Cabinet RIERA
Lettre d'information – Mars 2019

Dossier spécial : RGPD et entreprise : un enjeu pour les syndicats

AU SOMMAIRE

Pour un complément d'information, les Avocats du Cabinet RIERA se tiendront à votre disposition :

- **Maître Dominique RIERA, cabinet.riera@avocatem.com**
- **Maître Zahra AMRI-TOUCHENT, amri-touchent@avocatem.com**
- **Maitre Farida ASSAM, assamfarida@gmail.com**

RGPD et entreprise : un enjeu pour les syndicats

Face à la numérisation croissante de notre société, nos données personnelles ont pris de plus en plus de valeur et peuvent faire l'objet de dérives (*réseaux sociaux*) ou de menaces (*cybercriminalité*).

C'est pourquoi il était nécessaire de réaffirmer l'importance de la vie privée (*article 9 du code civil*) et de sa protection dans une nouvelle dynamique de sensibilisation collective.

Le GDPR pour General Data Protection Regulation ou encore en français RGPD Règlement Général sur la Protection des Données est un règlement européen qui détaille les nouvelles obligations liées à l'utilisation des données personnelles. Il concerne la législation sur les données personnelles et est entré en vigueur le 25 mai 2018.

Le RGPD renforce la protection des individus quant à l'utilisation qui pourrait être faite de leurs données personnelles. Avec ce règlement, il y a une inversion de méthode par rapport à la loi précédente : d'un contrôle à priori par obligation de déclaration, ce nouveau règlement met en place un contrôle à posteriori des organisations détenant des données personnelles par la CNIL.

Le RGPD poursuit plusieurs objectifs ambitieux :

- uniformiser au niveau européen la réglementation sur la protection des données ;
- responsabiliser davantage les structures concernées en développant l'autocontrôle ;
- renforcer le droit des personnes (*droit à l'accès, droit à l'oubli, droit à la portabilité, etc.*).

Qui est concerné par ce nouveau règlement ?

Le Règlement Européen sur la Protection des Données personnelles concerne toutes les structures qui rassemblent des données personnelles.

Depuis 25 mai 2018 toutes les organisations doivent à minima avoir entrepris les démarches pour se mettre en conformité avec ce règlement. Il s'applique aux acteurs économiques et sociaux, les entreprises bien sûr mais donc aussi les associations, les fondations, les administrations, les collectivités, les CSE … et les syndicats.

En revanche, le RGPD ne s'applique pas aux particuliers, c'est-à-dire, selon l'article 18 du règlement, aux personnes physiques qui effectuent des traitements de données à caractère personnel au cours d'activités strictement personnelles ou domestiques. Ces traitements de données doivent être sans lien avec une activité professionnelle ou commerciale.

Un simple nom est donc une donnée personnelle

Définition : une donnée personnelle correspond à toute information se rapportant à une personne physique identifiée ou identifiable […] directement ou indirectement

On entend par **donnée personnelle** toute information permettant d'identifier directement (*nom, prénom, par exemple*) ou indirectement (*numéro client, numéro de téléphone, numéro d'immatriculation pour la gestion d'un parking, donnée biométrique, etc.*) une personne. Une personne peut ainsi être identifiée à partir d'une seule donnée (*exemples : numéro de sécurité sociale*) ou à partir du croisement d'un ensemble de données (*personne vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association*)

La notion de **fichier** recouvre 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 (*exemple : dossiers classés par ordre alphabétique ou chronologique*).

Un **traitement de données personnelles** est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (*collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement*).

De ce fait, une liste de personnes gérée par un syndicat rentre dans le cadre de cette réglementation et le syndicat doit s'y conformer.

Un syndicat, qui collecte et utilise des informations sur les salariés de l'entreprise (*par exemple : le nom, le prénom, l'adresse e-mail, l'adresse postale, le numéro de téléphone, ...*) doit avoir au moins entrepris les actions nécessaires à la mise en conformité de sa base (ou ses bases) de données.

En cas de contrôle, il doit être en mesure de présenter son plan d'action et montrer les premières étapes mises en place.

Remarque : le RGPD s'applique aussi bien aux données papier qu'aux données numériques

Les grands principes

Pour un syndicat, être en conformité avec le RGPD signifie :

- demander et sauvegarder le consentement des personnes pour le traitement des données les concernant,
- informer la CNIL et les personnes concernées (*dans les 72 heures*) si leurs données personnelles ont été piratées dans la base,
- collecter uniquement les renseignements dont le syndicat a besoin,
- laisser la possibilité aux personnes dont les données sont collectées de connaître les éléments que le syndicat conserve sur elles,
- tracer l'ensemble des documents mis en place servant au traitement des données personnelles.

Le RGPD est l'occasion de questionner les pratiques du syndicat et des IRP en général et de reprendre les données qu'il collecte. Questionner la pertinence de ses collectes permet de mettre de l'ordre dans les bases de données du syndicat.

Tout salarié qui confie ses données personnelles au syndicat établit avec lui une relation de confiance et souhaite le respect de ses droits et de sa vie privée.

Le RGPD réaffirme les droits pour les salariés concernés de maîtriser leurs données en leur conférant des droits : droits d'accès, de rectification, d'effacement, d'opposition, etc. Respecter ces droits contribue à valoriser une image de sérieux et de responsable du syndicat.

Le RGPD est donc une opportunité de sceller une relation de confiance entre le syndicat et les salariés de l'entreprise.

Un enjeu syndical

Le RGPD est aussi une opportunité de sceller une relation de confiance entre les organisations syndicales et les salariés.

En effet, l'article 88 Règlement Général de Protection des Données concerne le *traitement des données dans les relations de travail*. Il prévoit en particulier une articulation possible entre le RGPD et des conventions collectives qui viendraient préciser les garanties apportées au respect des droits des travailleurs :

Les États membres peuvent prévoir, par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail, aux fins, notamment, du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de l'égalité et de la diversité sur le lieu de travail, de la santé et de la sécurité au travail, de la protection des biens appartenant à l'employeur ou au client, aux fins de l'exercice et de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail.
Ces règles comprennent des mesures appropriées et spécifiques pour protéger la dignité humaine, les intérêts légitimes et les droits fondamentaux des personnes concernées, en accordant une attention particulière à la transparence du traitement, au transfert de données à caractère personnel au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe et aux systèmes de contrôle sur le lieu de travail.

Cet article peut faire de la protection des données des travailleurs un enjeu de négociation syndicale et de démocratie sociale, envisagé d'emblée avec une dimension collective.

Cela rejoint l'idée d'un droit social des données et d'une protection sociale des données, mais envisagés sous l'angle de la sphère professionnelle.

Le RGPD prévoit que ses règles protectrices envers les salariés pourraient être remises en cause partiellement en fonction des *intérêts légitimes* des entreprises en matière de traitement de données.

La mise en œuvre du RGPD ne doit donc pas relever d'une définition unilatérale par les employeurs. Cela peut au contraire devenir un enjeu de négociation collective et de démocratie sociale.

Il s'agit de renouer avec les grands principes fondateurs du droit du travail, comme le principe de faveur et la hiérarchie des normes, qui ont reçu des coups très rudes avec la loi El Khomri et les ordonnances Macron, mais qui pourraient retrouver tout leur sens en matière de protection des données des employés : les normes inférieures – en l'occurrence les conventions collectives – viendraient en la matière ajouter des garanties supplémentaires par rapport au socle légal que constitue le RGPD.

C'est pourquoi il paraît essentiel que la protection des données devienne un enjeu syndical, notamment pour venir compenser le déséquilibre des forces en présence en ne laissant pas les salariés isolés face aux employeurs pour défendre leur vie privée. C'est dire en somme que l'intérêt légitime

de l'entreprise ne sera vraiment *légitime* que s'il est collectivement discuté selon les principes de la démocratie sociale.

Ce qui est vrai au niveau des conventions collectives l'est aussi au niveau individuel de l'entreprise dans le cadre d'un accord. Les organisations syndicales doivent se saisir de la problématique RGPD pour finaliser un accord dans l'entreprise concernant le traitement des données des salariés. Traitement réalisé par l'employeur, mais aussi par le CSE et les organisations syndicales elles-mêmes.

