Votre site internet à votre image

Protection des données (RGPD)

Règlement européen sur la protection des données.

Ce dernier, applicable aux états membres quel que soit le secteur d'activité, est par nature générique.
Il est complété de guidelines issues du G29 (groupement européen des autorités de contrôle qui devient le Comité Européen de la Protection des Données) qui visent à préciser certains articles du règlement.
Les dernières guidelines n'ont été publiées que très récemment, en conséquence, lors de récentes discussions de place, la CNIL a précisé que les nouveaux principes du règlement ne seraient contrôlés qu'à partir de 2019.
Eponim veillera à ce que ces données soient à tout moment et en tous lieux sécurisées contre les risques de perte, de vol, de divulgation ou contre toute autre compromission.

Définition de la donnée à caractère personnel :

Toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement.
Par exemple : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, plaque d'immatriculation etc.
Pour que ces données ne soient plus considérées comme personnelles, elles doivent être rendues anonymes de manière à rendre impossible toute identification de la personne concernée : noms masqués, visages floutés, etc.
Attention : s'il est possible par recoupement de plusieurs informations (âge, sexe, ville, diplôme, etc.) ou par l'utilisation de moyens techniques divers, d'identifier une personne, les données sont toujours considérées comme personnelles.
Certaines données sont considérées comme sensibles et leur accès doit être encore plus restreint (ex: données de santé).

Sur l'envoi de newsletters :

Dans le cadre d'un envoi de newsletter (échanges commerciaux, notification d'offres promotionnelles …) Eponim s'engage à effectuer ces envois qu'aux seules personnes qui en auront expressément exprimer leur accord préalable.
Les adresses e-mail des destinataires ne sauront en aucun cas données, vendues ou cédées à des tiers personnes ou sociétés.
Chaque personne dispose d'un droit sur ses données (adresses e-mail, nom / prénoms et cordonnées) et peut faire valoir son droit à faire supprimer ces données dans les bases par l'envoi d'un e-mail à contact@eponim.com

Sur l'obligation de sécurité des données :

Le règlement européen précise qu'afin de garantir la sécurité, l'entreprise doit évaluer les risques et mettre en œuvre des mesures pour les atténuer. Ces mesures devraient assurer un niveau de sécurité approprié, y compris la confidentialité, ...
Dans le cadre de l'évaluation des risques pour la sécurité des données, il convient de prendre en compte les risques tels que la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non

autorisé à de telles données, de manière accidentelle ou illicite.
Ainsi EPONIM garantit que l'accès à la donnée est limitée aux personnes qui en ont STRICTEMENT besoin dans le cadre de leurs activités.
Aucune ressource n’est ouverte à l'ensemble des collaborateurs ou à des tiers.
Les données de nos clients, sont stockées exclusivement en base de données, dont l’accès est sécurisé par notre hébergeur Datacampus (site internet : www.datacampus.fr).
Parallèlement, dans le but de leur traitement, les données de nos clients sont également stockées sur des fichiers informatiques (Traitement de texte, tableur …) eux mêmes stockées sur nos postes de travail respectifs, protégés par des mots de passe et donc inaccessibles de l'extérieur ou par des tiers personnes.

Rappel des sanctions en cas de manquement à ces règles :

Avec le règlement européen, elles peuvent s'élever à 4% du CA du groupe maximum, en cas de manquement à l'obligation de sécurité.
De plus, en cas de fuite de données, depuis le 25 mai, Eponim le notifiera à la CNIL sous 72 heures ainsi qu'aux personnes concernées.

Pour minimiser les risques d’accès aux données à des tiers non autorisés, la possibilité de consulter ou de manipuler des données de production doit être encadrée et les accès tracés. Avec notamment la signature d’un contrat de confidentialité entre les parties.