PROTECTION DES DONNÉES PERSONNELLES - RGPD

LA MALLETTE DU DIRIGEANT

HORESTO FORMATION SARL - LANAZIA - ZONE D'ACTIVITÉS LARRE LORE
314, RUE LARRE LORE - 64310 ASCAIN - SIRET : 80475775500017 - NAF : 7022 Z
N° Déclaration d'Activité : 72640374464 - N° TVA INTRACOMMUNAUTAIRE : 22804757755
TÉLÉPHONE : 05.59.24.36.13 - MAIL : CONTACT@HORESTO-FORMATION.FR

PLAN

1. Comprendre le RGPD
2. Comprendre les nouveaux principes de protection des données
3. Définir un plan d’actions pour se mettre en conformité

COMPRENDRE LE RGPD

HORESTO FORMATION SARL - LANAZIA - ZONE D'ACTIVITÉS LARRE LORE
314, RUE LARRE LORE - 64310 ASCAIN - SIRET : 80475775500017 - NAF : 7022 Z
N° Déclaration d'Activité : 72640374464 - N° TVA INTRACOMMUNAUTAIRE : 22804757755
TÉLÉPHONE : 05.59.24.36.13 - MAIL : CONTACT@HORESTO-FORMATION.FR

COMPRENDRE LE RGPD

- **Qu'est-ce que le RGPD ?**
  - *"Le Règlement général sur la protection des données (RGPD ou GDPR, pour General data protection regulation en anglais) est le nouveau cadre européen concernant le traitement et la circulation des données à caractère personnel, ces éléments sur lesquels les entreprises s'appuient pour proposer des services et des produits. Ce texte couvre l'ensemble des résidents de l'Union européenne."* (Source : *Numerama*)

COMPRENDRE LE RGPD

- **Qu'est-ce que sont les "Données à Caractère Personnel" ?**
  - *"Une donnée personnelle (ou donnée à caractère personnel) est une information qui permet d'identifier une personne physique, directement ou indirectement. Il peut s'agir d'un nom, d'une photographie, d'une adresse IP, d'un numéro de téléphone, d'un identifiant de connexion informatique, d'une adresse postale, d'une empreinte, d'un enregistrement vocal, d'un numéro de sécurité sociale, d'un mail, etc."* (Source : *Numerama*)

COMPRENDRE LE RGPD

- **Y a-t-il des données personnelles plus sensibles que d'autres ?**
  - Certaines données sont sensibles, car elles touchent à des informations qui peuvent donner lieu à de la discrimination ou des préjugés :
    - Une opinion politique, une sensibilité religieuse, un engagement syndical, une appartenance ethnique, une orientation sexuelle, une situation médicale ou des idées philosophiques sont des données sensibles. Elles ont un cadre particulier, qui interdit toute collecte préalable sans consentement écrit, clair et explicite, et pour des cas précis, validés par la CNIL et dont l'intérêt public est avéré.

COMPRENDRE LE RGPD

- **Quels sont les objectifs du RGPD ?**
  - *"L'objectif du RGPD est d'être le nouveau texte de référence dans l'Union européenne au sujet des données personnelles, en remplaçant une directive datant de 1995. Une réforme de la législation européenne apparaissait nécessaire au regard de sa vétusté, révélée par l'explosion du numérique, l'apparition de nouveaux usages et la mise en place de nouveaux modèles économiques."* (Source : *Numerama*)
  - Il s'agit aussi d'harmoniser le panorama juridique européen en matière de protection des données personnelles, afin qu'il n'y ait qu'un seul et même cadre qui s'applique parmi l'ensemble des États membres.