Fiche 1 Le syndicat en tant que représentant du personnel dans l'entreprise

De très nombreuses données personnelles relatives aux salariés sont nécessaires pour la gestion de leur carrière au sein de l'entreprise.

Par exemple, l'employeur a besoin de beaucoup d'informations pour assurer :

- la rémunération et les déclarations sociales obligatoires ;
- la tenue du registre unique du personnel ;
- la gestion administrative du personnel (*exemple : type de permis de conduire détenu ou coordonnées de personnes à prévenir en cas d'urgence*) ;
- l'organisation du travail (*exemple : photographie facultative de l'employé pour les annuaires internes et organigrammes*) ;
- l'action sociale prise en charge par l'employeur (*exemple : les informations concernant les ayants-droit de l'employé*).

L'employeur ne peut demander aux salariés que les informations utiles pour accomplir ces missions, et éviter de traiter des données dites *sensibles* (*activité syndicale, opinions politiques, religion, origine ethnique, santé*).

L'employeur dispose forcément d'informations particulières (*et donc à risque*) sur les salariés (*coordonnées bancaires pour la paie, numéro de sécurité sociale pour les déclarations sociales, etc.*).

Il doit donc s'assurer d'en garantir la confidentialité et la sécurité. Ainsi, seules les personnes habilitées doivent en prendre connaissance. Les actions sur les données effectuées par les personnes habilitées doivent être enregistrées (*savoir qui se connecte à quoi, quand et pour faire quoi*).

L'employeur doit informer les salariés à chaque fois qu'il leur demande des informations (*exemple : mise à jour des données administratives, demande de formation, formulaire d'entretien d'évaluation, etc.*).

Enfin, les salariés peuvent demander une copie de toutes les données les concernant détenues par l'employeur : copie d'un bulletin de paie, état d'un compte épargne-temps, mais aussi les enregistrements téléphoniques, relevés des badgeuses, ou encore des messages envoyés via le mail professionnel, y compris lorsqu'un employé n'est plus en poste ou est en litige avec l'employeur.

Certaines données des salariés sont accessibles aux représentants des salariés. Les syndicats peuvent consulter les données figurant dans le registre unique du personnel (*nom, nationalité, fonction occupée, date d'entrée dans l'organisme, etc.*).

Le syndicat peut, après information des salariés et en l'absence d'opposition, avoir accès à certaines données.

Les entreprises, et donc les syndicats, n'ont plus de formalités à déclarer auprès de la CNIL. En contrepartie, ils doivent tout mettre en œuvre pour assurer le respect des principes de la protection des données personnelles des salariés. S'ils ne le font pas, ils s'exposent à des sanctions bien plus élevées qu'auparavant.

Le rôle des institutions représentatives du personnel (*IRP*) est de s'assurer que les grands principes sur la protection des données sont respectés. Elles doivent en particulier s'assurer que l'utilisation des données personnelles par l'entreprise ne soit pas opaque pour les salariés.

Les représentants du personnel doivent contrôler les principes suivants. Ils sont au nombre de six :

Tout d'abord, la ***légalité***. L'entreprise doit justifier sur quelle base légale elle collecte les données des salariés : respect de la loi, obligations découlant du contrat de travail... L'intérêt légitime de l'entreprise peut également justifier un traitement, à condition qu'il ne devienne pas une justification *fourre-tout* ! L'entreprise qui se base sur son intérêt légitime doit être prudente et prendre des mesures beaucoup plus fortes pour justifier le traitement et assurer la sécurité des données.

Ensuite, la ***finalité*** : à quoi va servir le traitement ? Une caméra placée à l'extérieur de l'entreprise peut être utile pour des raisons de sécurité, mais elle ne doit pas être orientée vers un salarié à son poste de travail, ou bien pointer vers le local syndical.

Le traitement doit également être ***proportionné*** à la finalité. Lorsque l'entreprise met en place des dispositifs de contrôle restrictifs pour les libertés des salariés, les syndicats doivent se demander s'il n'y avait pas un autre moyen, moins invasif, d'assurer ce contrôle. Par exemple, le RGPD autorise l'employeur à recourir à l'utilisation des données biométriques des salariés (*empreintes digitales ou rétinienne, reconnaissance faciale, etc.*). Or ce sont des données très sensibles car intimement liées à la personne. Il faut toujours se demander si l'on peut recourir à un autre moyen, par exemple poster un vigile pour protéger l'entrée à certains lieux, plutôt que d'utiliser la biométrie.

Les représentants du personnel doivent vérifier la ***loyauté*** du traitement. Ils doivent s'assurer que le traitement n'est pas utilisé à d'autres fins que celles pour lequel il a été mis en place. Par exemple, l'employeur peut invoquer la sécurité de l'entreprise pour justifier la fourniture d'un badge d'accès à un salarié pour lui permettre d'entrer sur les lieux de travail. En revanche, le badge ne doit pas être utilisée pour traquer les déplacements du salarié dans l'entreprise. Des questions peuvent également se poser si ce même badge permet au salarié de payer son repas à la cantine : le badge enregistre-t-il le fait que le salarié ne mange pas de porc, ou qu'il est vegan ?

Le traitement doit enfin assurer la qualité des données collectées, garantir une ***durée de conservation limitée***, et assurer la ***sécurité des données*** conservées (*face aux hackeurs notamment*).

Article L 2312-38
Le comité social et économique est informé, préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi ainsi que sur toute modification de celles-ci.
Il est aussi informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci.
Le comité est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés.

Le code du travail impose d'informer et consulter les représentants du personnel préalablement à la mise en œuvre ou la modification de certains traitements automatisés :

- l'information-consultation portant sur les traitements automatisés de gestion du personnel et à leur modification, préalablement à leur introduction dans l'entreprise (*article L 2312-38*) ;
- les représentants du personnel doivent également être informés de la désignation d'un correspondant à la protection des données à caractère personnel et de la désignation d'un délégué à la protection des données (*DPO*). Cette désignation, obligatoire uniquement dans les entreprises qui traitent des données à grande échelle, est largement recommandée à toutes les entreprises par la CNIL ;
- la consultation doit prévoir les éléments qui justifient le recours à une collecte de données ;
- les IRP doivent également être informées et consultées sur les chartes informatique et interne de protection des données personnelles, documents généralement annexés au règlement intérieur.

Diffusion des communications syndicales

Selon l'article L 2142-6, un accord d'entreprise peut définir les conditions et les modalités de diffusion des informations syndicales au moyen des outils numériques disponibles dans l'entreprise.

A défaut d'accord, les organisations syndicales présentes dans l'entreprise peuvent mettre à disposition des publications et tracts sur un site syndical accessible à partir de l'intranet de l'entreprise, lorsqu'il existe.

L'utilisation par les organisations syndicales des outils numériques mis à leur disposition doit satisfaire l'ensemble des conditions suivantes :

- être compatible avec les exigences de bon fonctionnement et de sécurité du réseau informatique de l'entreprise ;
- ne pas avoir des conséquences préjudiciables à la bonne marche de l'entreprise ;
- préserver la liberté de choix des salariés d'accepter ou de refuser un message.

De plus dans les entreprises de moins de 300 salariés et dans les établissements appartenant à ces entreprises, le délégué syndical est, de droit, représentant syndical au comité social et économique.

Le délégué syndical est, à ce titre, destinataire des informations fournies au comité social et économique.

Un enjeu syndical à saisir

À travers la collecte (*big data*) et l'exploitation (*Intelligence artificielle*) des données par l'entreprise, c'est la place de l'homme et de la femme dans le travail de demain qui est en jeu. Les représentants du personnel ont un rôle primordial à jouer, la protection des données devient donc une nouvelle mission des IRP.

