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.*

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.

SG2685MARK-25 - Décembre 2025 - Studio graphique