Chloé Découst
Emmanuelle Orain
Jade Le Brouster
Leslie Planet
Rémi Pierron

2024/2025

BUT Science des Données

SAE – Droit

BUT SD2

Mr. Grégoire

2021 a été une année record pour l'action répressive de la CNIL (Commission Nationale de l'Informatique et des Libertés). En effet, depuis l'entrée en vigueur du RGPD (Règlement Général sur la Protection des Données) le 25 mai 2018, de nombreuses entreprises n'ont pris

aucune mesure pour se conformer au règlement. Par conséquent, ces entreprises se sont exposées à des sanctions administratives et dans certains cas, pénales.

Les sanctions administratives sont prononcées par la CNIL et peuvent aller d'un avertissement ou d'un rappel à une amende s'élevant jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires. Les sanctions pénales sont appliquées en cas de non-respect des finalités ou en cas de traitement de données sensibles. Elles peuvent aller jusqu'à 5 ans de prison et 300 000 euros d'amende.

En tant que délégués à la protection des données du service RH de l'entreprise X, nous sommes chargés de conseiller l'entreprise afin qu'elle soit en conformité avec le RGPD.

En quoi consiste le RGPD ?

Selon l'article 2, le RGPD "s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier".

En d'autres termes, le RGPD veille à la protection du traitement des données personnelles des acheteurs sur Internet, des salariés utilisant des outils informatiques et des citoyens qui s'exposent sur les réseaux sociaux.

Pour ce faire, la CNIL se base sur un système d'autocontrôle visant à responsabiliser les détenteurs de données personnelles quant au respect des cinq grands principes essentiels du RGPD :

- Le principe d'interdiction de traitement des données dites sensibles
- La proportionnalité et la pertinence des données
- Le principe d'une durée limitée de conservation des données
- La sécurité, l'intégrité et la confidentialité des données
- Le droit des personnes (le consentement)

Après avoir pris connaissance des données collectées par votre entreprise, nous devons vous informer des modifications et des procédures à mettre en place :

Premièrement, selon l'un des 5 grands principes du RGPD, il ne vous est pas permis de collecter ou de traiter des données à caractère personnel, c'est-à-dire, les données qui font apparaître directement ou indirectement les origines raciales/ethniques, l'appartenance syndicale des personnes ou les opinions politiques, philosophiques ou religieuses. En effet, l'utilisation de ces données constituerait une violation du principe d'interdiction de collecte de données sensibles.

Il vous est donc strictement interdit de collecter les données de vos salariés concernant l'appartenance syndicale, le nombre de jours de grève et l'indication des pathologies. C'est pourquoi, nous allons nous charger de les supprimer.

Deuxièmement, selon le RGPD, seules les données proportionnelles et pertinentes peuvent être collectées. Pour s'assurer que les données que l'on souhaite utiliser soient proportionnelles et pertinentes, il faut pouvoir répondre aux questions suivantes : est-ce que j'ai réellement besoin de cette donnée ? Si oui, suis-je capable de justifier pleinement de son utilisation ?
Dans notre cas, nous allons devoir supprimer des bases les données : la nature des études des enfants (sauf dans le cas d'aides ou de subventions de la part de l'entreprise) et la profession des parents.
Les sanctions disciplinaires à l'exclusion de celles consécutives à des faits amnistiés ne peuvent être collectées si leur utilisation a pour but d'évaluer la promotion ou la mutation d'un salarié.
Le type de permis de conduire quant à lui, peut être collecté seulement si l'employé est amené à effectuer des trajets professionnels.
Cependant, il est tout à fait possible de garder les données liées aux genres pour l'établissement d'études statistiques. En effet, ces études peuvent être utiles pour vérifier si la parité hommes-femmes dans l'entreprise est bien respectée.

Troisièmement, nous devons aborder le principe de conservation des données. D'après le RGPD, les informations ne peuvent être conservées de façon définitive dans les fichiers informatiques. Il est donc nécessaire qu'une durée de conservation précise soit définie en fonction de la finalité de chaque donnée.
De ce fait, en tant que DPO, nous devons vérifier que votre service ne conserve pas d'informations d'une durée supérieure à celle établie par la base active, c'est-à-dire, que la durée n'excède pas celle nécessaire à la réalisation d'objectifs ayant justifié une collecte ou enregistrement de données.
Il faudra aussi veiller à ne pas conserver les sanctions disciplinaires à des faits amnistiés qui concernent les sanctions ayant été juridiquement effacées. Par exemple, la durée de conservation d'une suspension d'un salarié ne doit pas dépasser 3 ans.