Il s'agit de s'emparer du sujet au plan collectif comme au plan individuel, à travers le syndicat ou la négociation d'accords collectifs permettant de négocier :

- un code de bonne conduite au sein de l'entreprise ;
- la mise en place d'une commission de veille ;
- l'accès aux certifications des prestataires, aux études d'impact ou le déclenchement d'un audit ;
- le contrôle de la mise en place opérationnelle des dispositifs pour vérifier qu'ils ne sont pas utilisés à d'autres fins ;

- la mise en conformité de fichiers locaux (*par exemple le cas des managers de proximité qui peuvent constituer des fichiers à leur seule destination contenant des données personnelles de leurs collaborateurs*) ;
- ou dans le cadre du pouvoir disciplinaire de l'employeur, les griefs qui pourraient être utilisés à l'encontre d'un salarié qui viendrait, par exemple, s'appuyer sur des données personnelles d'un client, doivent avoir fait l'objet d'une autorisation préalable de la part du client, d'utiliser ses données personnelles.

Fiche 2 Les données à caractère personnel détenues par le syndicat

Les rôles traditionnels des syndicats sont de deux ordres :

- un rôle de représentation des salariés,
- un rôle de négociation.

C'est ainsi que les syndicats s'attachent à garantir les droits des salariés dans l'entreprise, en termes de salaires, de statuts, de progression de carrière ou de conditions de vie.

Les syndicats disposent d'une grande liberté d'action :

- les syndicats disposent de moyens d'actions au sein de l'entreprise : notamment un local syndical permettant de se réunir, l'affichage de documents et de tracts syndicaux.
- les syndicats peuvent négocier avec l'employeur afin de défendre les droits et les intérêts de leurs adhérents et de tous les salariés de l'entreprise en général.
- en cas de conflit les syndicats peuvent engager des actions de protestation (*grèves, manifestations, pétitions...*).

Enfin, à l'échelle de l'entreprise, l'objectif des syndicats est d'agir dans le but de préserver les intérêts des salariés et d'en acquérir des nouveaux. Ils sont le relais entre le salarié et la direction mais aussi entre l'entreprise et le monde extérieur.

A ce titre, le délégué syndical représente son syndicat auprès de l'employeur et assure la défense des salariés. Il peut notamment :

- formuler des propositions, des revendications ou des réclamations,
- assister le salarié qui le souhaite lors d'un entretien préalable à une sanction disciplinaire,
- assister les salariés auprès du conseil des prud'hommes.

Chaque année, les délégués syndicaux négocient avec l'employeur sur les sujets suivants :

- salaires, durée et organisation du temps de travail
- objectifs d'égalité professionnelle entre hommes et femmes
- mesures relatives à l'insertion professionnelle et au maintien dans l'emploi des travailleurs handicapés.

L'employeur doit aussi engager chaque année, en l'absence d'accord existant, une négociation avec les délégués syndicaux sur les sujets suivants :

- épargne salariale (*intéressement, participation ou plan d'épargne*)
- conditions de mise en place d'un régime de prévoyance maladie
- droit d'expression des salariés.

L'employeur et les syndicats peuvent également à tout moment, en dehors des négociations obligatoires, négocier sur des thèmes qu'ils choisissent comme par exemple la mise en place du RGPD dans l'entreprise.

Avec le temps et le développement du syndicat (*au niveau national ou au niveau de l'entreprise*), le volume de données augmente et nécessite de mobiliser de plus en plus de moyens humains et techniques (*espace de stockage, logiciels adaptés, etc.*) pour les gérer, les mettre à jour, et en assurer la sécurité.

Le principe de « minimisation » des données (*Je ne collecte que les données dont j'ai vraiment besoin*) et l'obligation de tenir à jour la liste de ses fichiers permet au syndicat de faire le point sur les données qu'il collecte et d'identifier ses besoins réels.

Le RGPD exige par ailleurs que les données soient pertinentes par rapport à l'objectif pour lequel le syndicat collecte les données. Appliquer ces principes lui permet donc d'optimiser ses investissements.

L'arrivée du RGPD est ainsi une occasion forte de se poser les bonnes questions sur son activité et ses process (*comme cela a été par exemple le cas lors du passage du papier à la dématérialisation*).

La protection joue dès lors qu'il y a traitement de données par moyen électronique ou sous forme papier, quel qu'en soit le stade :

- la collecte, c'est-à-dire la récupération des données personnelles. Elle doit être faite exclusivement auprès des personnes concernées, avec leur accord préalable, et ce même si les données sont fournies par un partenaire. Elle peut être effectuée par le biais d'une fiche de renseignements, d'un bordereau d'inscription, d'un formulaire sur un site internet, par exemple.
- l'enregistrement : une fois les données collectées, l'action de les enregistrer dans une base de données, électronique ou non, est un traitement de données.
- la conservation : dès le stockage d'une donnée personnelle, il est nécessaire de définir la durée de conservation. En effet, il n'est pas utile de garder les données personnelles en dehors de la durée de leurs traitements. Cela accroît le risque de perte ou de violation de données.
- la communication, le transfert et l'interconnexion : l'exportation de données personnelles est soumise au RGPD. Il n'est pas autorisé de transférer les données sans autorisation explicite des personnes concernées.

Prospection syndicale

La prospection syndicale rentre dans le cadre du RGPD. La décision de la CNIL en date du 16 février 2012 rendue à l'encontre d'un syndicat en est une parfaite illustration.

En l'espèce, un syndicat des établissements d'enseignement supérieur de l'Académie de Lille avait envoyé plusieurs courriels de prospection syndicale (*et non commerciale*) non sollicités, sur les adresses de messagerie électronique professionnelle des salariés de l'Université de Lille 1.

Suite à ces envois, une des salariés a adressé au syndicat plusieurs demandes d'opposition. Le syndicat n'ayant donné aucune réponse à ses demandes, la salariée avait saisi la CNIL.

La CNIL avait mis en demeure le syndicat, par sa décision n° 2011-004 du 19 mai 2011, dans un délai d'1 mois à compter de sa notification, de :

- préciser les moyens par lesquels il a pris connaissance de l'adresse électronique des personnels de l'Université de Lille 1 et veiller à ne pas collecter des données à caractère personnel de manière déloyale ou illicite, en particulier ne pas collecter d'adresse électronique à des fins de prospection syndicale à l'insu des personnes concernées ;
- préciser les raisons pour lesquelles le droit d'opposition de la plaignante n'a été pris en compte que tardivement ;
- prendre toute mesure de nature à garantir qu'il soit tenu compte, de manière immédiate et systématique, du droit d'opposition exercé par toute personne concernée en application de l'article 38 de la loi du 6 janvier 1978 ;
- etc.

La CNIL avait alors considéré que le syndicat avait commis plusieurs manquements, notamment au titre de la collecte loyale des données (*article 6 1° LIL*). A cet égard, la CNIL avait relevé que :

- il est établi que le syndicat a fait usage, à des fins de prospection syndicale, d'adresses de messageries électroniques professionnelles.
  Celles-ci constituent des données à caractère personnel au sens de la loi du 6 janvier 1978 modifiée, dès lors qu'elles contiennent des informations relatives à des personnes physiques identifiées ou qui peuvent être identifiées au sens de l'article 2 alinéa 2 de la loi précitée.
- sur le fond, la CNIL constate qu'il ressort des termes de la plainte que l'intéressée n'a jamais sollicité d'envois de messages de prospection syndicale sur son adresse des messagerie professionnelle et qu'elle n'a jamais été informée préalablement à cette prospection.
  Elle considère, dès lors, qu'elle ne peut écarter le grief de collecte déloyale formulé à l'encontre du syndicat.

Avec l'application imminente du RGPD le 25 mai 2018, la vigilance sur ces sujets doit être accrue ainsi qu'une gestion rigoureuse des droits des personnes concernées.

Cela suppose de mettre en place au plus vite des actions de sensibilisation pour toutes les organisations, quelle que soit leur taille

Mise en œuvre du RGPD par le syndicat

Il convient de revoir les bulletins d'adhésion en intégrant une case à cocher, comme celle proposée par la CNIL :
« Si vous ne souhaitez pas recevoir les informations (mail et courrier postal) et newsletter de la part du syndicat xxxxx….merci de cocher cette case. »

De plus, l'organisation syndicale doit vérifier et mettre à jour régulièrement la base de données et veiller à ce que la mention relative à la désinscription soit bien présente et bien effective à la fin du courrier/courriel/sms adressé.