COMPRENDRE LE RGPD

- **Qui est concerné ?**
  - *"Toute entité manipulant des données personnelles concernant des Européens doit se conformer, qu'il s'agisse d'une entreprise, d'un sous-traitant ou même d'une association. Attention : le texte ne s'applique pas qu'aux organisations établies sur le territoire du Vieux Continent. Un groupe américain, japonais ou chinois qui collecte et mouline des données personnelles européennes doit aussi s'y conformer."* (Source : *Numerama*)

  - Pour simplifier : Vous tous ! (Ou presque)

COMPRENDRE LE RGPD

- **Qu'est-ce que cela implique pour l'entreprise ?**
  - Il est **important**, voir urgent si ce n'est pas encore fait, de vous mettre en règle avec le RGPD !
  - Dans le cas contraire, en cas de contrôl administratif ou de défaillance dans votre système de données, vous risquez lourdes amendes et d'importantes retombées.

COMPRENDRE LE RGPD

- **Qu'est-ce que cela implique pour l'entreprise ?**
  - L'entreprise doit mettre en place un système de collecte des données personnelles des utilisateurs conformes au RGPD.
  - L'entreprise doit donc se former afin de mettre en place un tel système.
  - L'entreprise doit obtenir le consentement de ses utilisateurs, ce qui modifie par la suite le traitement et l'utilisation de ces données personnelles.
  - L'entreprise ne peut pas faire ce qu'elle veut de ces données personnelles. Elle doit les utiliser dans le cadre de la loi RGPD

COMPRENDRE LES NOUVEAUX PRINCIPES DE PROTECTION DES DONNÉES

HORESTO FORMATION SARL - LANAZIA - ZONE D'ACTIVITÉS LARRE LORE
314, RUE LARRE LORE - 64310 ASCAIN - SIRET : 80475775500017 - NAF : 7022 Z
N° Déclaration d'Activité : 72640374464 - N° TVA INTRACOMMUNAUTAIRE : 22804757755
TÉLÉPHONE : 05.59.24.36.13 - MAIL : CONTACT@HORESTO-FORMATION.FR

COMPRENDRE LES NOUVEAUX PRINCIPES DE PROTECTION DES DONNÉES

- **Quelles nouveautés sont introduites par le RGPD ?**
  - La notion la plus fondamentale à retenir est que la responsabilité de la mise en œuvre de la protection des données **repose sur l'employeur** puisqu'il sera considéré comme le responsable du traitement (*article 4*).

  - Il revient donc à l'employeur de s'assurer que les outils qu'il utilise sont en conformité avec la réglementation sur les données personnelles. Ceci rentre dans la notion de *privacy by design* instituée par l'article 25 disposant que le responsable du traitement (employeur) : «*met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées*».

COMPRENDRE LES NOUVEAUX PRINCIPES DE PROTECTION DES DONNÉES

- **Quelles nouveautés sont introduites par le RGPD ?**
  - L'employeur à l'obligation de :
    - Pouvoir rectifier ou effacer des données inexactes, également de les supprimer de manière définitive.
    - Garantir la sécurité des données.
    - Pouvoir composer avec les demandes des salariés (rectification, suppression, etc).
    - Tenir un registre des données personnelles de ses employés et de ses utilisateurs collectées. Ce registre doit être consultable par la **CNIL** à tout moment et son contenu est développé par ledit article. Il s'agit, en vérité, de cartographier l'ensemble des traitements effectués au sein de l'entreprise.

COMPRENDRE LES NOUVEAUX PRINCIPES DE PROTECTION DES DONNÉES

- **Quelles nouveautés sont introduites par le RGPD ?**
  - En cas de violation des données personnelles, à moins qu'elle ne comporte pas un risque pour les droits et libertés des personnes physiques, une double obligation de notification s'impose à l'employeur (**article 33** et **article 34**).
    - À la CNIL (l'autorité compétente) : dans un délai de soixante-douze heures.
    - Au salarié (la personne concernée) : dans les meilleurs délais.

  - Une violation s'analyse comme «*entraînant de manière accidentelle ou illicite, la destruction, la perte, 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*» (**article 4.12**). Cette obligation suppose la création d'une procédure de notification effective.

