062 663 RCS Paris
Siège social : 2 rue Pillet-Will - 75009 Paris

Informations non contractuelles à caractère publicitaire données à titre purement indicatif et dans un but pédagogique. La compagnie ne saurait être tenue responsable d'un préjudice d'aucune nature lié aux informations fournies. La contractualisation éventuelle avec le partenaire nommé ci-dessus se fait sous votre seule et unique responsabilité et ne saurait engager la responsabilité des sociétés Generali en France. Le choix de contractualiser ou pas avec ce partenaire relève de la gestion de votre entreprise et est sans incidence sur vos contrats d'assurance Generali qui demeure tiers à vos relations.

La sécurité du réseau informatique de l'entreprise

Comme un grain de sable qui enraye une machine, le moindre virus peut avoir un impact majeur sur l'activité de votre PME. Raccordé en permanence à Internet, votre réseau doit être blindé contre les différentes attaques informatiques.

Le ciel peut vous tomber sur la tête du jour au lendemain, dès la première heure. Sans raison apparente, un virus vient de pénétrer votre réseau informatique. Dans de nombreux cas, il s'agit d'un ransomware (ou rançongiciel). Caché généralement dans la pièce jointe d'un email, ce code malveillant peut en quelques secondes « chiffrer » (ou crypter) tous vos dossiers.

Si vous avez mis en place une politique de sauvegarde cohérente, votre activité ne sera pas longtemps paralysée. Sinon, c'est la catastrophe. Fin septembre 2017, une petite entreprise du Puy-de-Dôme a été contrainte de mettre la clé sous la porte après ce type de piratage.

La sécurité du réseau informatique de l'entreprise : les mesures élémentaires à mettre en place

- **Première mesure : la sécurité physique**
  Trop souvent négligée, elle est pourtant essentielle ! **La pièce où sont installés les serveurs et l'équipement réseau doit être fermée à clé.** Son accès doit être réservé à quelques personnes dûment identifiées. Cette précaution qui ne coûte presque rien permet d'éviter des actes malveillants ou involontaires au cœur de l'entreprise, qui pourraient entraîner un effacement ou une fuite des données ou provoquer un dysfonctionnement de l'infrastructure.

- **Deuxième mesure : cloisonner son réseau**
  Après avoir déterminé les composants critiques (équipements, serveurs, postes de travail d'utilisateurs sensibles, etc.), il est nécessaire de cloisonner son réseau. Dans la Marine, si un bateau est touché il ne coule pas, car sa coque est divisée en parties indépendantes. Cela doit être la même chose pour un réseau informatique ; **si une partie est infectée, l'ensemble ne doit pas être contaminé** sous peine de bloquer toute l'activité.

- **Troisième mesure : sécuriser le Wi-Fi**
  Les accès sans fil de type Wi-Fi doivent utiliser un chiffrement en l'état de l'art (WPA2 pour « Wi-Fi Protected Access 2 » ou WPA2-PSK avec un mot de passe complexe). Il convient aussi de modifier le SSID (nom du réseau Wi-Fi fourni). Si un accès sans fil est disponible pour les personnes extérieures (techniciens pour la maintenance, stagiaires...), il doit être séparé du réseau interne et avoir un accès temporaire. Les clés d'accès au Wi-Fi doivent être « fortes » (comporter différentes lettres en minuscules et majuscules, des chiffres et des signes) et être changées tous les six mois par exemple.

- **Quatrième mesure : tenir un inventaire de ses équipements**
  Il est indispensable de tenir à jour la **liste précise de tous les équipements informatiques qui peuvent se connecter au réseau** (ordinateurs personnels, imprimantes, photocopieurs, etc.). Cet inventaire doit également indiquer les utilisateurs classés par droits d'accès (répertoires, applications, dossiers dans le Cloud, etc.) de façon graduée.