Quatrièmement, la sécurité, la confidentialité et l'intégrité sont un autre principe très important et primordial du RGPD. Plus de deux tiers des sanctions administratives prononcées par la CNIL depuis 2017 incluent un manquement à la sécurité. C'est pourquoi, il est important en tant que DPO de réaliser une revue annuelle des habilitations afin d'identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur.
De plus, il est essentiel d'être transparent avec les salariés vis-à-vis du traitement de leurs données.
En tant que DPO, nous allons devoir également mettre en place des moments pour sensibiliser et former les salariés face aux éventuels risques (cyberattaques notamment) et leur donner des règles à suivre pour se protéger correctement et efficacement lorsqu'ils travaillent à l'aide d'outils informatiques comme la création d'un mot de passe fort.

Enfin, même si le consentement n'est pas nécessaire pour le traitement des données liés aux obligations légales ou contractuelles (contrat, INSEE, autorité publique, prévention de la fraude,etc.), il constitue une règle très importante du RGPD.

Attention, le consentement est tout de même requis pour certains cas comme pour le traitement de données sensibles et à des fins de prospection.
Les photographies permettant de constituer le trombinoscope et/ou des badges peuvent faire l'objet de traitement seulement si le consentement a été donné par le salarié. Il en va de même pour la publication de photos sur les réseaux sociaux de l'entreprise ou dans des articles de presse, c'est ce que l'on appelle le droit à l'image.
Le numéro d'ordre et la copie du titre pour les employés étrangers sont nécessaires pour respecter la législation du droit du travail.
La simulation de carrière, la situation familiale, le motif de changement de situation professionnelle et la référence du passeport pourront être collectés par le service RH seulement si ces données peuvent être justifiées par une base légale sinon, elles devront être supprimées.

Pour conclure, il faut retenir qu'il est important de s'assurer que les données traitées soient nécessaires et appropriées tout en respectant la durée de conservation liée aux finalités spécifiques et en garantissant la sécurité, la confidentialité, ainsi que le consentement des salariés. Tout traitement de données ne respectant pas le RGPD devra être supprimé.
Normalement, toute entreprise qui se respecte doit tenir un registre des activités de traitement. Cependant, l'entreprise X étant une PME (entreprise qui comporte moins de 250 employés) n'est tenue de tenir ce registre que pour certains traitements, comme les traitements non-occasionnels ou risqués.
Nous nous chargerons en tant que DPO de remettre en conformité le traitement des données de l'entreprise X en suivant les principes énoncés précédemment pour permettre à l'entreprise d'éviter les sanctions évoquées précédemment.

Vous trouverez en annexe, un tableau récapitulatif des éléments à supprimer et leurs justifications.

ANNEXE

Identification de l'employé	Données relatives à l'identité : nom, prénom, photographie, sexe, date et lieu de naissance, nationalité, coordonnées professionnelles, ~~coordonnées personnelles~~, ~~références du passeport~~, situation familiale, situation matrimoniale, enfants à charge, ~~nature des études suivies par les enfants~~, type de permis de conduire détenu par l'employé, ~~profession des parents de l'employé~~.
	Données relatives à la situation professionnelle lieu de travail : numéro d'identification interne, date d'entrée dans l'entreprise, ancienneté, emploi occupé et coefficient hiérarchique, section comptable, nature du contrat de travail, taux d'invalidité, reconnaissance de la qualité de travailleur handicapé (RQTH).

	Données relatives au titre valant autorisation de travail : type, numéro d'ordre et copie du titre pour les employés étrangers.
	Coordonnées des personnes à prévenir en cas d'urgence.
Suivi de la carrière et de la formation de l'employé	Gestion de la carrière de l'employé : date et conditions de recrutement, date, objet et ~~motif des modifications apportées à la situation professionnelle de l'employé~~, ~~simulation de carrière~~, desiderata de l'employé en termes d'emploi, ~~sanctions disciplinaires à l'exclusion de celles consécutives à des faits amnistiés~~.
	Évaluation professionnelle de l'employé : dates des entretiens d'évaluation, identité de l'évaluateur, compétences professionnelles de l'employé, objectifs assignés, résultats obtenus, appréciation des aptitudes professionnelles, ~~appartenance syndicale du salarié lorsqu'elle est connue~~, ~~nombre de jours de grève suivis au cours des 10 dernières années~~.
	Suivi administratif des visites médicales des employés : dates des visites, aptitude au poste de travail (apte ou inapte, propositions d'adaptation du poste de travail ou d'affectation à un autre poste de travail formulées par le médecin du travail), ~~indication des pathologies des salariés lorsqu'elles sont connues~~.

Les données suivantes sont à supprimer car elles :

: Ne respecte pas le principe d'interdiction de collecter les données sensibles

: Ne respecte pas le principe de proportionnalité et de pertinence des données

: Ne respecte pas le principe de droit des personnes