Il est également recommandé d'intégrer sur le site internet, dans l'hypothèse d'une collecte de données personnelles la mention suivante à adapter bien sûr en fonction de la situation :
Les données à caractère personnel ainsi collectées font l'objet d'un traitement dont le responsable est [nom du syndicat et adresse – à compléter selon le cas].
Ces données sont collectées [par exemple dans le cadre des relations entre le syndicat et ses adhérents …. - à compléter selon le cas] et sont nécessaires à [par exemple la fourniture et à l'utilisation d'informations - à compléter selon le cas].
Elles sont destinées aux services en charge de [à compléter selon le cas], ainsi qu'aux prestataires externes auxquels le responsable de traitement fait appel [à adapter au cas d'espèce].
Elles seront conservées pendant [indiquer une durée : par exemple deux ans ou toute la durée d'adhésion ou toute la durée de l'utilisation du service ...]
Conformément à la règlementation applicable en matière de données à caractère personnel, vous disposez d'un droit d'accès, de rectification, d'opposition, de limitation du traitement, d'effacement et de portabilité de vos données que vous pouvez exercer [indiquer les modalités (par mail, par courrier...) et préciser l'adresse], en précisant vos nom, prénom, adresse et en joignant une copie recto-verso de votre pièce d'identité.

Lorsque les conversations téléphoniques sont susceptibles d'être enregistrées, il s'agit d'un traitement de données à caractère personnel. Il est donc nécessaire d'informer les personnes concernées (*salariés*

ou autres) de l'existence de cet enregistrement, même par oral, au début de la conversation téléphonique.
Afin d'améliorer la qualité du service, nous vous informons que la conversation téléphonique est susceptible d'être enregistrée par [nom du responsable de traitement]. Les données ainsi enregistrées sont à destination de [indiquer les destinataires] et sont strictement nécessaires à l'amélioration du service. Cet enregistrement sera conservé [durée de conservation].
Vous pouvez vous opposer à cet enregistrement.
Conformément à la réglementation en vigueur en matière de protection des données personnelles, vous disposez d'un droit d'accès aux informations vous concernant, ainsi qu'un droit de rectification, d'opposition, de limitation du traitement et de suppression que vous pouvez exercer par courrier/par mail en vous adressant à : adresse postale/adresse électronique.

Ce que le syndicat doit faire pour se conformer au RGPD

Comme toute entité traitant de données â caractère personnel, le syndicat doit désigner un responsable du traitement des données à caractère personnel.

D'après la CNIL, pour une société, le responsable du traitement est d'une manière générale *la personne morale incarnée par son représentant légal*. L'organisation syndicale dans l'entreprise doit désigner expressément un responsable du traitement des données.

D'après les textes légaux, c'est à ce responsable qu'il appartient de mettre en œuvre toutes les mesures appropriées pour démontrer que le ou les traitements dont il a la responsabilité sont effectués en conformité avec le RGPD. A ce titre, il doit réaliser et tenir un registre de traitement des données, qui permettra de prouver que le CSE respecte bien le RGPD.

L'organisation syndicale peut également décider de désigner un Délégué à la Protection des Données (*DPO*), qui pourra assister le responsable du traitement. Cette désignation n'est pas obligatoire mais peut s'avérer opportune pour les syndicats gérant un fichier important de salariés.

Le responsable du traitement doit mettre en place et tenir un registre de traitement des données qui liste, activité par activité du syndicat, les traitements de données personnelles.

Pour mettre en place ce registre, il convient de passer en revue les différentes activités du syndicat qui nécessitent la collecte et le traitement de données, et d'établir une fiche par activité.

Par exemple, la communication avec les salariés, les activités sociales et culturelles, etc. Chaque fiche doit comporter un certain nombre d'informations, parmi lesquelles :

- l'identité et les coordonnées du responsable du traitement,
- la finalité du traitement,
- les catégories de données utilisées,
- les personnes internes et externes au syndicat ayant accès aux données,
- la durée de conservation des données, etc.

La mise en place de ce registre doit être l'occasion de s'assurer que les données collectées sont bien utiles au syndicat, qu'elles ne sont pas conservées au-delà de ce qui est nécessaire et que seules les personnes habilitées ont seulement accès aux données dont elles ont besoin.

La mise en place du registre doit être l'occasion pour le syndicat de se poser une question, celle de savoir si les données collectées sont bien pertinentes et limitées à ce qui est nécessaire. Pas la peine

de demander des informations sur la situation de famille si le syndicat ne propose pas de prestations à leur destination.

L'organisation syndicale doit prendre toutes les mesures nécessaires pour garantir la sécurité des données. Par exemple :

- mise à jour des logiciels et de l'antivirus,
- changement régulier des mots de passe,
- création de différents profils utilisateurs,
- sécurisation du local du syndicat,
- insertion d'une clause de confidentialité dans le contrat de travail du salarié du syndicat,
- vérification des contrats conclus avec les prestataires utilisant les données personnelles,
- etc.

Le syndicat doit vérifier que les sous-traitant notamment les plateformes de billetterie en ligne, protègent correctement les données personnelles qu'ils reçoivent du syndicat car, en cas de *fuite de données*, le syndicat et le sous-traitant pourraient être coresponsables.

Remarque : le fait de sous-traiter n'exonère pas le syndicat de son obligation de respecter le RGPD.

Le Règlement prévoit également que, chaque personne qui fait l'objet d'une collecte de données personnelles la concernant, doit être informée de son droit :

- d'obtenir gratuitement une copie des données les concernant *(Article 15 du règlement)* ;
- de faire rectifier les données qui se révèleraient inexactes ou de les compléter *(Article 16 du règlement)* ;
- à l'effacement (*droit à l'oubli*), sous conditions, de ces données, notamment lorsqu'elles ne sont plus nécessaires, que l'intéressé s'oppose au traitement ou encore lorsqu'il retire son contentement *(Article 16 du règlement)* ;
- de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, au traitement des données, sauf motif légitime du responsable du traitement *(Article 21 du règlement)*.

Ainsi, pour pouvoir collecter et utiliser des données à caractère personnel, le syndicat a besoin du consentement, c'est-à-dire de l'accord, des salariés.

Ce consentement doit être obtenu préalablement à la mise en place du traitement des données et peut être recueilli de différentes manières (*document écrit signé par le salarié, formulaire à remplir, case à cocher sur le site du syndicat, etc.*).

Le syndicat doit fournir aux salariés un certain nombre d'informations relatives au traitement de données, parmi lesquelles :

- l'identité et les coordonnées du responsable du traitement,
- la finalité du traitement, c'est-à-dire ce à quoi il va servir,
- la durée de conservation des données,
- les personnes ayant accès aux données,
- etc.

Les salariés doivent également être informés de leur droit à accès, à rectification, à effacement, etc. Pour cela, on peut utiliser un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée pour permettre l'exercice de ces droits.

Lorsque les données ont été fournies au syndicat par l'employeur, les salariés doivent en plus être informés des catégories de données personnelles concernées et de la source des données personnelles.

Cependant, si les salariés ont déjà été informés par l'employeur, le syndicat est dispensé de son obligation d'information.

Questions

Le Responsable de la protection des données (*DPO*) de l'entreprise peut-il demander au syndicat de se justifier sur les mesures prises en matière de RGPD ?

> Il est plus que probable que le DPO se rapproche du syndicat pour s'enquérir des actions et des mesures prises par les responsables en matière de RGDP, dans la mesure où l'entreprise est susceptible de lui transmettre des données.

L'employeur peut-il refuser de transmettre les données relatives aux salariés ?

> Sous l'empire de l'ancienne loi, la CNIL dans une délibération du 17 octobre 2006 n° 2006-230 a déterminé très précisément les données qui pouvaient être transmise au syndicat dans le cadre de la gestion des œuvres sociales, à savoir, nom, prénom et coordonnées professionnelles.
> L'employeur avait déjà l'obligation formelle d'informer les salariés de cette transmission, de sa finalité et des modalités pour s'y opposer.
> Avec les nouvelles dispositions RGPD, l'employeur pourrait refuser de transmettre les données au syndicat, a fortiori, lorsqu'il sait que le syndicat n'a pas sécurisé leur traitement.