- **Cinquième mesure : filtrer les accès à son réseau**
  Cet objectif peut être atteint grâce à des **pare-feux dits de « nouvelle génération ».** Qu'il soit matériel ou logiciel, ce firewall intègre des capacités traditionnelles (filtrage de paquets, blocage d'URL…). Mais il peut également détecter et stopper de nombreuses attaques sophistiquées en analysant des applications et des protocoles de communication. À la différence des pare-feux de première génération, ceux-ci intègrent en effet des éléments de contexte supplémentaires (comme des bases de réputation des sites ou d'adresses IP malsaines) afin d'améliorer les processus de prise de décision. Il s'agit notamment d'identifier précisément les détails du trafic Web afin de bloquer les flux illégitimes et l'exploitation de vulnérabilités.

Ce qu'il ne faut pas faire

- **Ne jamais laisser les mots de passe par défaut**
  Même un appareil aussi anodin qu'une imprimante connectée ou une caméra de vidéosurveillance peut être utilisé pour pénétrer un réseau informatique. Dès que ces équipements sont installés, il est donc indispensable de modifier le mot de passe par défaut (que l'on peut trouver facilement sur internet pour chaque marque !) par un autre plus complexe et connu seulement de quelques personnes dans l'entreprise.

- **Ne pas se soucier des accès à distance**
  Qu'il s'agisse du télétravail, de la téléassistance ou de la téléadministration, cette connexion peut être à l'origine volontaire ou involontaire d'une infection de votre réseau informatique. Il **est donc recommandé d'installer un VPN**. Un « Virtual Private Network » ou « Réseau Privé Virtuel » désigne un accès sécurisé entre deux appareils ou plus. C'est en quelque sorte un tunnel réservé aux véhicules identifiés et autorisés. Il doit être mis en place pour le télétravail et les connexions à distance (cadres à l'étranger, télémaintenance…). L'accès à un VPN doit être sécurisé par l'utilisation de carte à puce ou d'un boîtier générateur de mots de passe à usage unique.

Pour aller plus loin

- **Protégez-vous contre le « phreaking »**
  Non sécurisé, votre réseau téléphonique peut vous coûter très cher. Surtout si vous êtes victime d'un **« phreaking »**, **un piratage de votre serveur téléphonique.**
  Fin août 2014, à l'issue d'un week-end, une entreprise implantée en région Rhône-Alpes constate que son serveur téléphonique a été piraté. Plusieurs centaines d'appels ont été émis essentiellement à destination de l'Afrique. Le préjudice est estimé à environ 12 000 € HT.

- **Pour limiter les risques :**
  - Verrouillez les lignes sortantes durant les périodes d'inactivité de l'entreprise (nuits, week-ends, jours fériés, vacances…).
  - Changer périodiquement les clés sécurisées d'accès au modem du serveur téléphonique et les mots de passe des comptes de messagerie vocale des salariés.

Pour vous accompagner dans la protection de vos postes de travail, découvrez l'offre Generali Protection Numérique
https://www.generali.fr/professionnel/assurance-cyber-risques/

Generali IARD. Société anonyme au capital de 94 630 300 euros. Entreprise régie par le Code des assurances - 552 062 663 RCS Paris
Siège social : 2 rue Pillet-Will - 75009 Paris

Informations non contractuelles à caractère publicitaire données à titre purement indicatif et dans un but pédagogique. La compagnie ne saurait être tenue responsable d'un préjudice d'aucune nature lié aux informations fournies. La contractualisation éventuelle avec le partenaire nommé ci-dessus se fait sous votre seule et unique responsabilité et ne saurait engager la responsabilité des sociétés Generali en France. Le choix de contractualiser ou pas avec ce partenaire relève de la gestion de votre entreprise et est sans incidence sur vos contrats d'assurance Generali qui demeure tiers à vos relations.

Le BYOD et la sécurisation des appareils mobiles

Tablette, smartphone, PC portable… Les outils modernes permettent de répondre plus rapidement aux attentes des clients. Qu'ils appartiennent à vos collaborateurs ou que vous les mettiez à leur disposition, leur usage doit être encadré afin de protéger votre entreprise.

Tous les salariés possèdent un téléphone mobile, voire un ordinateur portable. À l'aise avec leur propre équipement, ils peuvent être plus productifs s'ils travaillent avec au bureau. C'est ce qu'on appelle le BYOD (**« Bring your own device »** ou « Apporter votre équipement personnel de communication »).

