Manuel pratique

de mise en conformité au RGPD

destiné aux clients de CERFRANCE Saône-et-Loire

Ce manuel vous est proposé pour vous accompagner dans votre propre mise en conformité au Règlement Général sur la Protection des Données (RGPD) dans la mesure où vous mettez également en place des traitements de données personnelles dont vous assurez la responsabilité. En effet, cette nouvelle réglementation entrée en application le 25 mai 2018 fait peser de nouvelles obligations sur l'ensemble des organismes (sans distinction de taille de la structure), notamment afin de les responsabiliser au regard de la protection des données personnelles.

1. Quelles sont les mesures à mettre en place ?

- **Désigner la personne chargée de la protection des données personnelles**

Une personne chargée de la protection de vos données personnelles doit être désignée en interne ou en externe (le cas échéant, vous pouvez vous adresser à votre interlocuteur CERFRANCE pour plus de renseignements).

Il peut s'agir du délégué à la protection des données (DPO) dont la désignation est obligatoire si par exemple vous réalisez un suivi régulier et systématique à grande échelle des personnes concernées. Cette personne sera chargée au sein de la structure de veiller au respect de la protection des données personnelles.

- **Tenir un registre de vos traitements**

Vous devez tenir et mettre à jour un registre listant l'ensemble de vos traitements de données personnelles en fonction de leurs finalités, par exemple la gestion du recrutement, des ressources humaines, la gestion des badges et des accès, la gestion des commandes, des fournisseurs et de ses clients...

Le registre doit comporter pour chaque traitement les informations suivantes :

Noms et coordonnées du responsable du traitement, de son représentant et du délégué à la protection des données (DPO) si sa désignation est requise	Catégories de destinataires auxquels les données seront communiquées
Finalités du traitement	Transferts de données à caractère personnel mis en œuvre
Catégories de personnes concernées	Délais prévus pour l'effacement des différentes catégories de données
Catégories de données à caractère personnel	Mesures de sécurité techniques et organisationnelles

➢ **Respecter les principes essentiels de la protection des données personnelles**

Pour chaque fiche de registre créée, vérifiez que :

- les données personnelles que vous collectez sont traitées pour la réalisation d'un objectif précis qui correspond en général aux missions de l'organisme (**finalité déterminée et légitime**).
- les données que vous traitez sont **adéquates, pertinentes, non excessives et mises à jour** à ce qui est strictement nécessaire 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.
- vous conservez vos données pendant une durée déterminée et proportionnelle à la finalité poursuivie (**durée de conservation limitée**).
- des mesures techniques et organisationnelles appropriées ont été mises en place pour préserver la confidentialité et l'intégrité de vos données (**obligation de sécurité**) : par exemple : utilisation d'un mot de passe, recours à un hébergement sécurisé de vos données.
- vous **respectez les droits des personnes** tels que définis ci-dessous.

➢ **Respecter les droits des personnes concernées**

Le RGPD renforce l'obligation d'information et de transparence à l'égard des personnes dont vous traitez les données (clients, collaborateurs, salariés, prospects, fournisseurs, etc.).

À chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information comprenant les éléments suivants :

- la finalité (pourquoi vous collectez les données ?)
- le fondement juridique (ce qui vous autorise à traiter ces données) : 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 ».
- les destinataires ou catégories de destinataires de ces données : exemple : les services internes compétents, les personnes habilitées en interne, un prestataire (comme une des agences du réseau CERFRANCE), etc.
- la durée de conservation de vos données : exemple : 5 ans après la fin de la relation contractuelle.
- les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits d'accès, de rectification, d'opposition, d'effacement, de portabilité de leurs données et de limitation du traitement : par exemple via leur espace personnel ou par un formulaire de contact sur votre site internet, par un message envoyé à une adresse email dédiée, par un courrier postal à un service identifié.
- si vous transférez des données hors de l'Union européenne : dans ce cas précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données.

✓ **Sécurisez vos données**

Garantissez l'intégrité de vos données en minimisant les risques de pertes 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.

✓ **Notifiez les violations de vos données personnelles**

Vous devez notifier toute violation de vos données personnelles (vos données ont été de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées ou vous avez constaté un accès non autorisé à vos données) à la CNIL dans les meilleurs délais et au plus tard dans les 72 heures après en avoir pris connaissance et que si cette violation est susceptible de présenter un risque pour les droits et libertés des personnes.

Exemple de risques pour les personnes : la perte de contrôle sur leurs données personnelles, la limitation de leurs droits, un vol ou une usurpation d'identité, une perte financière, etc.

Si ces risques sont élevés pour les personnes, elles doivent également en être informées.

Vous devez être à tout moment en mesure de démontrer le respect des principes de protection des données qui s'appliquent également à vos sous-traitants. Si tel est le cas, vous devez vous assurez que leurs nouvelles obligations ont été prises en compte dans les contrats que vous avez conclus.

2. Comment CERFRANCE Saône-et-Loire peut vous accompagner dans vos démarches ?

➢ **Tenir un registre de vos traitements**

Pour avoir un registre exhaustif et à jour, il faut en discuter et être en contact avec toutes les personnes de l'organisme susceptibles de traiter des données personnelles. Ainsi, dans le cadre de la réalisation de leurs prestations au sein de votre organisme, vos interlocuteurs CERFRANCE pourront vous accompagner pour la tenue de ce registre. En effet, grâce à leurs connaissances et à leurs compétences dédiées au profil de votre organisme, les interlocuteurs CERFRANCE pourront échanger avec les différents personnes ayant accès aux données personnelles traitées.

➢ **Respecter les principes essentiels de la protection des données personnelles**

Les agences de CERFRANCE Saône-et-Loire peuvent vous accompagner afin de :

- ✓ distinguer les différentes finalités mises en place au sein de votre organisme.
- ✓ minimiser la collecte des données en déterminant celles qui doivent être éliminées de vos formulaires de collecte et vos bases de données toutes les informations inutiles.
- ✓ poser des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans vos applications.
- ✓ mettre en place des mesures de sécurité notamment en déposant l'ensemble de la documentation portant sur vos traitements de données au sein de la GED pour y accéder à partir de votre espace personnel (*indiquer ici le nom de votre portail client*)

➢ **Respecter les droits des personnes concernées**

Des exemples de mentions sont disponibles sur le site internet de la CNIL.

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.

CERFRANCE Saône-et-Loire peut vous accompagner pour mettre en place un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts (1 mois au maximum).

✓ **Sécurisez vos données**

Pour évaluer le niveau de sécurité des données personnelles dans votre organisme, CERFRANCE vous invite d'ores et déjà à vous interroger sur les points suivants :

- les comptes utilisateurs internes et externes sont-ils protégés par des mots de passe d'une complexité suffisante ?
- les accès aux locaux sont-ils sécurisés ?
- des profils distincts sont-ils créés selon les besoins des utilisateurs pour accéder aux données ?
- avez-vous mis en place une procédure de sauvegarde et de récupération des données en cas d'incident ?

S'il existe des risques élevés pour les droits et libertés des personnes concernées (par exemple le traitement des données relatives à l'appartenance syndicale), CERFRANCE peut vous assister dans la réalisation d'une étude d'impact sur la protection des données (« *Privacy Impact Assessment* » ou PIA).

✓ **Notifiez les violations de vos données personnelles**

Dans le cas où la violation de données personnelles doit être notifiée, CERFRANCE Saône-et-Loire peut vous assister dans la mise en place d'une procédure interne.

******