La responsabilité de l'employeur peut-elle être engagée en cas de problème avec les données transmises en syndicat (*fuites des informations personnelles des salariés par exemple*) ?

> Désormais avec les nouvelles obligations RGPD, c'est bien le syndicat qui est responsable du traitement et de la conservation des données qui lui sont transmises.
> Le syndicat pourra faire l'objet de sanctions administratives, civiles et pénales en cas de préjudice.
> Toutefois, si l'employeur transmet sciemment les données relatives aux salariés alors que le syndicat n'a pas initié les mesures de protection des données des salariés et de leurs ayants-droits, alors il semble que la responsabilité de l'employeur pourrait être recherchée.

Fiche 3 Syndicat : bonnes pratiques pour respecter le RGPD

Les bonnes pratiques suivantes intéressent les organisations syndicales ainsi que toutes structures concernées par le traitement de données :

DPD	Trouver un(e) responsable RGPD au sein de la structure (*association, entreprise, CSE, syndicat*) : Délégué à la protection des données (*DPD*) ou Responsable de la protection des données (*RPD*) ou DPO (*Data Protector Officer*)
	Missions d'information, de conseil et de contrôle en interne
	Cette personne sera un le pilote pour mener à bien la conformité de la structure. Qualités requises, doté de rigueur, d'organisation et s'intéresse au RGPD
	DPO : sensibilisation et formation de l'ensemble des salariés en collaboration avec l'employeur. Le but : que chacun puisse prendre en compte la réglementation en amont de chaque mission

Pour mesurer concrètement l'impact du règlement européen sur la protection des données traitées par le syndicat, il faut commencer par recenser de façon précise les traitements de données personnelles. L'élaboration d'un registre des traitements permet de faire le point

Un registre recensant les activités de traitement est obligatoire pour les entreprises de plus de 250 employés

En deçà de ce seuil, le registre reste obligatoire lorsque le traitement effectué :

- est susceptible de comporter un risque pour les droits et libertés des personnes concernées ;
- est non occasionnel ;
- concerne des données sensibles (*origine ethnique, opinion religieuse, donnée biométrique...*) et/ou relatives à des condamnations pénales et à des infractions.

Bilan	Qui	Identifier les responsables des services opérationnels traitant les données au sein de la structure
		Établir la liste des sous-traitant
	Quoi	Identifier les catégories de données traitées
		Identifier les données susceptibles de soulever des risques en raison de leur sensibilité particulière (*par exemple, les données relatives à la santé ou les infractions*)
	Pourquoi	Indiquer la ou les finalités pour lesquelles la structure collecte ou traite ces données (*exemple : gestion de la relation commerciale, gestion RH…*)
	Où	Déterminer le lieu où les données sont hébergées
		Indiquer quels pays les données sont éventuellement transférées
	Jusqu'à quand	Indiquer, pour chaque catégorie de données, combien de temps la structure les conserve
	Comment	Quelles mesures de sécurité sont mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées ?

Information	La structure a le devoir d'informer les salariés, adhérents, bénévoles, donateurs, bénéficiaires, etc. de ses actions
	Il en va de même pour leurs données. Si la structure les utilise, il faut les avertir et encore mieux, leur demander leur consentement au préalable

Priorités	Sur la base du registre, il faut identifier les actions à mener pour que la structure se conforme aux obligations actuelles et à venir
	Prioriser ces actions au regard des risques que font peser les traitements sur les droits et les libertés des personnes
	S'assurer que seules les données strictement nécessaires à la poursuite des objectifs sont collectées et traitées
	Identifier la base juridique sur laquelle se fonde le traitement (*exemples : consentement de la personne, intérêt légitime, contrat, obligation légale*)
	Réviser les mentions d'information afin qu'elles soient conformes aux exigences du règlement
	Vérifier que les sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités, la structure doit s'assurer 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
	Prévoir les modalités d'exercice des droits des personnes concernées (*droit d'accès, de rectification, droit à la portabilité, retrait du consentement...*)
	Vérifier les mesures de sécurité mises en place

S'il a été identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, la structure doit mener, pour chacun de ces traitements, une analyse d'impact relative à la protection des données, AIPD (*en anglais, Data protection impact assessment*)		
Gestion des risques	Quoi	C'est une analyse aidant à construire des traitements de données respectueux de la vie privée et permettant de démontrer la conformité de son traitement au RGPD. Une AIPD est un outil d'évaluation d'impact sur la vie privée. Elle repose sur 2 piliers : - les principes et droits fondamentaux, *non négociables*, fixés par la loi. Ils ne peuvent faire l'objet d'aucune modulation, quelles que soient la nature, la gravité et la vraisemblance des risques encourus ; - la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriée pour protéger les données personnelles
		Une AIPD contient : - une description du traitement étudié et de ses finalités ; - une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ; - une évaluation des risques pour les droits et libertés des personnes concernées les mesures envisagées pour faire face aux risques
	Quand	De manière générale, réaliser une AIPD est une bonne pratique pour s'assurer de créer un traitement conforme au RGPD et respectueux

		de la vie privée, que celui-ci soit susceptible ou non d'engendrer des risques élevés sur la vie privée
		L'AIPD doit être réalisée avant la mise en œuvre du traitement. C'est un processus itératif, les analyses doivent être revues et corrigées de manière régulière, en particulier lors de changements majeurs des modalités d'exécution du traitement
		Mener une AIPD est obligatoire pour tout traitement susceptible d'engendrer des risques élevés pour les droits et libertés des personnes concernées (*Article 35 du RGPD*). Afin d'aider la structure à déterminer si le traitement est susceptible d'engendrer des risques élevés, les 9 critères suivants sont définis dans les lignes directrices du G29 : - évaluation ou notation ; - décision automatisée avec effet juridique ou effet similaire significatif ; - surveillance systématique ; - données sensibles ou données à caractère hautement personnel ; - données personnelles traitées à grande échelle ; - croisement d'ensembles de données ; - données concernant des personnes vulnérables ; - usage innovant ou application de nouvelles solutions technologiques ou organisationnelles ; - exclusion du bénéfice d'un droit, d'un service ou contrat.
		Si le traitement rencontre au moins 2 de ces critères, alors il est vivement conseillé de faire une AIPD

Pour garantir un haut niveau de protection des données personnelles en permanence, il faut mettre en place des procédures internes qui garantissent la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (exemples : *faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire*)	
Organisation	Organiser les processus implique notamment : - de prendre en compte de la protection des données personnelles dès la conception d'une application ou d'un traitement (*minimisation de la collecte de données au regard de la finalité, cookies, durée de conservation, mentions d'information, recueil du consentement, sécurité et confidentialité des données, s'assurer du rôle et de la responsabilité des acteurs impliqués dans la mise en œuvre de traitements de données*). Pour cela, il faut s'appuyer sur les conseils du délégué à la protection des données ; - de sensibiliser et d'organiser la remontée d'information en construisant notamment un plan de formation et de communication auprès des collaborateurs de l'association ; - de traiter les réclamations et les demandes des personnes concernées quant à l'exercice de leurs droits (*droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement*) en définissant les acteurs et les modalités (*l'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen*) ; - d'anticiper les violations de données en prévoyant, dans certains cas, la notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais

Afin de prouver la conformité de la structure au règlement, il faut constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu		
Documentation	La documentation sur le traitement des données personnelles	Le registre des traitements (*pour les responsables de traitement*) ou des catégories d'activités de traitements (*pour les sous-traitants*)
		Les analyses d'impact relatives à la protection des données (*AIPD*) 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, les BCR et certifications*)
	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
	Les contrats	Les contrats avec les sous-traitants
		Les procédures internes en cas de violations de données
		Les preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base

Fiche 4 L'impact du RGPD sur la BDES

Dès lors que l'effectif d'un établissement ou de l'entreprise atteint 50 salariés, l'employeur doit mettre en place une base de données économiques et sociales (*BDES*), à destination des instances représentatives du personnel.