Même s'il est apparu en France il y a déjà quelques années, ce phénomène reste encore assez marginal. Selon une étude d'ISlean consulting (Cabinet de conseil en stratégie et organisation), **environ 5 % des PME et ETI françaises ont décidé de mettre en place une politique de BYOD généralisé en 2017**. Cela signifie que tous les employés peuvent travailler avec leur propre ordinateur et smartphone (d'un point de vue légal, des personnes peuvent refuser cette proposition et dans ce cas, l'entreprise leur fournit le matériel nécessaire).

Le BYOD « partiel » est plus important (10 % selon cette même étude). Il s'explique par l'usage mixte du téléphone. Les salariés l'utilisent à la fois pour consulter leurs emails personnels, mais aussi pour envoyer des courriers professionnels. D'autres utilisent leur tablette pour accéder à des logiciels en ligne (mode SaaS pour « Software as a Service ») et éditer un devis par exemple.

Ces appareils personnels peuvent donc contenir des données à caractère personnel et parfois des informations sensibles.

Quels sont les risques ?

- **Une infection du réseau ou de l'appareil**
  En accédant à votre réseau informatique avec son appareil mobile, un salarié peut être à l'origine (volontairement ou non) d'une infection virale ou d'une perte de données. « En 2018, nous devrions observer une évolution des attaques de type ransomware vers l'environnement mobile », avertit Lookout, une société spécialisée dans la sécurité des mobiles.
  Ce type de menace résulte très souvent d'une faible sécurité de l'équipement. Le collaborateur n'a pas forcément mis à jour son téléphone ou n'a pas installé un antivirus. Il peut aussi avoir téléchargé un clone d'un programme anodin qui va infecter son appareil. En novembre 2017, une fausse application WhatsApp, qui affichait de la publicité, a été téléchargée par 1 million d'utilisateurs d'Android.
- **Une perte de données**
  Les informations stockées sur les appareils mobiles des salariés peuvent être dérobées par un code malveillant (de type keylogger par exemple). Autre risque : la perte de ces équipements. Qui n'a jamais perdu son téléphone dans un taxi ? Qui n'a jamais été victime d'un vol de smartphone laissé par erreur sur une terrasse de café ?
- **Un vol de données à caractère personnel**
  En prenant le contrôle d'un smartphone ou d'un PC portable, un pirate peut récupérer des dossiers contenant des informations personnelles de vos salariés ou de vos clients. Cette faille de sécurité démontre une absence de conformité de votre entreprise avec le RGPD. En cas de fuite de données à caractère personnel, vous pouvez être sanctionné par la CNIL.

Le BYOD et la sécurisation des appareils mobiles : les mesures élémentaires à mettre en place

- **Première mesure : fournir des appareils mobiles**
  Afin d'avoir un parc homogène et identifié, vous pouvez interdire le BYOD et favoriser le… **COPE (« Corporate Owned Personally Enabled »**). Cela signifie que vous fournissez des appareils préconfigurés et qui vous appartiennent (d'où des obligations de maintenance, de gestion des licences et de protection des données).

Cette option vous permet de conserver le contrôle d'un terminal et de le sécuriser grâce à une solution logicielle appelée Mobile Device Management (MDM). Un MDM permet :
- un cloisonnement des usages,
- une sélection des applications autorisées.

- **Seconde mesure : désactiver la connexion automatique au Wi-Fi**
  Aucun smartphone ou PC portable ne doit pouvoir se connecter à votre réseau sans fil sans avoir été au préalable identifié et autorisé.

- **Troisième mesure : renforcer la sécurité des appareils mobiles**
  Les formations de sensibilisation aux risques numériques doivent être l'occasion de rappeler aux salariés quelques précautions de base :
  - Pour les smartphones et les tablettes : activer le code PIN pour qu'il soit demandé à chaque démarrage et **activer le code de verrouillage** afin qu'il soit exigé après chaque mise en veille réglée sur quelques minutes. Les mises à jour d'iOS et d'Android, ainsi que des applications, sont obligatoires. Enfin, **conserver le code IMEI** (15 à 17 chiffres) du smartphone. En cas de perte ou de vol, il permettra à l'opérateur de le bloquer à distance.
  - Pour les PC portables : comme pour les ordinateurs de bureau, il est indispensable d'avoir **un mot de passe « fort »** (c'est-à-dire comprenant majuscules, minuscules et caractères spéciaux), **d'activer le verrouillage de la session** de Windows ou de MacOS, de **télécharger les mises à jour** et **d'installer un antivirus et un pare-feu.**

Ce qu'il ne faut pas faire

- **Conserver des données sensibles sur sa messagerie mobile**
  Étant donné les capacités élevées de stockage des webmail, il peut être tentant d'y conserver des documents professionnels. Si l'appareil est volé ou perdu et qu'il est mal sécurisé, une personne malveillante (ou un concurrent…) pourra accéder à des informations confidentielles.

