FICHE
#5

LA MISE EN CONFORMITÉ RGPD

IT Les services IT se trouvent **au coeur de la mise en place du RGPD** au sein des entreprises, en effet ce sont eux qui sont en charge de **mettre en place les solutions techniques et informatiques** afin de sécuriser les traitements et les données.

ACSEL
Le hub de la transformation digitale
LEXING
ALAIN BENSOUSSAN AVOCATS

1

SÉCURITÉ DES DONNÉES À CARACTÈRE PERSONNEL

Les données à caractère personnel doivent être traitées de manière à **garantir une sécurité et une confidentialité appropriées**, notamment pour :

PRÉVENIR L'ACCÈS NON AUTORISÉ

à ces données et à l'équipement utilisé pour leur traitement

ET L'UTILISATION NON AUTORISÉE

de ces données et de cet équipement.

Le service IT doit s'assurer que le réseau ou le système d'information est capable de résister, dans la limite du raisonnable, à des événements accidentels ou à des actions illégales ou malveillantes

qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données à caractère personnel conservées ou transmises.

ANALYSES D'IMPACT

Afin de garantir la sécurité, il convient de réaliser des analyses d'impact.

Ces analyses doivent permettre d'évaluer les risques *inhérents au traitement pour mettre en œuvre des mesures pour les atténuer, telles que le chiffrement, la pseudonymisation et des moyens techniques de résilience.*

Les risques *sont notamment la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral.*

FICHE
#5

LA MISE EN CONFORMITÉ RGPD

IT Les services IT se trouvent **au coeur de la mise en place du RGPD** au sein des entreprises, en effet ce sont eux qui sont en charge de **mettre en place les solutions techniques et informatiques** afin de sécuriser les traitements et les données.

ACSEL
Le hub de la transformation digitale
LEXING
ALAIN BENSOUSSAN AVOCATS

2

VIOLATION DES DONNÉES

Une violation de données à caractère personnel est une violation de la sécurité entraînant, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données.

72h

En cas de violation de données à caractère personnel il convient de notifier la violation en question à la Cnil dans les meilleurs délais et, si possible, **72 heures** au plus tard après en avoir pris connaissance. La notification doit :

CNIL

> Décrire la nature de la violation de données à caractère personnel

Y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés

> Communiquer le nom et les coordonnées du délégué à la protection des données

ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues

> Décrire les conséquences probables

de la violation de données à caractère personnel

> Décrire les mesures prises ou que le responsable du traitement propose de prendre

pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives

3

SOUS-TRAITANT

CONTRAT DE PRESTATION

En cas de recours à un sous-traitant, **le contrat de prestation doit définir les garanties** que le sous-traitant présente quant à la **mise en œuvre de mesures techniques et organisationnelles appropriées.**

NIVEAU DE SÉCURITÉ

Le sous-traitant doit prendre **toutes les mesures afin de garantir un niveau de sécurité adapté au risque** comme cela a été décrit dans les paragraphes précédents.