La BDES a été créée par l'accord national interprofessionnel pour la sécurisation de l'emploi du 11 janvier 2013 et la loi de sécurisation de l'emploi du 14 juin 2013, puis enrichie par la loi Macron du 6 août 2015 et la loi Rebsamen du 17 août 2015.

Accessible à tout moment et mise à jour régulièrement, elle regroupe l'ensemble des informations destinées aux représentants du personnel.

Le RGPD du 27 avril 2016 a supprimé toutes les déclarations préalables à la CNIL relatives à la BDES.

Il oblige néanmoins l'entreprise à établir un registre de traitement des données à chaque collecte de données personnelles.

En principe la BDES ne contient pas d'informations nominatives permettant d'identifier une personne de manière directe ou indirecte. Cependant, si l'employeur choisit d'intégrer des données nominatives, il devra établir un registre de traitement des données personnelles collectées.

Il en sera de même si l'accès à la BDES des représentants du personnel nécessite, par exemple, un code d'accès avec des informations nominatives des utilisateurs, ou que l'employeur trace leur navigation etc…

Fiche 5 Les salariés sont concernés par le RGPD

Employeurs et recruteurs ont fréquemment recours à la collecte de données personnelles dans le cadre de la gestion des ressources humaines. Elle commence dès le recrutement, avec les curriculums vitae et les tests d'évaluation, et se poursuit ensuite tout au long de la carrière du salarié via par exemple, les déclarations sociales et fiscales, les arrêts maladie, ou encore les échanges de correspondance.

L'employeur ne doit collecter que les données nécessaires au regard des finalités pour lesquelles elles ont été collectées.

Dans le cadre d'un recrutement, les données collectées doivent donc être limitées à celles strictement nécessaires à l'évaluation des capacités du candidat à occuper le poste proposé (*diplômes, emplois précédents, etc.*).

A l'embauche du candidat, l'employeur peut collecter des informations complémentaires. Celles-ci doivent être soit nécessaires au respect d'une obligation légale (*par exemple, les déclarations sociales obligatoires*), soit utiles :

- à la gestion administrative du personnel (*type de permis de conduire détenu, coordonnées de personnes à prévenir en cas d'urgence, numéro de sécurité sociale, informations bancaires, etc.*). Attention le numéro de sécurité sociale ne peut être traité, sauf cas très spécifiques, que pour la paye et les déclarations sociales obligatoires.
- à l'organisation du travail (*photographie du salarié pour les annuaires internes et organigrammes, etc.*)
- à l'action sociale prise en charge par l'employeur (*informations concernant les ayants droit du salarié, etc.*).

Les salariés doivent être informés du traitement de leurs données personnelles de façon claire et précise. Cette information peut se faire sur différents supports comme le règlement intérieur de l'entreprise ou encore le contrat de travail.

Elle doit notamment inclure :

- l'identité ;
- les coordonnées du Délégué à la Protection des Données (DPO) ;
- la durée de conservation des données ;
- la finalité du traitement ;
- les droits du salarié (*droit d'accès, de rectification ou d'effacement, droit d'introduire une réclamation, etc.*).

Par exemple, l'information du salarié est obligatoire en cas d'instauration d'un dispositif de vidéo-surveillance, de contrôle des horaires, de géolocalisation des véhicules, ou encore d'enregistrement et écoute téléphonique.

La collecte de certaines données, comme des photos d'identité, impose l'obtention préalable du consentement du salarié, qui doit être recueilli de façon explicite et non équivoque.

Les données personnelles des salariés ne peuvent être conservées que pour la durée nécessaire :

- à l'exécution de leur contrat de travail ;

- ou/et au respect d'obligations légales (*fiscales et sociales*) ;
- ou/et à l'accomplissement de l'objectif qui était poursuivi lors de la collecte.

Quelques illustrations :

- les données relatives à un candidat doivent être effacées au plus tard 2 ans après le dernier contact ;
- la conservation des données relatives aux accès aux locaux est limitée à 3 mois après leur enregistrement ;
- la conservation des données relatives à la gestion de la paie ou au contrôle des horaires des salariés est limitée à 5 ans ;
- la conservation des données figurant dans un dossier médical peut aller jusqu'à 10 ans à compter de la consolidation du dommage.

Droits des salariés

Le RGPD donne aux salariés des droits liés à leurs données personnelles. Les entreprises (*et les organisations syndicales*) doivent faire savoir aux salariés comment ils peuvent exercer ces droits et répondre à leurs demandes rapidement. Le non-respect de cette règle constitue une violation du RGPD et peut mener à des actions disciplinaires.

Droit d'être informé	Les entreprises doivent informer les salariés concernant les données qui sont collectées, comment elles sont utilisées, combien de temps elles sont conserves et si elles seront ou non partagées avec des tierces parties
	Ces informations doivent être communiquées de manière concise et dans un langage clair
Droit d'accès	Les salariés concernés peuvent soumettre une demande d'accès, obligeant les entreprises à leur fournir une copie de toutes les données qu'ils détiennent à leur sujet
	Les entreprises ont 1 mois pour fournir ces informations, bien qu'il y ait des exceptions pour les demandes étant manifestement infondées, répétitives ou excessives
Droit de rectification	Si un salarié découvre que les informations détenues à son sujet par une entreprise sont inexactes ou incomplètes, il peut demander à ce qu'elles soient mises à jour
	Comme pour le droit d'accès, les entreprises ont 1 mois pour s'y conformer, et les mêmes exceptions s'appliquent
Droit à l'effacement	Dans certains cas, les salariés peuvent demander à ce que les entreprises suppriment leurs données. Par exemple : - lorsque les données ne sont plus nécessaires, - lorsque les données sont traitées de manière illégitimes, - ou lorsque les données ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées
	Cela comprend les cas où les salariés concernés retirent leur consentement
	Le droit à l'effacement est également connu sous le nom de droit à l'oubli
Droit à la limitation du traitement	Les salariés peuvent demander aux les données de limiter l'utilisation de leurs données personnelles
	Il s'agit d'une alternative au droit d'effacement et peut être utile lorsqu'un salarié conteste l'exactitude de ses données personnelles ou lorsque les informations ne sont plus utiles mais que les entreprises en ont besoin pour établir, exercer ou défendre une revendication légale

Droit à la portabilité des données	Les salariés peuvent obtenir et réutiliser leurs données personnelles à leurs propres fins et pour différents services.
Droit d'opposition	Les salariés peuvent s'opposer au traitement des données personnelles collectées sur la base de l'intérêt légitime ou de l'exécution d'une tâche d'intérêt public ou relevant de l'exercice d'une autorité publique
	Ce droit ne s'applique qu'aux données personnelles qu'un salarié a fourni aux responsables du traitement via un contrat ou son consentement
	Les entreprises doivent arrêter de traiter des informations à moins de pouvoir avoir des raisons légitimes sérieuses au traitement, surpassant les intérêts, droits et libertés des salariés ou si le traitement a pour but la mise en place ou l'exercice de la défense en cas de revendications juridiques
Droits liés à la prise de décision automatisée y compris le profilage	Le RGPD comprend les dispositions concernant les décisions prises sans participation humaine, tel que le profilage, utilisant les données personnelles afin de faire des hypothèses calculées concernant les salariés. Il y a des règles strictes concernant le type de traitement, et les salariés peuvent contester et demander une révision du traitement s'ils croient que les règles ne sont pas suivies

Le droit d'accès à ses données personnelles en pratique

L'article 15 du Règlement Général de Protection des Données (*RGPD*) prévoit le droit d'obtenir une copie des données à caractère personnel faisant l'objet d'un traitement.

L'article 70-19 de la loi n° 2018-493 du 20 juin 2018 reprend cette disposition en précisant que *la personne concernée a le droit d'obtenir du responsable de traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, le droit d'accéder auxdites données*.

Par conséquent, les salariés peuvent exercer leur droit d'accès pour obtenir de nombreux documents. Mais :

- qu'en est-il de l'effectivité de ce droit ?
- quels arguments l'employeur peut-il leur opposer ?
- comment les contourner ?