- **Ne pas mettre d'antivirus sur son smartphone**
  Un téléphone mobile est un PC de poche. Il peut donc être infecté par un virus. Il est donc important d'y installer un antivirus. Pas n'importe lequel. Sur le PlayStore d'Android, il y a en effet de multiples applications de sécurité qui ne sont pas développées par des éditeurs spécialisés. Ne vous fiez pas à leurs excellentes notes et **privilégiez les programmes proposés par les éditeurs connus sur Windows.**
  Sachez qu'il n'y a pas d'antivirus pour les iPhone. Cela ne signifie pas que ces smartphones ne peuvent pas être touchés par un virus. Mais Apple refuse ce type de solutions. Par ailleurs, sa politique d'intégration des applications est plus « stricte » que sur Android où les logiciels sont mis en ligne sans contrôle a priori.

Pour aller plus loin

Les obligations des employeurs

Différents textes de loi (dont l'article 34 de la loi du 6 janvier 1978) précisent que les entreprises ont des obligations en matière de sécurité informatique et notamment concernant les données à caractère personnel qu'elles traitent.

L'employeur étant maître de son Système d'Information (SI), il doit indiquer aux salariés désirant utiliser leur terminal qu'ils doivent respecter des règles très strictes en matière de sécurité (indiquées dans la charte informatique).

Pour vous accompagner dans la protection de vos postes de travail, découvrez l'offre Generali Protection Numérique
https://www.generali.fr/professionnel/assurance-cyber-risques/

Generali IARD. Société anonyme au capital de 94 630 300 euros. Entreprise régie par le Code des assurances - 552 062 663 RCS Paris
Siège social : 2 rue Pillet-Will - 75009 Paris

Informations non contractuelles à caractère publicitaire données à titre purement indicatif et dans un but pédagogique. La compagnie ne saurait être tenue responsable d'un préjudice d'aucune nature lié aux informations fournies. La contractualisation éventuelle avec le partenaire nommé ci-dessus se fait sous votre seule et unique responsabilité et ne saurait engager la responsabilité des sociétés Generali en France. Le choix de contractualiser ou pas avec ce partenaire relève de la gestion de votre entreprise et est sans incidence sur vos contrats d'assurance Generali qui demeure tiers à vos relations.

Le chiffrement des données

Derrière cette obscure expression se cache une solution efficace pour protéger vos données les plus sensibles. Elle vous évite le pire si vous perdez votre PC portable ou une clé USB.

Il n'est pas nécessaire d'être un crac du piratage pour récupérer des informations confidentielles sur une entreprise. Les salons professionnels font en effet le bonheur de concurrents un peu trop curieux. Il suffit de ramasser discrètement une clé USB ou de tomber par « hasard » sur un PC portable (ou un smartphone) pour mettre la main sur de précieux fichiers. La tâche est un jeu d'enfant si ces appareils mobiles ne sont pas sécurisés (voir notre fiche sur le BYOD) !

Par contre, cette opération devient un casse-tête si justement vous avez « chiffré » les documents sensibles qu'ils contiennent. Plus connue sous le terme de « cryptage », cette méthode consiste **à protéger vos fichiers en les rendant illisibles par toute personne n'ayant pas la clé dite de déchiffrement.** Sans le bon mot de passe, le contenu reste inaccessible.

Malheureusement, cette pratique est loin d'être généralisée. « La moitié des données stockées dans Google Drive sont partagées avec des utilisateurs situés à l'extérieur de l'entreprise », constate Bitglass, spécialiste américain de la protection totale des données, dans son étude parue en septembre 2017. Or, l'absence de chiffrement expose les entreprises à des fuites d'informations ou à des modifications malveillantes des données.

