LE RGPD

Le Règlement Général sur la Protection des Données

FÉDÉRATION NATIONALE
DE L'ACTION SOCIALE FO
7 PASSAGE TENAILLE
75 014 PARIS
T. 01 40 52 85 80
F. 01 40 52 85 79
lafnas@fnasfo.fr

MAI 2018

TEXTE INTÉGRAL

https://www.cnil.fr/fr/reglement-europeen-protection-donnees

https://www.cnil.fr/fr/le-reglement-europeen-sur-la-protection-des-donnees-en-dataviz

Après quarante ans de bons et loyaux services, la loi informatique et libertés va prendre sa retraite. À compter du vendredi 25 mai, ce texte adopté en janvier 1978 pour protéger les Français des potentielles dérives du fichage, qui s'est développé en même temps que l'informatique, va disparaître. Son remplaçant est un texte européen qui uniformise les règles en vigueur dans les 28 pays membres de l'UE. Son nom : le règlement général sur la protection des données personnelles, ou RGPD.

Ce règlement va entrer en vigueur dans un contexte devenu électrique, avec l'utilisation indue des données personnelles de millions d'utilisateurs de Facebook par Cambridge Analytica, mais pas seulement. Les récents scandales comme ceux de Ashley Madison (site de rencontres extra-conjugales dont des millions de membres se sont vu leurs données divulguées) ou Uber (dont les données de 50 millions de clients et 7 millions de chauffeurs ont été volées) concernent les données personnelles du public, l'on peut aussi mentionner le scandale qui a frappé le magasin d'ameublement Ikea, accusé de mettre en œuvre des pratiques d'espionnage à l'égard de ses employés qui, alors même qu'il s'agissait de données RH, a eu un impact client.

Ce règlement a été construit autour d'un principe majeur : son contenu s'appliquera à toutes entreprises, **associations**, administrations, collectivités territoriales qui manipulent des informations concernant des résidents européens, y compris si certaines sont basées hors de l'UE.

Voici l'essentiel des points à retenir.

La réforme sur la protection des données à caractère personnel poursuit 3 objectifs :

1. **Renforcer les droits des personnes**, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures
2. **Responsabiliser les acteurs** traitant des données (responsables de traitement et sous-traitants)
3. **Crédibiliser la régulation** grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées.

LES DISPOSITIONS GÉNÉRALES

L'objectif est de protéger les données à caractère personnel de traitements automatisés en tout ou partie ou de traitements non automatisés.

Cette réglementation concerne le territoire de l'Union Européenne et tout territoire sur lequel un établissement participe à la collecte des données.

Les principes

La réglementation doit respecter les principes suivants :

- **Le traitement des données à caractère personnel doit être** licite, loyal et transparent.
- Les données doivent être collectées pour des **finalités déterminées**, **adéquates, pertinentes** et **limitées** aux **finalités déterminées**. De plus, elles doivent être **exactes** ou tenue à jour, **conservées** le temps nécessaire et identifiables pour chaque individu concerné et surtout **protégées** contre un traitement non autorisé.
- **En ce qui concerne la licéité du traitement, l'établissement doit obtenir le consentement de la personne concernée si elle est âgée d'au moins 16 ans ou le consentement du titulaire de la responsabilité de la personne si l'âge est inférieur à 16 ans.**
- **Le traitement doit obligatoirement participer** à **l'exécution d'un contrat**, au **respect d'obligation légale**, aux **intérêts vitaux de la personne** concernée, à **l'exécution d'une mission d'intérêt public** et aux fins **d'intérêts légitimes** poursuivis par le responsable du traitement.
- **Le consentement de la personne concernée** impose que le **responsable du traitement** soit en mesure de **démontrer la preuve** de la personne concernée. La **personne** a le **droit de retirer son consentement** à tout moment et le **responsable du traitement** doit **informer clairement** la personne concernée si l'exécution d'un contrat **nécessite le traitement de données** à caractère personnel.
- **Les données suivantes sont interdites dans les traitements**, notamment si le consentement et la licéité ne sont pas démontrés. Le responsable du traitement et les sous-traitants ne doivent en aucun cas traiter les données concernant l'origine **raciale** ou **ethnique**, les **opinions politiques**, les convictions **religieuses** ou **philosophiques**, l'appartenance **syndicale**, l'**orientation sexuelle**, les **données génétiques**, **biométriques** et les **condamnations pénales et les infractions**.

Les droits de la personne concernée

Le responsable du traitement (généralement le service RH) prend des mesures appropriées pour fournir en toute transparence toutes les Informations visées aux **articles 13 et 14** ainsi que pour procéder à toute communication au titre des **articles 15 à 22** et de **l'article 34**.