1) Étendue du droit d'accès aux données personnelles pour les salariés

(*article 15 RGPD et article 70-19 de la loi du 20 juin 2018*).

Un salarié ou ancien salarié peut obtenir en vertu de l'article 15 du RGPD, un droit d'accès à l'ensemble des données le concernant, peu importe le support de conservation (*numérique ou papier*).

Ainsi, un salarié a droit d'accéder aux données relatives à :

- son recrutement ;
- son historique de carrière ;
- sa rémunération ;
- l'évaluation de ses compétences professionnelles (*entretiens annuels d'évaluation, notation*) ;
- son dossier disciplinaire.
- tout élément ayant servi à prendre une décision à son égard (*exemple : une promotion, une augmentation, un changement d'affectation, une sanction*).

Le salarié peut, se voir opposer un certain nombre de limites par l'employeur afin de refuser la transmission des documents demandés.

Le droit d'accès ne peut porter atteinte aux droits des tiers (*article 15 § 4 RGPD*). L'employeur peut légitimement refuser de transmettre un document contenant les données personnelles de plusieurs personnes.

L'article 15 paragraphe 4 du RGPD prévoit expressément que *le droit d'obtenir une copie […] ne porte pas atteinte aux droits et liberté d'autrui*.

En conséquence :

- L'employeur peut, par exemple, refuser de transmettre un e-mail, ou une correspondance impliquant un des collègues du salarié.

> **Conseil pour obtenir un document :** demandez à l'employeur de supprimer les noms et prénoms des personnes en copie ou signataire ; ainsi anonymisé, il ne s'agit plus d'une atteinte à leurs données personnelles

- L'employeur peut refuser de transmettre une vidéo dans laquelle un salarié apparaît entouré de tiers.

> **Conseil pour flouter une vidéo :** demandez à l'employeur de réaliser un floutage des visages des autres personnes concernés pour ne garder en clair que votre visage

Par ailleurs, le droit d'accès ne peut porter atteinte au secret des correspondances garantie par les articles 11 de la Déclaration des droits de l'homme et du citoyen de 1789 et 8 de la Convention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

Le secret des correspondances constitue une liberté fondamentale reconnue à tous les citoyens. Dès lors, un salarié ne saurait, en principe, exiger l'obtention d'emails entre l'employeur et le service RH le concernant.

En effet, leur avis sur le salarié est protégé au titre du secret des correspondances.

Le droit d'accès ne peut porter atteinte au secret des affaires (*considérant n° 63 RGPD*). L'employeur peut également opposer aux salariés :

- la confidentialité des données, souvent l'objet d'une clause dans le contrat de travail du salarié.
- le secret des affaires, limite expresse prévue par le RGPD.

En effet, le considérant n° 63 du RGPD précise que le droit d'accès *ne devrait pas porter atteinte aux droits ou libertés d'autrui, y compris au secret des affaires ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel. Cependant, ces considérations ne devraient pas aboutir à refuser toute communication d'informations à la personne concernée*.

> **Conseil pour obtenir un document :** il est conseillé aux salariés de préciser, autant que possible, leurs demandes de droit d'accès, et de définir clairement les documents auxquels ils souhaitent accéder

Plusieurs conseils aux salariés pour faire valoir son droit d'accès à ses données personnelles. Avant tout, il faut éviter que la demande de droit d'accès puisse être qualifiée d'abusive.

Exemple : ne pas demander une copie de l'intégralité des données personnelles sur l'ensemble de la carrière

Ensuite, le salarié doit circonstancier sa demande de droit d'accès, le principe d'utilité et de proportionnalité ressort du considérant n° 63 du RGPD :

- il est nécessaire d'être précis dans les documents demandés ;
- un motif de demande de droit d'accès n'est pas exigé, toutefois il est recommandé de justifier sa demande, pour obtenir plus facilement les données.

L'employeur doit répondre dans les meilleurs délais à une demande de droit d'accès et dans un délai maximum d'1 mois (*article 12.3 RGPD*).

Une prolongation de 2 mois est possible, *compte tenu de la complexité et du nombre de demandes*, à condition d'en informer la personne concernée dans le délai d'1 mois suivant la réception de la demande (*article 12.3 RGPD*).

En cas de refus, ou à défaut de réponse de l'employeur, il est possible d'adresser une plainte auprès de la CNIL avec les éléments attestant des démarches préalables.

Salariés - Modèles de lettre droit d'accès à ses données personnelles

Vous trouverez ci-dessous, pour les salariés, 2 modèles de lettres afin de faire valoir leur droit d'accès, auprès de l'employeur.

Exemple 1.
Objet : demande droit d'accès aux données personnelles
Madame, Monsieur,
En vue de la préparation de mon entretien de suivi annuel de forfait jours, je souhaiterais en vertu du droit d'accès à mes données personnelles (art 15 RGPD), obtenir une copie, en langage clair, dans un format compréhensible de l'ensemble de mes données de connexion à mon poste de travail sur les années 2018-2019.
Je vous remercie de me faire parvenir votre réponse dans les meilleurs délais et au plus tard dans un délai d'un mois à compter de la réception de ma demande (article 12.3 du RGPD).
Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

Exemple 2.
Objet : demande droit d'accès aux données personnelles
Madame, Monsieur,
Suite à mon licenciement, et au titre de l'article 15 du Règlement général sur la protection des données (RGPD), je souhaiterais en vertu du droit d'accès à mes données personnelles, obtenir une copie, en langage clair, dans un format compréhensible, les documents suivants :
Exemples :
- Mon dossier disciplinaire sur les 3 dernières années (2019-2017) ;
- La vidéo surveillance litigieuse du 27 janvier 2019. (Lister précisément les données souhaitées.)
Je vous remercie de me faire parvenir votre réponse dans les meilleurs délais et au plus tard dans un délai d'un mois à compter de la réception de ma demande (article 12.3 du RGPD).
Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

Attention, si le salarié envoie sa demande par voie électronique, les informations lui seront fournies par la même voie, à moins de demander qu'il en soit autrement.

Obligations des salariés

Conformément à la réglementation française et européenne en matière de protection des données personnelles, les informations relatives à des personnes physiques ne peuvent être utilisées que de manière transparente et, le cas échéant, avec le consentement des personnes concernées.

Ainsi, les salariés sont soumis à une obligation de confidentialité pour l'ensemble des données, notamment des informations personnelles, auxquelles ils ont accès dans le cadre de leurs fonctions (*qu'il s'agisse des données d'adhérents, de fournisseurs, de salariés…*).

Tout usage ou réutilisation illicite de ces données constitue une violation de la réglementation en matière de protection des données personnelles, et notamment du RGPD, et engage la responsabilité de l'entreprise (*ou du syndicat, du CSE, de l'association, …*) qui peut être sanctionnée par une amende administrative.

Par ailleurs, chaque salarié est soumis à un engagement contractuel de confidentialité à l'égard de son employeur et, qu'à ce titre, toute diffusion ou utilisation illicite d'informations est susceptible de sanctions disciplinaires.

Il est donc important que chacun salarié reste vigilant face à tous types de sollicitations, y compris pour l'accès à des bases de contact.

Fiche 6 La violation des données à caractère personnel

Les attaques sur les données personnelles prennent des formes très diverses :
- la prise des données en otage ou ransomware (*61 %*) ;
- la défiguration de site web (*23 %*) ;
- le vol de données personnelles (*18 %*).

La plupart de ces intrusions sont le résultat d'une négligence humaine.

Suite à une faille de sécurité, des données traitées ou stockées permettant d'identifier une personne physique (*salarié, adhérent, prospect, fournisseur…*), ont pu faire l'objet d'une destruction, d'une altération ou, le plus souvent, d'une communication à un tiers non autorisé (*un hacker, un concurrent…*).