COMPRENDRE LES NOUVEAUX PRINCIPES DE PROTECTION DES DONNÉES

- **Quelles nouveautés sont introduites par le RGPD ?**
  - L'employeur ne doit pas collectées des données trop personnelles de l'employé ou du futur employé.
    - Un exemple précis peut s'effectuer au niveau du recrutement ; demander un numéro de sécurité sociale ou des précisions sur la situation matrimoniale d'un candidat n'est pas pertinent au regard de la finalité du traitement.
  - L'employeur n'a pas le droit de nous forcer à communiquer sur une plateforme dont il ne contrôle pas la collecte des données.
    - Exemple : Un employeur qui nous force à avoir des communications professionnelles sur WhatsApp, Facebook ou autre, est exposé à amende importante.

COMPRENDRE LES NOUVEAUX PRINCIPES DE PROTECTION DES DONNÉES

- **Quelles nouveautés sont introduites par le RGPD ?**
  - Lorsque c'est prévu par le RGPD, l'entreprise devra également désigner un « **Data Protection Officer** » (DPO), c'est-à-dire un délégué à la protection des données personnelles. Cette désignation est obligatoire dans plusieurs cas : lorsque le traitement des données est effectué par une autorité ou un organisme public, lorsque les données font l'objet d'un suivi régulier ou lorsqu'il s'agit de données sensibles.

COMPRENDRE LES NOUVEAUX PRINCIPES DE PROTECTION DES DONNÉES

- **Quelles nouveautés pour l'utilisateur ?**
  - Du point de vue de l'internaute, le RGPD met en place ou conforte un certain nombre de protections. Il faut par exemple que les entreprises récoltent au préalable un consentement écrit, clair et explicite de l'internaute avant tout traitement de données personnelles, ou qu'elles s'assurent que les enfants en-dessous d'un certain âge aient bien reçu l'aval de leurs parents avant de s'inscrire sur un réseau social.

COMPRENDRE LES NOUVEAUX PRINCIPES DE PROTECTION DES DONNÉES

- **Quelles nouveautés pour l'utilisateur ?**
  - Le RGPD inclut aussi une reconnaissance d'un droit à l'oubli pour obtenir le retrait ou l'effacement de données personnelles en cas d'atteinte à la vie privée, le droit à la portabilité des données, pour pouvoir passer d'un réseau social à l'autre, d'un FAI à l'autre ou d'un site de streaming à l'autre sans perdre ses informations, le droit d'être informé en cas de piratage des données.

  - Les internautes peuvent aussi être défendus par les associations dans le cadre d'une action de groupe en vue de faire cesser la partie illicite d'un traitement de données.

COMPRENDRE LES NOUVEAUX PRINCIPES DE PROTECTION DES DONNÉES

- **Quels risques juridiques et les sanctions qui pèsent sur l'entreprise ?**
  - Les organisations ont tout intérêt à respecter à la lettre le RGPD car les plafonds des sanctions sont particulièrement élevés : en cas d'infraction, des amendes jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent sont prévues pour l'organisme fautif, sachant que c'est le montant le plus élevé qui est retenu entre les deux cas de figure.

COMPRENDRE LES NOUVEAUX PRINCIPES DE PROTECTION DES DONNÉES

- **Quels risques juridiques et les sanctions qui pèsent sur l'entreprise ?**
  - Il faut imaginer ce que cela peut représenter pour des géants du net si une procédure est lancée contre eux. L'amende pourrait atteindre des dizaines ou des centaines de millions de dollars, voire davantage. Il convient aussi de noter qu'une société doit veiller à ce que son sous-traitant reste bien dans les clous de la loi, sous peine d'en subir les conséquences, du fait de sa qualité de responsable du traitement.

COMPRENDRE LES NOUVEAUX PRINCIPES DE PROTECTION DES DONNÉES

- **Quels risques juridiques et les sanctions qui pèsent sur l'entreprise ?**
  - Cela étant, les multinationales ne sont pas nécessairement les plus exposées : si ce sont elles qui risquent les amendes les plus fortes, elles ont des détachements de juristes et d'experts qui travaillent déjà à plein temps depuis des mois pour être absolument dans les clous du RGPD. Le risque est en revanche plus grand pour les entités plus petites, comme une TPE, une PME ou une association.