Le responsable du traitement ne doit en aucun cas demander un paiement pour fournir les informations. Il doit fournir un accès aux informations suivantes :

- identité et coordonnées du responsable ou du représentant du traitement
- coordonnées du délégué à la protection des données
- les finalités et la base juridique du traitement
- les destinataires du traitement
- la durée de conservation
- l'existence d'une prise de décision automatisée y compris l'usage de profilage.

La personne concernée a le droit de demander la rectification et l'effacement de ses données personnelles, telles que son droit à l'oubli s'il ne va pas à l'encontre, de la *liberté d'expression et d'information*, au respect d'une *obligation légale*, dans la sauvegarde des *intérêts publics*, à des fins archivistes et pour garantir la *défense de droits en justice* (**article 17 du RGPD**).

Le salarié peut également demander à l'entreprise de rectifier ses données à caractère personnel lorsque ces dernières sont inexactes (**article 16 du RGPD**). Le RGPD maintient également un droit au gel temporaire des données personnelles (en cas notamment de contestation de l'exactitude des données, ou en attendant la vérification du traitement si ce dernier est contesté en justice) (**article 18 du RGPD**).

Action de groupe : vers des condamnations de l'entreprise à des dommages et intérêts
La loi Justice du XXIe siècle a introduit une action de groupe en matière de protection des données à caractère personnel. Cette action, qui peut être exercée par une organisation syndicale de salariés représentative (lorsque le traitement affecte des salariés) tend exclusivement à faire cesser le manquement à la loi Informatique et libertés de 1978. Toutefois, un amendement au projet de loi sur la protection des données personnelles introduit la possibilité d'exercer une action de groupe aux fins de réparation du dommage causé par ce manquement. Les employeurs pourraient donc être condamnés à verser des dommages et intérêts aux salariés en cas d'infraction à la règlementation sur la protection des données personnelles.

Le responsable du traitement doit informer la personne concernée de toutes modifications, tout effacement, toute limitation de traitement des données à caractère personnel. Il doit en outre garantir le droit à la portabilité des données de la personne concernée.

La personne concernée a également le droit de ne pas faire l'objet d'un traitement automatisé et le responsable du traitement doit tout mettre en œuvre pour préserver les droits et libertés de la personne concernée par un traitement automatisé.

En revanche, les droits individuels peuvent être ouverts dans les situations suivantes :

- Sécurité nationale
- Défense nationale
- Sécurité publique
- Préventions et détections d'infractions
- Intérêts publics
- Indépendance de la justice
- Respects des professions réglementées
- Mission de contrôle
- Protection des droits et libertés d'autrui
- L'exécution des demandes de droit civil

L'INFORMATION ET LE CONSENTEMENT PRÉALABLE DES SALARIÉS

Concrètement, les salariés doivent être informés du traitement de leurs données personnelles de façon claire et précise. Cette information peut se faire sur plusieurs supports tels que le règlement Intérieur de l'entreprise ou encore le contrat de travail et contient, de manière non exhaustive :

- les modalités du traitement et ses finalités ;
- un rappel des droits de l'employé sur ses données ;
- si les données feront l'objet d'un transfert à une autre entité juridique (au sein d'un Groupe d'entreprises par exemple).

La collecte de certaines données (photographie du salarié par exemple) imposera l'obtention du consentement préalable du salarié concerné. Ce consentement devra être recueilli de façon explicite et non équivoque pour les traitements concernés, notamment par un écrit ou une case à cocher (**RGPD, art. 7**).

L'EXIGENCE DE MINIMISATION DES DONNÉES PERSONNELLES COLLECTÉES

Si l'employeur est amené à traiter un nombre important de données personnelles, il doit pour autant et conformément à **l'article 5 du RGPD**, ne traiter que les données nécessaires à l'objectif pour lequel il traite ces données.

Par exemple, lors de la phase de recrutement d'un salarié, les données collectées devront être limitées à celles strictement nécessaires à l'évaluation des capacités du candidat à occuper le

poste proposé. Par conséquent, les formulaires de candidature ne peuvent imposer la divulgation de la situation matrimoniale d'un candidat ou l'étendue de sa paternité.

Des modalités particulières sont par ailleurs prévues pour les emplois où un extrait du casier judiciaire est nécessaire. Dans ce cas, l'employeur a l'interdiction de conserver ledit extrait ou des notes relatives à celui-ci.

