

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. N° d'identifiant unique ADEME FR232327_01NBYI.
Siège social : 89 rue Taitbout - 75009 Paris.
Société appartenant au Groupe Generali immatriculé sur le registre italien des groupes d'assurances sous le numéro 026.

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 demeurent tiers à vos relations.

