RGPD

Règlement Général Protection des Données

PRESTATIONS RGPD 2020

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
RGPD (source CNIL) (lien vers le règlement intégral)

1-AUDIT DE MISE EN CONFORMITE RGPD (Registres de traitements)

Actions à mener pour une mise en conformité RGPD ? *(Ces actions doivent perdurer dans le temps pour être efficaces).*

1-1Registre de traitement

Le registre listant vos traitements de données vous permettra d'avoir une vision d'ensemble.

Identifiez ou cartographiez les activités principales de votre entreprise qui nécessitent la collecte et le traitement de données (exemples : recrutement, gestion de la paye, formation, gestion des badges et des accès, statistiques de ventes, gestion des clients prospects, etc.).

Dans votre registre, créez une fiche (sous-registre) pour chaque activité ou traitement recensés, en précisant :

- **Les acteurs :** le(s) responsable de traitement (l'entreprise), les sous-traitants.
- **Les catégories de données utilisées** (exemple pour la paie : nom, prénom, date de naissance, salaire, etc.).
- **Descriptif du risque** : (vol, piratage, pertes de données).
- **L'objectif poursuivi ou** la finalité (exemple : Gestion du personnel, obligations légales, paiement des salaires).
- **Déterminer le flux de données** : (exemples : PC, disques dur externes, cloud, supports papier).
- **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).
- **Données nécessitant** la mise en place d'une analyse d'impact (PIA).
- **Mesures de sécurité** : Mises en œuvre et préventions pour protéger les données à caractère personnel.
- **Identification et priorisation des actions à mener**.

Le registre est placé sous la responsabilité du dirigeant de l'entreprise. Pour avoir un registre exhaustif et à jour, il faut en discuter et être en contact avec toutes les personnes de l'entreprise susceptibles de traiter des données personnelles.

En constituant votre registre, vous aurez une vision d'ensemble sur vos traitements de données.

1-2-Documentation

Vous devez constituer une documentation attestant de la conformité au RGPD.

Pour prouver la conformité au règlement, il est nécessaire de constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

LA DOCUMENTATION SUR VOS TRAITEMENTS DE DONNÉES PERSONNELLES

- **Le registre des traitements** (pour les responsables de traitements) ou des catégories d'activités de traitements (pour les sous-traitants).
- **Les analyses d'impact sur la protection des données** (PIA) pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes.
- **L'encadrement des transferts** de données hors de l'Union européenne (notamment, les clauses contractuelles types, les BCR et certifications)

L'INFORMATION DES PERSONNES

- **Les mentions d'information**
- Les modèles de **recueil du consentement des personnes concernées**,
- Les procédures mises en place pour **l'exercice des droits**

LES CONTRATS QUI DÉFINISSENT LES RÔLES ET LES RESPONSABILITÉS DES ACTEURS

- **Les contrats avec les sous-traitants**
- Les procédures internes **en cas de violations de données**
- Les preuves que les personnes concernées **ont donné leur consentement** lorsque le traitement de leurs données repose sur cette base.

1-3-Registre sous-traitant

En tant que sous-traitant, vous devez tenir un registre des catégories d'activités de traitement que vous effectuez pour le compte de vos clients. Ce registre doit être tenu par écrit et contenir :

- Le nom et les coordonnées de chaque client pour le compte duquel vous traitez des données.
- Le nom et les coordonnées de chaque sous-traitant ultérieur, le cas échéant.
- Le nom et les coordonnées du délégué à la protection des données, le cas échéant.

- Les catégories de traitements effectués pour le compte de chaque client.
- Les transferts de données hors UE que vous effectuez pour le compte de vos clients, le cas échéant.

- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles que vous mettez en place.

2-Charte informatique

(Elle définit les règles de sécurité, d'utilisation et de protection informatiques dans l'entreprise, elle n'est pas nécessairement liée à un site internet)

Le contenu d'une charte est libre, à la différence de celui du règlement intérieur qui est juridiquement encadré.

Dans le domaine informatique, le règlement intérieur contient souvent quelques dispositions relatives à l'utilisation par les salariés du matériel informatique ou des nouvelles technologies appartenant à l'entreprise à des fins personnelles.

Une charte informatique, annexée au règlement intérieur et régulièrement déposée et communiquée, permet de compléter les règles fixées par le règlement intérieur dans ce domaine, en fixant un cadre adapté à l'utilisation par les salariés des nouvelles technologies de l'information et de la communication (NTIC) : ordinateur, logiciel, messagerie électronique, Internet, Intranet.

Attention : Une charte ne peut pas porter atteinte à des dispositions impératives et d'ordre public. Ainsi par exemple, elle ne peut pas porter une atteinte injustifiée aux droits de la personne ou aux libertés individuelles et collectives.