LA RECONNAISSANCE DU DROIT DE L'EMPLOYÉ SUR SES DONNÉES PERSONNELLES

Le RGPD créé également de nouveaux droits comme le droit à la portabilité des données personnelles ou le droit à l'oubli. Tout salarié pourra saisir son service RH (ou la personne désignée) pour exercer les droits qu'il détient sur ses données personnelles. Sa demande devra être suivie d'une réponse dans le mois, ce qui implique la mise en place de mesures techniques adaptées pour respecter ce délai (**RGPD, art. 3**).

L'employeur doit donc mesurer la problématique du stockage de ces données puisqu'il devra connaître leur emplacement exact afin de répondre efficacement aux demandes des salariés.

LA DURÉE DE CONSERVATION DES DONNÉES PERSONNELLES DES SALARIÉS

Les données personnelles des salariés ne peuvent être conservées que pour la durée nécessaire (**RGPD, art. 5)** :

- à l'exécution de leur contrat de travail ;
- et/ou au respect d'obligations légales (fiscales par exemple) ;
- et/ou à l'accomplissement de l'objectif qui était poursuivi lors de leur collecte.

À titre d'illustrations, les données collectées sur un candidat non retenu à l'embauche doivent être effacées deux ans après le dernier contact et les données personnelles d'un salarié relatives à la paie ne peuvent être conservées au-delà de cinq ans.

L'ACCÈS DES SALARIÉS À LEURS DOSSIERS PROFESSIONNELS

L'EXERCICE ACTUEL DES DROITS DU SALARIÉ SUR SON DOSSIER PROFESSIONNEL

L'article 39 de la Loi « *Informatiques et Libertés* » du 6 janvier 1978 permettait déjà aux salariés d'exercer leur droit d'accès auprès de leur employeur et d'exiger de lui la confirmation que ses données sont traitées ou non, les finalités du traitement, le destinataire des données, la catégorie des données traitées, le transfert éventuel des données, la copie des données.

Toutefois, force était de constater que les entreprises ne respectaient pas forcément ce droit. En effet, certaines refusaient l'accès des salariés à leurs dossiers professionnels, notamment dans le cadre de litiges entre le salarié et l'entreprise.

Ainsi, en 2016, 14 % des plaintes reçues par la Commission Nationale Informatique et Liberté (CNIL) concernaient les ressources humaines.

Le Règlement général sur la protection des données (RGPD), qui entre en vigueur le 25 mai 2018, va changer la donne.

LES NOUVEAUX DROITS DU SALARIÉ SUR SON DOSSIER PERSONNEL

Outre les informations que le responsable de traitement devait déjà fournir à la personne concernée qui en faisait la demande, **l'article 15 du RGPD** en liste de nouvelles :

- La durée de conservation des données
- Les garanties particulières prises en cas de transfert de données vers un pays tiers ou une organisation internationale
- L'existence d'une décision automatisée fondée sur un profilage

L'employeur doit également rappeler au salarié qui exerce son droit d'accès qu'il détient d'autres droits :

- Le droit à rectification et à effacement des données
- Le droit de réclamation auprès d'une autorité de contrôle

Ces informations doivent être communiquées par écrit au salarié qui en fait la demande, et peut l'être sous forme électronique lorsque la demande a été présentée sous cette forme.

En outre, le RGPD ne prévoit pas le paiement de frais basés sur les coûts administratifs du Responsable. La copie doit donc être gratuite même si les copies ultérieures peuvent être payantes.

L'exercice de ce droit d'accès ne doit évidemment pas impacter négativement les droits et libertés du salarié.

Le renforcement du droit d'accès par le RGPD augmentera nécessairement le nombre de réclamations des salariés pour mieux contrôler l'évolution de leurs carrières, réclamations elles-mêmes rendues plus accessibles. Les employeurs devront donc prendre soin de se conformer pleinement au RGPD dans la tenue des dossiers du personnel, et notamment de ne pas glisser dans les dossiers professionnels des informations qui ne devraient pas s'y trouver (appréciations subjectives sur le caractère du salarié, par exemple).

Ce nouveau droit d'accès demandera également une mise à jour des procédures internes pour traiter ces demandes salariales.

RGPD QUELS SONT LES IMPACTS SUR LA BDES ?

Le RGPD peut notamment avoir des répercussions qui sont liées au contenu de la BDES et aux accès accordés.

RGPD : IMPACT SUR LES OBLIGATIONS DE L'EMPLOYEUR CONCERNANT LE CONTENU DE LA BDES

La base de données économique et sociale (BDES), obligatoire pour les entreprises d'au moins 50 salariés sous peine de sanction, centralise les informations à communiquer aux représentants du personnel.

Même si cela n'est pas systématique, il se peut que certaines données personnelles soient mentionnées dans le contenu de la BDES.