Pourquoi chiffrer ses documents et ses répertoires ?

- **Pour renforcer la sécurité de vos données**
  Le chiffrement assure la confidentialité de vos projets les plus importants pour votre activité économique, mais également la sécurité des données à caractère personnel que vous stockez en interne, chez un prestataire informatique ou dans le Cloud. Ce procédé cryptographique permet également d'assurer l'intégrité d'une information (elle ne peut pas être modifiée).

- **Pour limiter les effets négatifs d'une perte de données**
  Si une personne perd ou se fait voler son ordinateur portable lors d'un déplacement, les conséquences seront réduites, car ses dossiers importants seront chiffrés.

Le chiffrement des données : les principales mesures à prendre

- **Première mesure : chiffrer les données confidentielles**
  Tout répertoire comportant des informations sensibles ou à caractère personnel doit être chiffré. Cette technique permet en effet de restreindre les accès et de disposer de preuves en cas de fuite de données. Cette mesure concerne aussi bien les dossiers en interne ou stockés dans le Cloud.

- **Deuxième mesure : chiffrer des e-mails**
  Un courrier électronique non « crypté » c'est comme une carte postale : tout le monde peut le lire. Il est transmis en « clair ». En étant chiffré, un e-mail ne pourra être lu que par le destinataire disposant de la bonne clé. Attention, ce procédé « masque » le contenu et la pièce jointe, mais pas l'intitulé du message. Évitez d'indiquer des termes trop explicites… Cette technique permet aussi d'authentifier un e-mail en le signant.

- **Troisième mesure : chiffrer les appareils mobiles**
  Les salariés voyageant beaucoup à l'étranger ou se rendant dans des salons professionnels doivent posséder un PC portable et/ou un smartphone dont le disque dur est chiffré entièrement ou partiellement (seuls quelques dossiers sont protégés).

Ce qu'il ne faut pas faire

Utiliser n'importe quelle solution de chiffrement

Il existe de très nombreuses solutions cryptographiques. Mais **elles ne bénéficient pas toutes de vérifications assurées par des experts ou certifiées par l'ANSSI** (Agence nationale de la sécurité des systèmes d'information).

Par exemple, si vous envisagez d'utiliser le logiciel Truecrypt pour chiffrer des documents ou des dossiers, une seule version (la 6.0a) est reconnue par l'Agence de sécurité des systèmes d'information.

Pour aller plus loin

La signature électronique : la dématérialisation sécurisée

Adoptée par l'Assemblée nationale le 29 février 2000 (décrets d'application parus le 30 mars 2001), la signature électronique donne à un e-mail ou à un document électronique (contrats, mandats de prélèvement SEPA...) valeur de preuve au même titre que la feuille de papier. Mais l'article 1366 du Code civil français précise : « sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ». Vous devez donc vous adresser à un tiers de confiance (agréé et certifié) qui mettra à disposition les outils que vous utiliserez pour signer.

Votée en 2016, la loi Lemaire rend possible l'envoi d'un recommandé électronique à une administration (article 93, III). Cette disposition codifiée à l'article L. 112-15 du code des relations entre le public et l'administration a fait l'objet d'un décret d'application paru dans le Journal officiel du 23 décembre 2017.

LEXIQUE

Un système à clé publique (ou asymétrique) est un système cryptographique qui utilise deux clés, une clé publique et une clé secrète :

- **la clé publique :** librement publiable, elle est nécessaire à la mise en œuvre du chiffrement. Elle peut également servir à vérifier les signatures électroniques réalisées par la clé privée associée ;
- **la clé privée :** gardée confidentielle par son détenteur, elle sert à « signer » des données et à déchiffrer celles chiffrées par la clé publique associée.

Pour tout savoir sur votre protection numérique,
découvrez l'offre Generali Protection Numérique !