L'employeur a intérêt à annexer la Charte informatique au Règlement Intérieur afin de lui donner une force contraignante.

Cette charte doit à minima contenir les éléments suivants :

- Rappel des règles de protection des données et les sanctions encourues en cas de non-respect de celles-ci ;
- Le champ d'application de la charte qui inclut notamment :

  -> Les modalités d'intervention des équipes chargées de la gestion des ressources informatiques de l'organisme ;
  -> Les moyens d'authentification utilisés par l'organisme ;
  -> Les règles de sécurité auxquelles les utilisateurs doivent se conformer, ce qui doit inclure notamment de :

  - Signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ;
  - Ne jamais confier son identifiant/mot de passe à un tier ;
  - Ne pas installer, copier, modifier, détruire des logiciels sans autorisation ;
  - Verrouiller son ordinateur dès que l'on quitte son poste de travail ;
  - Ne pas accéder, tenter d'accéder ou supprimer des informations si cela ne relève pas des tâches incombant à l'utilisateur ;
  - Respecter les procédures préalablement définies par l'organisme afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité

La Charte Informatique doit préciser les modalités d'utilisation des moyens informatiques et de télécommunications mis à disposition comme :

- Le poste de travail ;
- Les équipements nomades (notamment dans le cadre du télétravail) ;
- Les espaces de stockage individuels ;
- Les réseaux sociaux ;
- Les conditions d'utilisation des dispositifs personnels ;
- L'internet ;
- La messagerie électronique
- La téléphonie

La Charte Informatique doit préciser les conditions d'administration du système d'information et l'existence, le cas échéant de :

- Systèmes automatiques de filtrage ;
- Systèmes automatiques de traçabilité ;
- Gestion du poste de travail

Enfin, la Charte Informatique doit définir les responsabilité et sanctions encourues en cas de non-respect de cette dernière.

3-Avenant au contrat de travail

(RGPD collecte des données personnelles des salariés et Engagement de confidentialité des salariés)

Le Règlement Européen sur la Protection des Données Personnelles renforce le droit des salariés.

Il est par conséquent impératif pour l'employeur de mettre à jour les contrats de travail sur deux points :

- **La définition des missions du salarié** pour lesquelles ce dernier va traiter ou collecter des données personnelles ;
- **La définition des nouveaux droits du salarié** (droit d'accès, rectification, etc…).

L'avenant au contrat doit prévoir :

3-1Collecte des données personnelles des salariés

- La durée de conservation des données personnelles du salarié doit être mentionnée. Cette durée peut être précise (3 ans) ou liée à la survenue d'un évènement (licenciement, etc…) ;
- Les mesures de sécurité mises en place pour garantir la confidentialité des données ;
- Les destinataires des données ;
- L'identité du responsable de traitement ;
- Les coordonnées du responsable de traitement.

En cas d'une demande d'un salarié relative aux articles 15 à 22 du Règlement Européen sur la Protection des Données Personnelles (droit d'accès, de rectification, d'effacement, de limitation, de portabilité ou d'opposition des données), le responsable de traitement (l'employeur) doit répondre à cette demande dans les meilleurs délais et en tout état de cause dans un **délai d'un mois**.

A noter que ce délai peut être **prolongé de deux mois**, compte tenu de la complexité du nombre de demandes (article 12-3 du Règlement Européen sur la Protection des Données Personnelles).

3-2Engagement de confidentialité des salariés

L'employeur devant prendre toutes les mesures nécessaires pour sécuriser la collecte et le traitement des données personnelles, il est impératif de sensibiliser les salariés amenés à traiter ou collecter lesdites données.

A ce titre, **la signature d'un engagement de confidentialité** pour les personnes ayant vocation à manipuler des données à caractère personnel est indispensable.

Si cet engagement sensibilisera les salariés concernés par la manipulation de données, il est important de préciser ce que doit faire ou ne pas faire le salarié (utilisation des données uniquement dans le cadre de ses missions/Ne divulguer ses données qu'aux seules personnes habilitées/Ne pas faire de copies de ces données/Etc…).

Cet engagement doit **être signé par le salarié en 2 exemplaires** (un pour l'employeur et un pour le salarié).

Il sera **annexé à la documentation RGPD** visant à justifier de toutes les démarches de prévention mises en œuvre.

4-Politique de Confidentialité (site internet)

La Politique de Confidentialité d'un site internet doit comporter les dispositions suivantes pour satisfaire au Règlement Européen sur la Protection des Données :

- Définition d'une donnée à caractère personnel ;
- Identité du responsable de traitement ;
- Objectif de la Politique de Confidentialité ;
- Les données collectées ;
- La durée de conservation des données ;
- La finalité de la collecte et du traitement des données ;
- Le destinataire des données collectées ou traitées ;
- La base juridique que laquelle se fonde le traitement ou la collecte de données ;
- Les éventuels transferts de données au sein ou en dehors de l'Union Européenne ;
- Les droits liés aux données personnelles ;
- La confidentialité d'un identifiant ou mot de passe (le cas échéant) ;
- Les mesures de sécurité mises en place pour garantir la sécurité des données ;
- La modification de la Politique de Confidentialité ;
- Une rubrique contacts.