Si le règlement européen a supprimé toutes les déclarations préalables à la CNIL concernant la BDES, il impose toutefois qu'un registre de traitement soit établi à chaque collecte de données. Les données personnelles qui peuvent apparaître dans la base de données sont celles permettant d'identifier une personne de manière directe ou indirecte.

RGPD : IMPACT SUR LA FORME DE LA BDES

Le RGPD doit amener à s'interroger sur la sécurité apportée à la BDES.

Cette dernière ne doit pas être accessible trop aisément comme par exemple un simple classeur rangé dans un placard non fermé à clef. Mieux vaut privilégier une BDES numérique où il sera plus simple d'assurer un niveau de sécurité élevé : données cryptées, accès par codes, etc.

Cependant, si la base de données est numérique et que vous avez accordé des accès particuliers selon les différents représentants, des données personnelles pourront être captées pour créer les accès. Il ne faudra pas oublier dans ce cas de le mentionner dans le registre de traitement.

LES DISPOSITIONS PARTICULIÈRES

Certaines activités peuvent exercer un droit de réserve sur le respect in extenso du traitement des données à caractère personnel notamment :

- le traitement au regard de la **liberté d'expression et d'information**
- le traitement et **l'accès du public** aux **documents officiels**
- **les garanties et dérogations applicables** aux traitements à des **fins** archivistiques d'intérêt public, de recherche scientifique, de recherche historique ou à des statistiques
- **les obligations de secret** pour respecter la Sécurité et La Défense nationale et la Sécurité publique
- **les règles existantes** des **églises** et **associations religieuses** en matière de protection des données.

ANNEXE

Les Terminologies officielles

Voici à ce jour, les termes officiels qu'il convient de s'approprier pour bien comprendre le fond et le sens de cette nouvelle réglementation.

1. « **données à caractère personnel** », toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale

2. «**traitement**», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction

3. «**limitation du traitement**», le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur

4. «**profilage**», toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique

5. «**pseudonymisation**», le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable

6. «**fichier**», tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique

7. «**responsable du traitement**», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du

traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre

8. « **sous-traitant** », la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement

9. « **destinataire** », la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement

10. « **tiers** », une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel

11. « **consentement** » de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement

12. «**violation de données à caractère personnel**», une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données

13. « **données génétiques** », les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question

14. «**données biométriques**», les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques

15. « **données concernant la santé** », les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne

16. « **établissement principal** », en ce qui concerne un responsable du traitement établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens du traitement de données à caractère

personnel soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement a le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal.

17. en ce qui concerne un sous-traitant établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union ou, si ce sous-traitant ne dispose pas d'une administration centrale dans l'Union, l'établissement du sous-traitant dans l'Union où se déroule l'essentiel des activités de traitement effectuées dans le cadre des activités d'un établissement du sous-traitant, dans la mesure où le sous-traitant est soumis à des obligations spécifiques en vertu du présent règlement

18. « **représentant** », une personne physique ou morale établie dans l'Union, désignée par le responsable du traitement ou le sous-traitant par écrit, en vertu de l'article 27, qui les représente en ce qui concerne leurs obligations respectives en vertu du présent règlement

19. « **entreprise** », une personne physique ou morale exerçant une activité économique, quelle que soit sa forme juridique, y compris les sociétés de personnes ou les associations qui exercent régulièrement une activité économique

20. « **groupe d'entreprises** », une entreprise qui exerce le contrôle et les entreprises qu'elle contrôle

21. « **règles d'entreprise contraignantes** », les règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe

22. « **autorité de contrôle** », une autorité publique indépendante qui est instituée par un État membre en vertu de l'article 51

23. « **autorité de contrôle concernée** », une autorité de contrôle qui est concernée par le traitement de données à caractère personnel parce que:

24. le responsable du traitement ou le sous-traitant est établi sur le territoire de l'État membre dont cette autorité de contrôle relève

25. des personnes concernées résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectées par le traitement ou sont susceptibles de l'être ou

26. une réclamation a été introduite auprès de cette autorité de contrôle

27. « **traitement transfrontalier** »,

28. un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres, ou

29. un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres

30. « **objection pertinente et motivée** », une objection à un projet de décision quant à savoir s'il y a ou non violation du présent règlement ou si l'action envisagée en ce qui concerne le responsable du traitement ou le sous-traitant respecte le présent règlement, qui démontre clairement l'importance des risques que présente le projet de décision pour les libertés et droits fondamentaux des personnes concernées et, le cas échéant, le libre flux des données à caractère personnel au sein de l'Union

31. « **service de la société de l'information** », un service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil

32. « **organisation internationale** », une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d'un tel accord.