Generali IARD. Société anonyme au capital de 94 630 300 euros. Entreprise régie par le Code des assurances - 552 062 663 RCS Paris
Siège social : 2 rue Pillet-Will - 75009 Paris

Informations non contractuelles à caractère publicitaire données à titre purement indicatif et dans un but pédagogique. La compagnie ne saurait être tenue responsable d'un préjudice d'aucune nature lié aux informations fournies. La contractualisation éventuelle avec le partenaire nommé ci-dessus se fait sous votre seule et unique responsabilité et ne saurait engager la responsabilité des sociétés Generali en France. Le choix de contractualiser ou pas avec ce partenaire relève de la gestion de votre entreprise et est sans incidence sur vos contrats d'assurance Generali qui demeure tiers à vos relations.

Le contrat d'infogérance

Pour se focaliser sur leur cœur de métiers, les PME peuvent confier leur gestion informatique à des prestataires ou à des fournisseurs dans le Cloud. Mais cette délégation ne les dispense pas d'assurer la protection de leurs données.

À chacun son métier ! L'informatique est un poste complexe qui évolue rapidement au gré des innovations technologiques et des nouvelles contraintes réglementaires. Pour de nombreux chefs d'entreprise, c'est un casse-tête. D'où le recours à des contrats d'infogérance.

Ce terme regroupe :

- **la gestion d'infrastructures :** location de matériels, supervision d'équipements réseau, sauvegarde…
- **la gestion des applications :** activités de support fonctionnel, maintenance…
- **l'hébergement de service :** logiciel accessible en ligne (mode SaaS), c'est- à-dire dans le Cloud.

Le renforcement de ces droits accentue par conséquent les obligations de toutes les entreprises qui collectent, traitent et stockent des données personnelles.

Aujourd'hui, de nombreuses sociétés ne protègent pas assez leur réseau informatique, par manque de moyens ou de prise de conscience des risques numériques. Résultat, **onze incidents de cybersécurité seraient comptabilisés chaque jour en milieu professionnel en France,** d'après le cabinet de conseil PwC.

Face aux menaces numériques (phishing, infiltration sur le réseau informatique, virus…) pouvant entraîner une fuite de données - non seulement celles de vos clients, mais aussi celles de votre entreprise - vous devez renforcer votre niveau de sécurité.

Quels sont les risques ?

Faire appel à des prestataires vous permet de vous concentrer sur votre activité. Mais **ne confiez pas la gestion de votre parc informatique les yeux fermés.** Vous pouvez en effet être à la fois victime d'un piratage et être tenu pour… responsable.

En 2014, la CNIL a condamné Orange après deux intrusions dans ses fichiers clients et prospects (soit 1,3 million de données personnelles). Des pirates avaient profité d'une faille pour accéder à un serveur du prestataire secondaire (sous-traitant de rang 2). Pour la CNIL, l'opérateur aurait dû mener un audit de sécurité qui aurait permis de repérer cette vulnérabilité et de la corriger. Cette négligence lui a valu cette condamnation.

Cette affaire confirme que vous devez impérativement v**ous assurer qu'une sous-traitance en cascade ne conduira pas à rendre inefficaces les contraintes de sécurité** que vous avez exigées de votre prestataire de rang 1.
Ce dernier doit par ailleurs être lui aussi en conformité avec le Règlement européen sur la protection des données à caractère personnel (voir notre fiche sur le RGPD).

Le contrat infogérance : les principales mesures à prendre

- **Première mesure : précisez vos exigences de protection**
  En tant que client, vous devez préciser vos exigences en matière de sécurité, qui seront détaillées dans un **Plan d'assurance sécurité (PAS)**. Ce contrat peut mentionner : la réalisation d'audits de sécurité, la confidentialité des informations (voir notre annexe), etc.

- **Seconde mesure : indiquer les engagements du prestataire**
  Le contrat doit préciser la **liste exhaustive des équipements et des programmes** concernés par la maintenance informatique et l'assistance sur site. Soyez attentif à la gestion des mises à jour de l'antivirus et du pare-feu.

- **Troisième mesure : surveiller certains indicateurs-clés**
  Vous pouvez demander à tout moment un **extrait des journaux des événements** enregistrés par votre prestataire
  Soyez attentifs à certains indicateurs :
    - fréquence et suivi des mises à jour effectuées ;
    - durée d'indisponibilité maximum et suivi de ces indisponibilités ;
    - fréquence des sauvegardes et tests de restauration effectués. Les opérations de sauvegardes donnent lieu à un compte-rendu par messagerie avec indicateur de réussite ou d'échec.

