RGPD

Subteno IT

Mise en conformité
25 Mai 2018

INTRODUCTION DE LA RGPD

La RGPD, Réglementation Générale à la Protection des Données, approche à grands pas. A compter du 25 mai 2018, tous les sociétés devront être en mesure de prouver les actions entreprises relatives à la sécurisation des données personnelles, qu'elles soient directement ou indirectement liées à la personne. Cette nouvelle réglementation apporte un changement majeur dans le traitement des données, et implique pour certaines entreprises de nombreux changements relatifs à leur mise en conformité vis à vis de cette réglementation.

Odoo est-il concerné par la RGPD ? La réponse est oui. Subteno IT vous détaille les étapes importantes de votre mise en conformité.

QU'EST CE QU'UNE DONNEE PERSONNELLE ?

Sont concernées par la RGPD toutes les entreprises stockant des données personnelles, sans contrainte d'échelle ou de secteur d'activité.

Pour rappel, une donnée personnelle représente une information, conservée par l'entreprise avec ou sans le consentement direct de la personne physique concernée, permettant de l'identifier directement ou indirectement. Entrent en ligne de compte les informations professionnelles de cette personne. Sont concernée par la RGPD les données collectées numériquement ou sur format papier.

QUE FAIRE POUR SE METTRE EN CONFORMITE ?

Afin de vous mettre en conformité, il est nécessaire que votre entreprise soit en mesure de prouver la mise en place d'actions relatives à la sécurisation des données personnelles qu'elle stocke. Plusieurs étapes peuvent être suivies pour s'assurer de la mise en conformité de votre entreprise vis à vis de cette réglementation

DESIGNATION D'UN RÉFÉRENT (DPO)

La désignation d'un Délégué à la Protection des Données est fortement recommandé. C'est la personne en charge de tout ce qui concerne les données personnelles pour l'entreprise.

Avoir une personne référente vous permettra, en cas de vérification de la part de l'autorité compétente, de disposer d'une source d'information fiable concernant les actions mises en oeuvres par votre entreprise vis à vis de cette nouvelle réglementations. Quoi qu'il en soit, il est obligatoire de définir une personne référente dans 2 cas bien distincts (Source : CNIL) :

- Lorsque vos activités de base vous amènent à réaliser un suivi à grande échelle, régulier et systématique des personnes.

- Lorsque vos activités de base vous amènent à traiter à grande échelle des données dites "sensibles" (orientation sexuelle, convictions religieuses, données biométriques, génétiques ou de santé, origine raciale ou ethnique, etc), ou relatives à des condamnations pénales ou infractions.

LE ROLE DU DPO

La personne désignée en tant que CIL est chargée (Source : CNIL) :

- D'informer et conseiller le responsable de traitement ou le sous-traitant ainsi que leurs employés.
- De contrôler le respect du règlement et du droit national en matière de protection des données.
- De conseiller l'organisme sur la réalisation d'études d'impact sur le protection des données et d'en vérifier l'exécution.
- De coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Rapprochez vous de la l'autorité compétente de votre pays pour la mise en place des missions de votre référent.

CARTOGRAPHIER LES TRAITEMENTS DE DONNÉES

Dans l'optique de mesurer concrètement l'impact de cette nouvelle règlementation vis à vis de votre entreprise, il est nécessaire de réaliser une cartographie complète des données personnelles que vous traitez, afin de les recenser de façon précise.

La mise en place d'un registre des traitements vous permettra de le faire.

Pour chacun des traitements que vous allez réaliser, vous pouvez vous poser les questions suivantes :

- Qui est en charge de ces traitements ? Qui sont les acteurs majeurs agissants sur ces traitements de données ?
- Quelles sont les données traitées ? Sont-elles des données sensibles ?
- Pourquoi ces données sont-elles traitées ? Quelle est la finalité du traitement de ces données ?
- Où se situent ces données tout au long de leur traitement ? Quel est le parcours suivi par ces données ?
- Jusqu'à quand ces données sont-elles conservées ?
- Comment ces données sont-elles sécurisées ? Quelles dispositions sont prises pour assurer la protection de ces données ?

- Cette première étape de réflexion et de recensement vous permettra de définir votre plan d'action par la suite, afin de définir les tâches à réaliser pour vous mettre en conformité avec la RGPD.

