QUELQUES CONSEILS PRATIQUES DANS VOTRE DÉMARCHE DE CONFORMITÉ AU RGPD.

Conseils pratiques publié le **15/12/2022**, vu **814 fois**, Auteur : La zone du droit

Comme vous le savez, le responsable du traitement doit faciliter l'exercice des droits (12.2 du Règlement général sur la protection des données - RGPD) et informer les personnes concernées de manière claire.

Comme vous le savez, le responsable du traitement doit faciliter l'exercice des droits (12.2 du Règlement général sur la protection des données - RGPD) et informer les personnes concernées de manière claire, notamment de la durée de conservation des données et de l'exercice de leurs droits [1].

Lorsque vous êtes victime d'un traitement de vos données personnelles (mails personnels, numéros de téléphone, mails professionnels, caméra de vidéoprotection/vidéosurveillance etc…) sans votre consentement ou à votre insu, vous avez la possibilité de vous adresser directement à l'organisme (Responsable de Traitement (RT)) qui pourrait être potentiellement incriminé en cas de refus de vous répondre au titre de vos droits recensés aux articles [2]. A défaut, vous pouvez saisir la Commission Nationale de l'Informatique et des Libertés (CNIL) afin qu'elle intervienne auprès de l'organisme incriminé.

Pour rappel, la majorité des plaintes s'articule autour des droits d'accès le plus souvent sur les dispositifs innovants tels que les caméras de vidéos surveillance/protection ou sur la problématique de la durée de conservation des données personnelles et celle de la non-conformité lors des traitements des données à caractère personnel des personnes concernées.

Voyons quelques points problématiques et les conseils qui en découlent.

I. Faciliter le droit d'accès aux personnes concernées.

Afin d'assurer l'effectivité du droit d'accès, il appartient donc à l'Entreprise incriminée de mettre en place des procédures internes permettant de le favoriser. Des actions de sensibilisation et des formations doivent notamment être mises en œuvre afin que ces procédures soient connues par l'ensemble des collaborateurs.

En outre, il faille garantir l'intégrité des données traitées et leur disponibilité, conformément à [3].

II. La conformité sur l'installation d'un système de vidéosurveillance.

Un autre exemple des plaintes portées devant les autorités de CNIL concernant l'installation d'un système de « *vidéosurveillance* » (dispositif installé dans un lieu non ouvert au public : lieux de

stockage, zones réservées au personnel), doit répondre à un but précis et légitime, comme la sécurité des personnes et des biens [4].

Les caméras installées dans un lieu de travail ne peuvent être utilisées pour un autre objectif que celui prévu initialement. Par exemple, le visionnage à distance des images sur une tablette ou un téléphone ne doit pas conduire à surveiller les employés pour leur faire des remarques sur la qualité du travail.

Le dispositif de vidéosurveillance doit être proportionné à son objectif. Cette proportionnalité s'apprécie au regard, notamment, du nombre de caméras installées, de leurs emplacements, orientations, fonctionnalités (zoo, son…), périodes de fonctionnement, de la nature des tâches accomplies par les employés, etc.

En pratique, les caméras ne doivent pas placer sous surveillance constante un employé particulier ou un groupe d'employés sur leurs postes de travail, sauf circonstances exceptionnelles liées à la sensibilité du poste occupé.

Le dispositif doit donc respecter la vie privée des employés sur le lieu de travail.

Ainsi, les zones de pause ou de repos des employés, les toilettes, les vestiaires et les locaux syndicaux ou leurs accès ne doivent pas être filmés. De même, les caméras ne doivent pas permettre de capter le son, avec ou sans enregistrement, sauf déclenchement à l'initiative de l'employé concerné en cas d'évènement le justifiant.

A titre d'illustration, la formation restreinte de la CNIL a prononcé une sanction de 20.000 euros à l'encontre d'un organisme qui plaçait les salariés sous surveillance vidéo constante [5].

Si votre dispositif de vidéosurveillance n'est pas en conformité, vous devrez prendre les mesures nécessaires telles que le retrait de la caméra, réorientation ou apposition de caches, désactivation de la captation de son, informations à compléter, limitation des accès aux images, respect de la durée de conservation, etc.

III. Conformité et messagerie professionnelle.

Un employeur qui met en œuvre des traitements de données à caractère personnel pour permettre à ses salariés d'accomplir leurs missions (poste informatique, messagerie professionnelle, accès à Internet etc.), est tenu de se conformer notamment aux dispositions du Règlement sur la protection des données personnelles (RGPD).

Ainsi, les données à caractère personnel ne peuvent être conservées que pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

En conséquence, lorsqu'un salarié quitte une entreprise, les données à caractère personnel le concernant sont susceptibles d'être périmées, notamment son adresse de messagerie électronique professionnelle et les informations apparaissent sur l'intranet, à l'exception des données dont la conservation est prévue par un texte légal ou réglementaire.

Par ailleurs, les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes et être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées [6].

De plus, le responsable de traitement doit veiller à garantir la sécurité et la confidentialité des données qu'il traite [7] et article 32 du RGPD.

Ainsi, permettre l'accès de la messagerie professionnelle à des tiers ou mettre en œuvre une procédure de redirection systématique des courriels réceptionnés à l'adresse électronique de l'employé absent ou parti, vers une autre adresse électronique professionnelle soulèvent des difficultés, notamment en matière de sécurité et de confidentialité des données.

En outre, si les messages envoyés et reçus via la messagerie électronique professionnelle sont présumés avoir un caractère professionnel, une utilisation résiduelle de la messagerie à des fins personnelles est, en principe, tolérée.

Ainsi, une redirection systématique des courriels vers une autre messagerie n'apparait pas comme suffisamment garant du respect du secret des correspondances dont la violation est une infraction pénalement sanctionnée [8].

C'est pour cela que la CNIL recommande la mise en place d'un message indiquant que la personne est absente ou que l'adresse électronique du salarié est devenue inactive et qu'à cet égard les interlocuteurs disposent d'une autre adresse électronique vers laquelle ils peuvent envoyer leurs messages. Cette pratique permet d'assurer la continuité de l'activité de l'organisme.

S'agissant de la conservation de courriels à caractère professionnel postérieurement au départ d'un salarié, celle-ci apparaît légitime si leur conservation a pour objet, notamment, d'assurer la continuité de service.

En revanche, les messages identifiés comme personnels doivent être supprimés au moment du départ du salarié. La CNIL recommande à l'employeur d'avertir le salarié concerné préalablement à la suppression des messages afin qu'il soit en mesure de les récupérer.

Pour conclure, la CNIL recommande aux employeurs de mettre en place une charte informatique afin d'organiser l'utilisation des outils mis à la disposition des salariés et notamment, le devenir de ces outils à l'issue de la relation de travail.

Notes de l'article:

[1] Articles 12 et 13 du RGPD.

[2] 15 RGPD, 16 RGPD, 17 RGPD, 18 RGPD, 20 RGPD et 21 RGPD.

[3] Article 32 du RGPD.

[4] Article 5.1 b et c) du RGPD.

[5] Délibération n°SAN-2019-006 du 13 juin 2019.

[6] Articles 5.1 b) et c) du RGPD.

[7] Article 5.1 f).

[8] Articles 226-15 et 432-9 du Code pénal.

[9] https://www.privacy-regulation.eu/fr/15.htm