• Quatrième mesure : sécuriser les transactions bancaires

Si vous avez une activité de e-commercant par exemple, vérifiez bien que vous êtes - ainsi que votre hébergeur de données bancaires - **en conformité avec le PCI DSS**. Cet acronyme anglais de « Payment Card Industry Data Security Standard » (ou « Standard de sécurité des données pour l'industrie des cartes de paiement ») s'applique à tout acteur qui stocke, traite ou transmet des données de cartes bancaires. Pour être conforme au PCI DSS tout acteur doit réaliser des tests de vulnérabilité trimestriels de ses points d'accès sur Internet.

Ce qu'il ne faut pas faire

Oublier d'imposer une clause de réversibilité

Ce n'est pas lorsque vous souhaiterez changer de prestataire que vous devrez vous préoccuper de la présence de cette clause. **Elle vous permet de récupérer en fin de contrat l'ensemble de vos données** confiées à un sous-traitant. Il est très important de préciser le format dans lequel devront être livrés vos fichiers.

En cas de différend, vous pourrez saisir les tribunaux. En novembre 2012, le parti politique UMP avait décidé de changer de prestataire pour la gestion et l'hébergement de ses données personnelles et donc de les récupérer auprès d'Oracle. « Ce dernier avait fait valoir à l'UMP qu'une fonction d'exportation de son logiciel Oracle CRM On Demand ne fonctionnait pas. En référé, le Président du Tribunal de Nanterre avait dit que ce n'était pas le problème de l'UMP. La juridiction a fait injonction à Oracle, sous astreinte de 5000 € par jour de retard, de se débrouiller pour que la réversibilité soit faite. Cette affaire confirme que la réversibilité est un enjeu qui est compris par les juges », a précisé Maître Olivier Iteanu au site spécialisé securiteoff.com.

Pour aller plus loin

Le Guide de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) :
« Maîtriser les risques de l'infogérance ».

LEXIQUE

Modèle de clause de confidentialité en cas de sous-traitance* :

Les supports informatiques et documents fournis par la société ..... [identité du responsable de traitement] à la société ..... [identité du prestataire] restent la propriété de la société ..... [identité du responsable de traitement].

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal), il en va de même pour toutes les données dont la société ..... [identité du prestataire] prend connaissance à l'occasion de l'exécution du présent contrat.

Conformément à l'article 34 de la loi informatique et libertés modifiée, la société..... [identité du prestataire] s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

La société ..... [identité du prestataire] s'engage donc à respecter les obligations suivantes et à les faire respecter par son personnel :

- ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la présente prestation prévue au contrat, l'accord préalable du maître du fichier est nécessaire ;
- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;
- ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- prendre toutes mesures de sécurité, notamment matérielles, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du présent contrat ;
- et en fin de contrat, à procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.

À ce titre, la société ..... [identité du prestataire] ne pourra sous-traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché sans l'accord préalable de la société ..... [identité du responsable de traitement].

La société ..... [identité du responsable de traitement] se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par la société ..... [identité du prestataire].

** Clause de confidentialité publiée par l'ANSSI et inspirée de celle proposée par la CNIL en cas de sous-traitance.*

Pour vous accompagner dans la prévention des cyber risques,
découvrez l'offre Generali Protection Numérique.

Generali IARD. Société anonyme au capital de 94 630 300 euros. Entreprise régie par le Code des assurances - 552 062 663 RCS Paris
Siège social : 2 rue Pillet-Will - 75009 Paris

Informations non contractuelles à caractère publicitaire données à titre purement indicatif et dans un but pédagogique. La compagnie ne saurait être tenue responsable d'un préjudice d'aucune nature lié aux informations fournies. La contractualisation éventuelle avec le partenaire nommé ci-dessus se fait sous votre seule et unique responsabilité et ne saurait engager la responsabilité des sociétés Generali en France. Le choix de contractualiser ou pas avec ce partenaire relève de la gestion de votre entreprise et est sans incidence sur vos contrats d'assurance Generali qui demeure tiers à vos relations.

GAMP0002FCA - Mars 2018