COMPRENDRE LES NOUVEAUX PRINCIPES DE PROTECTION DES DONNÉES

- **Pour se conformer à la nouvelle réglementation, les entreprises doivent également apporter certaines garanties en termes de sécurité et d'utilisation des données sur plusieurs points :**
  - Conservation et sécurisation des données
  - Respect de la protection des données
  - Suppression des données une fois l'autorisation de traitement expiré (13 mois pour le consentement pour les cookies par exemple)
  - Droit d'information et de déréférencement
  - Droit à la portabilité des données
  - Enfin, les entreprises doivent pouvoir prouver la conformité à tout moment.

DÉFINIR UN PLAN D'ACTIONS POUR SE METTRE EN CONFORMITÉ

HORESTO FORMATION SARL - LANAZIA - ZONE D'ACTIVITÉS LARRE LORE
314, RUE LARRE LORE - 64310 ASCAIN - SIRET : 80475775500017 - NAF : 7022 Z
N° Déclaration d'Activité : 72640374464 - N° TVA INTRACOMMUNAUTAIRE : 22804757755
TÉLÉPHONE : 05.59.24.36.13 - MAIL : CONTACT@HORESTO-FORMATION.FR

DÉFINIR UN PLAN D'ACTIONS POUR SE METTRE EN CONFORMITÉ

- 1. **Recensez vos fichiers**
  - Le registre listant vos traitements de données vous permettra d'avoir une vision d'ensemble. Identifiez les activités principales de votre entreprise qui nécessitent la collecte et le traitement de données (exemples : recrutement, gestion de la paie, formation, gestion des badges et des accès, statistiques de ventes, gestion des clients prospects, etc.).

DÉFINIR UN PLAN D'ACTIONS POUR SE METTRE EN CONFORMITÉ

- Dans votre registre, créez une fiche pour chaque activité recensée, en précisant :
  - **L'objectif poursuivi** (la finalité - exemple : la fidélisation client)
  - **Les catégories de données utilisées** (exemple pour la paie : nom, prénom, date de naissance, salaire, etc.)
  - **Qui a accès aux données ?** (le destinataire - exemple : service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs)
  - **La durée de conservation de ces données** (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive)

DÉFINIR UN PLAN D'ACTIONS POUR SE METTRE EN CONFORMITÉ

- 2. **Faites le tri dans vos données**
  - Pour chaque fiche de registre créée, vérifiez :
    - Que les données que vous traitez sont nécessaires à vos activités (par exemple, il n'est pas utile de savoir si vos salariés ont des enfants, si vous n'offrez aucun service ou rémunération attachée à cette caractéristique)
    - Que vous ne traitez aucune donnée dite « sensible » ou, si c'est le cas, que vous avez bien le droit de les traiter.
    - Que seules les personnes habilitées ont accès aux données dont elles ont besoin.
    - Que vous ne conservez pas vos données au-delà de ce qui est nécessaire.

DÉFINIR UN PLAN D'ACTIONS POUR SE METTRE EN CONFORMITÉ

- À cette occasion, améliorez vos pratiques !
  - Minimisez la collecte de données, en éliminant de vos formulaires de collecte et vos bases de données toutes les informations inutiles. Redéfinissez qui doit pouvoir accéder à quelles données dans votre entreprise. Pensez à poser des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans vos applications.