MISE EN PLACE DES ACTIONS DE PROTECTIONS

Suite à la cartographie réalisée sur les données collectées et traitées par votre entreprise, il est nécessaire de prioriser les actions à mener pour leur sécurisation.

Il est important de prioriser ces actions en fonctions des risques évalués, créés par les traitements en place au sein de votre entreprise, au regard de la vie privée des personnes concernées.

Quelques points sont importants à cette étape (Source : CNIL) :

- Assurez-vous que seules les données strictement nécessaire à la poursuite de vos objectifs sont collectées et traitées.
- Identifiez la base juridique sur laquelle se fonde votre traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale).
- Révisez vos mentions d'information afin qu'elles soient conformes aux exigences du règlement.
- Vérifiez que vos sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités, assurez-vous de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées.
- Prévoyez les modalités d'exercice des droits des personnes concernées (droits d'accès, de rectification, droit à la portabilité, retrait du consentement ...).
- Vérifiez les mesures de sécurité mises en place.

- Une vigilance particulière doit être portée vis à vis de certains types de données, de leur effet ou des possibles transferts auxquelles elles sont exposées.

ANALYSER ET GÉRER LES RISQUES RELATIFS

Il est important de mesurer les risques toujours existants ou directement créés suite à la mise en place de vos actions de sécurisation des données personnelles.

Afin de prendre connaissance de ces risques, et les mesurer, il est alors nécessaire de mener une "Etude d'impact sur la protection des données".

Le but de cette étude d'impact est de mettre en place un traitement des données personnelles respectueux de la vie privée des personnes physiques, en appréciant les impacts de ces traitements et en démontrant le respect des principes fondamentaux de la RGPD.

Cette étude doit contenir différents éléments (Source : CNIL) :

- Une description du traitement et de ses finalités.
- Une évaluation de la nécessité et de la proportionnalité du traitement.
- Une appréciation des risques sur les droits et libertés des personnes concernées.
- Les mesures envisagées pour traiter ces risques et se conformer au règlement.

ORGANISATION DES PROCESSUS INTERNES

Dans le cadre de votre mise en conformité avec la RGPD, il vous est ensuite vivement conseillé d'organiser les processus internes relatifs à la collecte et au traitement des données personnelles des personnes physiques.

Il est notamment demandé que ces processus respectent le cadre légal d'obtention de la donnée personnelle. La sensibilisation et l'organisation des retours d'information doivent être réalisés pour permettre le respect de la RGPD.

Le traitement des réclamations des personnes concernées, ayant pour objet l'exercice de leurs droits, doit faire l'objet d'un processus interne à votre entreprise leur permettant de les exercer.

Enfin, il vous est demandé, en cas de violation des données personnelles des personnes physiques, de prévenir l'autorité de protection des données dans les 72 heures, ainsi que d'en informer les personnes concernées dans les meilleurs délais.

DOCUMENTATION DE LA MISE EN CONFORMITÉ

Comme nous l'avons défini à l'introduction de la RGPD, il est nécessaire pour votre entreprise d'être en capacité de prouver la mise en conformité de celle-ci à la nouvelle règlementation adoptée au sein de l'Union Européenne.

Il est par conséquent nécessaire de documenter toutes les actions et réflexions entreprises pour cela. Il est par conséquent demandé (Source : CNIL) :

La documentation sur vos traitements des 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 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 ou les BCR).

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 des personnes.

Les contrats qui définissent les rôles et les responsabilités des acteurs :

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

Quoi qu'il en soit, la RGPD s'applique à toutes les entreprises. Ce guide a pour but de vous aider dans les étapes à réaliser pour vous mettre en conformité, mais ne représente en aucun cas un guide de procédure complet à suivre. Renseignez vous auprès de l'autorité compétente dans ce domaine de votre pays.

MENTIONS LÉGALES

Est mentionné, dans certaines parties de ce document, la mention : "Source : CNIL".

Chacune de ces mentions tient à créditer, pour ces parties, le document : Règlement européen sur la protection des données personnelles - Se préparer en 6 étapes.

« Source : CNIL – http://www.cnil.fr »

Contenu extrait le : 25/04/2018

Licence :