5-Conditions générales de vente

Pour être en conformité avec le Règlement Européen sur la Protection des Données, les Conditions Générales de Vente doivent disposer d'une clause spécifique comprenant :

- Identité de la société et du responsable de traitement ;
- La finalité et la base juridique du traitement de données ;
- L'éventuelle transmission des données à un sous-traitant/tiers ;

- Le pays vers lequel sont transférées les données ;
- La durée de conservation des données ;
- La mention du droit d'accès, de rectification, de limitation, et d'effacement des données ;
- La possibilité de s'opposer au traitement et à la portabilité des données ;
- La possibilité de retirer son consentement au traitement effectué ;
- La possibilité d'effectuer une réclamation auprès de l'autorité de contrôle.

6-Conditions générales d'utilisation

(Données à caractère personnel site internet)

Le Règlement Européen sur la Protection des Données impose une mise à jour des sites internet.

A ce titre, les mentions égales et Conditions Générales d'utilisation doivent désormais intégrer une clause RGPD qui doit notamment préciser :

- Le renvoi à une Politique de Confidentialité (via un lien hypertexte) ;
- Le droit d'accès, rectification, effacement, portabilité de vos données ou limitation du traitement de ces dernières ;
- Identité et coordonnées du responsable de traitement.

7-Clauses contractuelles de sous-traitance

Lors de l'utilisation d'un sous-traitant, le Règlement Européen sur la Protection des Données impose aux entreprises dans son article 28-1 de faire « …uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée ».

Par conséquent, chaque entreprise doit veiller à mettre à jour les contrats passés avec ses sous-traitants afin de se mettre en conformité avec le Règlement Européen.

A noter de ces contrats constitueront une partie de la documentation RGPD que doit mettre en place chaque entreprise afin de justifier de sa conformité au Règlement Européen.

L'avenant au contrat comprend :

- L'objet du contrat
- La description du traitement faisant l'objet de la sous-traitance
- La durée du contrat
- Les obligations du sous-traitant vis-à-vis du responsable de traitement

8-Clause d'information pour l'utilisation de badges

L'utilisation de badges pour règlementer l'accès aux locaux constitue un registre de traitements. Plusieurs données sont effectivement susceptibles d'être collectées (nom, prénom, numéro de matricule interne, numéro de badge, date d'entrée et de sortie, etc…).

A ce titre, il est impératif de prévoir :

- Un panneau d'information affiché à proximité du dispositif de contrôle d'accès aux locaux
- Une notice d'information complète relative à la gestion des données personnelles et aux droits des personnes.

  Cette notice doit être tenue **à disposition des visiteurs** (à l'accueil des locaux par exemple) **et des salariés**. Pour ces derniers, cette notice peut être transmise par mail ou au moment de l'embauche, lors de la signature du contrat de travail.

Cette notice doit comporter :

- L'objet du traitement ;
- Les données enregistrées ;
- Les destinataires des données ;
- La durée de conservation des données ;
- Le droit des personnes.

9-Clause d'information en cas de géolocalisation des véhicules des salariés

L'utilisation d'un système de géolocalisation des véhicules constitue un registre de traitements. Plusieurs données sont effectivement susceptibles d'être collectées (nom, prénom, coordonnées professionnelles, matricule interne, numéro de plaque d'immatriculation du véhicule, etc…).

A ce titre, il est impératif de prévoir :

- La remise d'une note à chaque salarié ;
- Une notice d'information complète relative à la gestion des données personnelles et aux droits des personnes.

  Cette notice doit transmise **aux salariés**. Pour ces derniers, elle peut être transmise par mail ou au moment de l'embauche, lors de la signature du contrat de travail.

Cette notice doit comporter :

- L'objet du traitement ;

- Les catégories de données ;
- Les destinataires des données ;
- La durée de conservation des données ;
- Le droit des personnes.

10-Clause d'information en cas de vidéosurveillance sur les lieux de travail

L'utilisation d'un système de vidéosurveillance constitue un registre de traitements. L'image d'un salarié, visiteur, client est une donnée et doit faire l'objet de plusieurs actions.

A ce titre, il est impératif de prévoir :

- Un panneau d'information affiché dans les locaux de l'endroit (panneau visible) ;
- Une notice d'information complète relative à la gestion des données personnelles et aux droits des personnes.