DÉFINIR UN PLAN D'ACTIONS POUR SE METTRE EN CONFORMITÉ

- 3. **Respectez les droits des personnes**
  - À chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information.Vérifiez que l'information comporte notamment les éléments suivants :
    - Pourquoi vous collectez les données (« la finalité » ; par exemple pour gérer l'achat en ligne du consommateur)
    - Ce qui vous autorise à traiter ces données (le « fondement juridique » : il peut s'agir du consentement de la personne concernée, de l'exécution d'un contrat, du respect d'une obligation légale qui s'impose à vous, de votre « intérêt légitime »)

DÉFINIR UN PLAN D'ACTIONS POUR SE METTRE EN CONFORMITÉ

- 3. **Respectez les droits des personnes**
  - À chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information.Vérifiez que l'information comporte notamment les éléments suivants :
    - Qui a accès aux données (indiquez des catégories : les services internes compétents, un prestataire, etc.)
    - Combien de temps vous les conservez (exemple : « 5 ans après la fin de la relation contractuelle »)
    - Les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (via leur espace personnel sur votre site internet, par un message sur une adresse email dédiée, par un courrier postal à un service identifié)
    - Si vous transférez des données hors de l'Union européenne(précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données).

DÉFINIR UN PLAN D'ACTIONS POUR SE METTRE EN CONFORMITÉ

- 3. **Respectez les droits des personnes**
  - Pour éviter des mentions trop longues au niveau d'un formulaire en ligne, vous pouvez par exemple, donner un premier niveau d'information en fin de formulaire et renvoyer à une politique de confidentialité/page vie privée sur votre site internet.

DÉFINIR UN PLAN D'ACTIONS POUR SE METTRE EN CONFORMITÉ

- 3. **Respectez les droits des personnes**
  - Permettez aux personnes d'exercer facilement leurs droits
    - Les personnes dont vous traitez les données (clients, collaborateurs, prestataires, etc.) ont des droits sur leurs données, qui sont d'ailleurs renforcés par le RGPD : droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement.
    - Vous devez leur donner les moyens d'exercer effectivement leurs droits. Si vous disposez d'un site web, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée. Si vous proposez un compte en ligne, donnez à vos clients la possibilité d'exercer leurs droits à partir de leur compte.Mettez en place un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts (1 mois au maximum).

DÉFINIR UN PLAN D'ACTIONS POUR SE METTRE EN CONFORMITÉ

- 4. **Sécurisez vos données**
  - Garantissez l'intégrité de votre patrimoine de données en minimisant les risques de pertes de données ou de piratage.
  - Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas d'incident.
  - Différentes actions doivent être mises en place : mises à jour de vos antivirus et logiciels, changement régulier des mots de passe et utilisation de mots de passe complexes, ou chiffrement de vos données dans certaines situations. En cas de perte ou vol d'un outil informatique,il sera plus difficile pour un tiers d'y accéder.

DÉFINIR UN PLAN D'ACTIONS POUR SE METTRE EN CONFORMITÉ

- 4. **Sécurisez vos données**
  - Les failles de sécurité ont également des conséquences pour ceux qui vous ont confié des données personnelles. Ayez à l'esprit les conséquences pour les personnes de la perte, la divulgation, la modification non souhaitée de leurs données, et prenez les mesures nécessaires pour minimiser ces risques
  - Exemple :
    - Vous êtes restaurateur et vous livrez à domicile. Vos clients vous communiquent leur adresse précise et le code d'entrée de leur immeuble. Si ces informations sont piratées ou perdues, elles peuvent être utilisées pour s'introduire frauduleusement au domicile de votre client. Conséquence désastreuse pour vos clients, mais aussi pour vous.

CONCLUSION

HORESTO FORMATION

WWW.HORESTO-FORMATION.FR

ÉTUDES DE CAS DES STAGIAIRES

HORESTO FORMATION SARL - LANAZIA - ZONE D'ACTIVITÉS LARRE LORE
314, RUE LARRE LORE - 64310 ASCAIN - SIRET : 80475775500017 - NAF : 7022 Z
N° Déclaration d'Activité : 72640374464 - N° TVA INTRACOMMUNAUTAIRE : 22804757755
TÉLÉPHONE : 05.59.24.36.13 - MAIL : CONTACT@HORESTO-FORMATION.FR