RGPD AVOIR TOUJOURS LES BONS RÉFLEXES

Fiche n°5

Quelle sensibilisation ou formation pour les collaborateurs en entreprise ?

CONTEXTE

Le RGPD soulève des questions en permanence et oblige les entreprises à mettre régulièrement à jour toutes les procédures de traitement d'informations. Il est préférable d'habituer et d'informer toutes les personnes impactées et concernées par la gestion et la manipulation de données.

Il est donc intéressant de différencier les types de collaborateurs et les formations liées et à adapter en fonction de leur profil :

Personnes référentes RGPD
Chefs de projet SI, concernés par la mise en place et le pilotage des systèmes sur l'ensemble de l'entreprise.
Tous salariés pouvant constater les infractions, les violations, etc.
Ils doivent pouvoir réagir en fonction des situations : sensibilisation et sécurité informatique.

L'ESSENTIEL À RETENIR

- Avertir et sensibiliser toutes les personnes de l'entreprise sur la conformité RGPD et les risques potentiels
- Transmettre les coordonnées des personnes référentes RGPD et du DPD
- Adapter les formations/sensibilisations en fonction des missions des différents profils collaborateurs
- Suivre et mettre à jour les documents

ACTIONS À RÉALISER

Doit-on encore sensibiliser, former et si oui comment ?

Mettre en place une sensibilisation d'accueil

Pour toutes nouvelles arrivées (et aussi pour tout salarié déjà présent, lors de la mise en place de la formation), aborder différentes thématiques clés : sécurité, protection de l'information, données personnelles...
Mettre en place une charte de sécurité engageant les salariés ayant vocation à manipuler des données à caractère personnel.

Déterminer le besoin de formation/sensibilisation

Cela va dépendre des organisations, du type de données abordées et potentiellement traitées.
En fonction de l'impact du RGPD sur les différents publics, élaborer une liste de thème à aborder.

Salariés peu impactés

Pour tous les salariés, mettre en place des capsules de sensibilisation où l'on aborde le RGPD.
Créer une page d'information sur les méthodes à respecter avec des exemples concrets parlant de condamnation par la CNIL, de fuite de données...

Chefs de projet SI

Mettre en place des procédures pour sensibiliser et responsabiliser les « chefs d'équipe »
Prévoir tous les 6 mois un point pour remplir les registres, les reprendre, effectuer un suivi régulier et le consigner. Les chefs de projet ne sont pas impactés de la même manière, certains domaines sont plus touchés et sensibles : RH (Paye, suivi de carrière, médecine du travail).

Référents RGPD métier lorsqu'ils sont présents dans l'organisation (fortement souhaité)

Ils sont les appuis directs aux DPD (Délégué à la Protection des Données) : Prévoir des formations continues à l'aide de MOOC CNIL avec attestations (par exemple). Ce MOOC peut aussi être suivi par les Chefs de Projet SI dont les applications sont les plus impactées par le RGPD.
Se référer au site de la CNIL : https://www.cnil.fr/fr/tag/mooc

Préconiser et déterminer la fréquence des sensibilisations

Prévoir le risque d'audit en s'assurant que les personnes ont été sensibilisées, comment et s'assurer que cela ait bien été fait. Par exemple, mesurer la sensibilisation des personnes par des tests/QCM.
Fréquence conseillée :
- Population sensible : 2 fois par an.
- Agents peu impactés : obligation tous les ans ou tous les 2 ans en fonction de leurs missions.

Mettre en place un tableau de bord des formations

Mettre à jour les Référentiels des projets

Mettre en exergue dans les procédures spécifiques liées aux projets, les points d'attention et activités des projets directement liés au RGPD.

Sensibiliser tous les services de l'entreprise liés à la réalisation et l'utilisation de systèmes informatiques, d'appareils, de logiciels ou d'applications

Il est fortement recommandé d'obtenir l'approbation explicite du département SI, pour tous ces usages, notamment concernés par la collecte ou le traitement de données personnelles car il peut y avoir des risques de sécurité tels que des fuites de données. (cf. cas d'un Shadow IT).

Sensibiliser sur le fait que la prise en compte du RGPD doit être le plus en amont possible du projet, dès le Cahier des Charges

Ne pas le traiter à « quelques jours » de l'ouverture du service.

POINTS DE VIGILANCE

S'appuyer au maximum sur son DPD et lui remonter toutes les questions que l'on se pose.

S'assurer que les sous-traitants sont régulièrement formés et qu'ils restent au fait des dernières actualités. On peut imposer à la société de prouver qu'elle a formé ses salariés.

Ne pas conserver les données à caractère personnel au format papier.

Transmettre des tableaux (format .ods) par un lien sécurisé – Recommandé par la CNIL.

RISQUES

Sans formation ou sensibilisation, il est difficile de :
Traiter et réagir aux demandes liées aux données personnelles.
Comprendre et prendre en compte le RGPD dans la réalisation des projets.

Autres risques financiers :
Devoir reprendre les procédures et les systèmes RGPD mis en place car non-conformes.
Payer une amende suite à une sanction de la CNIL.
Atteinte à l'image de marque dû au « name and shame ».