  Cette notice doit transmise **aux salariés**. Pour ces derniers, elle peut être transmise par mail ou au moment de l'embauche, lors de la signature du contrat de travail.

- La notice doit être à disposition des salariés sur l'**intranet** ou dans le **Règlement Intérieur** de l'entreprise. En l'absence d'intranet ou de Règlement Intérieur, elle doit pouvoir être fournie à tout moment au salarié qui en fait la demande au responsable de traitement.

- La notice doit également être tenue à disposition des visiteurs pouvant être amenés à être filmés lors de leurs passages dans les locaux de l'entreprise (transmission directe ou à distance si la demande est faite ultérieurement).

11-Engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel

L'employeur devant prendre toutes les mesures nécessaires pour sécuriser la collecte et le traitement des données personnelles, il est impératif de sensibiliser les salariés amenés à traiter ou collecter lesdites données.

A ce titre, **la signature d'un engagement de confidentialité** pour les personnes ayant vocation à manipuler des données à caractère personnel est indispensable.

Si cet engagement sensibilisera les salariés concernés par la manipulation de données, il est important de préciser ce que doit faire ou ne pas faire le salarié (utilisation des données uniquement dans le cadre de ses missions/Ne divulguer ses données qu'aux seules personnes habilitées/Ne pas faire de copies de ces données/Etc…).

Cet engagement doit **être signé par le salarié en 2 exemplaires** (un pour l'employeur et un pour le salarié).

Il sera **annexé à la documentation RGPD** visant à justifier de toutes les démarches de prévention mises en œuvre.

12-Modèle de clause pouvant être utilisée en cas de maintenance par un tiers

Les opérations de maintenance réalisées par des tiers doivent faire l'objet d'un encadrement pour maîtriser l'accès aux données par des tiers.

A ce titre, l'employeur doit :

- Etablir un tableau de bord des diverses opérations de maintenance (date, nature de l'intervention, nom du prestataire, etc…).
- Insérer une clause de sécurité dans ses contrats de maintenance.

Pour les opérations de maintenance à distance, l'employeur doit s'assurer de l'utilisation d'un système permettant d'identifier la provenance de chaque intervention extérieure et obtenir l'accord préalable de la personne concernée avant le début de l'opération (utilisation de systèmes tels que go to assist, TeamViewer, etc…).

13-Bandeau d'information préalable (pour site internet)

Tout internaute se rendant sur un site internet doit être informé :

- Des finalités précises des cookies utilisés ;
- De la possibilité de s'opposer à ces cookies et de changer les paramètres en cliquant sur le lien présent dans le bandeau ;
- Du fait de sa validation de l'utilisation des cookies en poursuivant sa navigation sur le site internet ;

Le responsable du site peut proposer une page « **en savoir plus** » afin d'informer plus précisément l'internaute sur ce qu'est un cookie.

A noter : Le bandeau de consentement ne doit pas disparaître tant que l'internaute n'a pas choisi de continuer sa navigation. Pour acter le consentement de l'internaute, il est conseillé d'utiliser un bouton « opt-in » (ou case à cocher).

14-Information du candidat à l'embauche

Pour être en conformité avec le Règlement Européen sur la Protection des Données, le recrutement d'un salarié doit faire l'objet d'une note informative comprenant :

- Identité de la société et du responsable de traitement ;
- La finalité, la base juridique et le process du traitement de données ;
- L'éventuelle transmission des données à un sous-traitant/tiers ;
- Le pays vers lequel sont transférées les données ;
- La durée de conservation des données ;
- La mention du droit d'accès, de rectification, de limitation, et d'effacement des données ;
- La possibilité de s'opposer au traitement et à la portabilité des données ;
- La possibilité de retirer son consentement au traitement effectué ;
- La possibilité d'effectuer une réclamation auprès de l'autorité de contrôle.

15-Note informative sur la mise en place du RGPD

Une note informative concernant la mise en place du RGPD doit être mise à disposition auprès des salariés, clients, fournisseurs, prestataires, sous- traitants. Elle peut être intégrée au site web.

16-Attestation justificative mise en conformité RGPD

Depuis le 25 mai 2018 et l'entrée en vigueur du Règlement Européen sur la Protection des Données, tout organisme doit lancer une démarche visant à se mettre en conformité avec ledit règlement.

Toute société ou organisme doit attester auprès de ses clients avoir réalisé cette démarche.

La société doit notamment attester qu'elle a bien Cartographié ses données en définissant tous registres de traitements.
La société doit démontrer qu'elle a Etabli une documentation visant à justifier de sa conformité avec le Règlement Européen sur la Protection des Données.

17-Recommandation de la CNIL dans le cas d'une authentification des utilisateurs basée sur des mots de passe

18-Formulaire de notification et violation CNIL

19-Support registre sous-traitant