Les failles dans la sécurité des données de la structure (*CSE, entreprise, syndicat, association*) ne sont pas seulement le fait d'attaques extérieures, elles sont parfois le résultat de négligences internes, voire d'erreurs dues à la méconnaissance des consignes et des enjeux liés à la sécurité ou à une violation des consignes de sécurité au sein de l'entreprise. Sont en cause :

- la multiplication des canaux de communication que l'entreprise a déployés dans le cadre de sa stratégie numérique (*pages Facebook, LinkedIn, Viadeo, forums, sites web, Blog, Twitter, …*) ;
- les réseaux sociaux et toutes les informations personnelles permettant de passer les barrières de sécurité (*type mot de passe et login*) utilisés sur les appareils de l'entreprise ou non ;
- la perméabilité des appareils (*ou devices*) : la multiplication de nouveaux usages (*BYOD/mobilité, télétravail, plateformes collaboratives, …*) impliquent de se connecter à des réseaux qui sont parfois insuffisamment protégés ;
- une tentative d'installation d'un logiciel par un salarié ou la méconnaissance des risques de phishing (*hameçonnage*).

Plus de 8 entreprises françaises sur 10 ont été visées par une cyberattaque en 2015. Une cyberattaque peut induire :

- des pertes de fichiers importantes ;
- un impact négatif sur l'image de l'entreprise vis-à-vis de ses clients, fournisseurs et prospects.

S'il y a eu violation, que doit faire le responsable de traitement ?

1ère étape
Déterminer la nature de la violation
Évaluer les risques que la situation est susceptible d'engendrer pour les droits et les libertés
⬇
2ème étape
Prendre les mesures nécessaires pour remédier à cette faille de sécurité (*par exemple : rétablir la disponibilité du serveur*)
⬇
3ème étape
Évaluer si cette faille de sécurité nécessite une notification à la CNIL, voire aux personnes dont les données ont été violées

Ce que doit faire le responsable de traitement des données en cas de violation des données :

1ère hypothèse		
La violation des données n'est pas susceptible d'engendrer un risque pour les droits et les libertés des personnes physiques	➡	le responsable de traitement n'est pas tenu de la notifier
2ème hypothèse		
La violation des données est susceptible d'engendrer un risque pour les droits et les libertés des personnes physiques	➡	le responsable de traitement devra impérativement en informer la CNIL
3ème hypothèse		
La violation des données est susceptible d'engendrer un risque élevé (*risque réel de réutilisation non consentie des informations*) pour les droits et les libertés des personnes physiques	➡	le responsable de traitement devra également en informer toutes les personnes concernées

Délai de notification :

- à la CNIL : dans les meilleurs délais et, si possible, 72 heures au plus tard après avoir pris connaissance de l'incident
  Si le délai de 72 h ne peut pas être respecté, il convient de :
  - notifier le plus rapidement possible, en précisant les motifs du retard ;
  - transmettre les informations, même de façon échelonnée, dès qu'elles sont à disposition.
- aux personnes dont les données ont été violées : dans un délai aussi raisonnable que possible

Il est possible d'éviter des failles de sécurité en les anticipant C'est-à-dire en ayant pris des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Les obligations de sécurité décrites dans le RGPD doivent donc être regardées comme des pare-feux utiles face aux risques de failles informatiques.

Sécurisation de son système d'information

Plusieurs démarches doivent être mises en œuvre en interne pour protéger les données :

- sensibiliser son personnel aux pratiques élémentaires de sécurité informatique (*règles de navigation sur internet, accès à la messagerie personnelle…*) ;
- prévoir une charte relative à l'usage des réseaux sociaux, notamment si l'entreprise est présente sur ces réseaux ;
- identifier les données les plus sensibles (*liste des salariés, données RH, adhérents…*) et effectuer un inventaire des comptes bénéficiant de droits étendus sur ces données ;
- encadrer les règles permettant au personnel d'utiliser un équipement informatique personnel au sein de l'entreprise ;
- authentifier et contrôler les accès en évitant la configuration des systèmes d'information par défaut (*exemple : nom d'utilisateur : admin, mot de passe : 12345*) ;
- faire une information sur la configuration des mots de passe pour les rendre plus fiables tout en les changeant régulièrement ;
- sécuriser les postes de travail en interdisant par exemple le branchement des clés USB sur les ordinateurs.

Fiche 7 Sanctions en cas de non-conformité

Les organisations syndicales ainsi que les CSE, contrairement aux entreprises, ne sont pas la cible principale de cette nouvelle réglementation. Les entreprises sont davantage dans le viseur. Notamment pour toutes les utilisations de données collectées à des fins publicitaires.

Néanmoins, les organisations syndicales CSE sont elles aussi soumis à la réglementation et susceptibles d'être contrôlées.

La CNIL s'assure que le responsable de traitement ou le sous-traitant respecte, les dispositions relatives à la protection des données personnelles.

Les quatre catégories de contrôle :

- sur place : dans les locaux professionnels du responsable du traitement et/ou du sous-traitant avec accès aux serveurs et ordinateurs où sont stockées les données ;
- sur pièces : il concerne la demande de communication de documents ;
- sur convocation : elle parvient à la personne auditionnée au moins 8 jours avant la date du contrôle ;
- en ligne : il s'effectue au sein de la CNIL à partir d'une plateforme et d'une connexion internet dédiée. Il porte sur la consultation de données librement accessibles ou rendues accessibles, y compris par imprudence, négligence ou du fait d'un tiers. Généralement ces contrôles s'effectuent sur le dépôt de cookies et autres traceurs, les mentions d'information à l'attention des utilisateurs, la sécurité du site internet…

Remarque : ces différents modes de contrôle peuvent se combiner

Les responsables de traitement et les sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement.

Les autorités de protection peuvent notamment :

- prononcer un avertissement ;
- mettre en demeure l'entreprise ou le syndicat ;
- limiter temporairement ou définitivement un traitement ;
- suspendre les flux de données ;
- ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- ordonner la rectification, la limitation ou l'effacement des données.

Constituent un délit d'entrave sanctionné d'1 an de prison et de 15 000 euros d'amende :

- le refus de communiquer, la dissimulation, la destruction des renseignements et documents nécessaires au contrôle ;
- la communication d'informations non conformes au contenu initial des enregistrements ;
- la présentation d'un contenu sous une forme qui n'est pas directement accessible…

En cas d'infraction au RGPD, des sanctions lourdes (*jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial d'une organisation*) peuvent être appliquées.

Et ce n'est pas une légende... Un mois après l'entrée en vigueur du RGPD, l'ADEF (*Association pour le Développement des Foyers*) a été sanctionnée pour une faille de sécurité concernant son site web par la CNIL. L'amende a été établie à 75 000 euros.

Le 21 janvier 2019, la CNIL (*Commission nationale de l'Informatique et des Libertés*) a condamné la société Google à 50 millions d'euros d'amende. L'autorité accuse en effet le géant américain d'avoir manqué aux obligations imposées par le RGPD.

Article 226-16
Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de 5 ans d'emprisonnement et de 300 000 euros d'amende.

Fiche A Une formation en ligne réalisée par la CNIL

Une formation en ligne, réalisée par la CNIL, ouverte à tous (*MOOC*) intitulée L'atelier RGPD propose aux professionnels de découvrir ou mieux appréhender le RGPD. Il permet ainsi d'initier une mise en conformité de leur organisme et d'aider à la sensibilisation des opérationnels.

Cet outil de formation gratuit est accessible à tous. Une fois son compte créé, l'utilisateur progresse à son rythme.

Principe du MOOC : Massive Open Online Courses : des cours sur Internet (*à distance*), gratuits et ouverts à tous. Le principe se rapproche de la formation par correspondance ou de l'e-learning, mais la révolution vient du concept d'ouverture car aucune barrière de compétence ou de frais d'inscription ne sont demandés aux participants

Une attestation de suivi est délivrée dans le MOOC à tout participant ayant parcouru la totalité des contenus et ayant répondu correctement à 80 % des questions par module.

Ce MOOC s'adresse principalement aux Délégués à la Protection des données (*DPO*) et futurs délégués et aux professionnels voulant appréhender le sujet RGPD. Il convient aussi bien aux profils techniques que juridiques et peut être suivi par toute personne curieuse de cette matière.

Ce MOOC a été élaboré par les juristes et experts de la CNIL. Il est composé de vidéos, de textes, d'illustrations et de cas concrets et propose des quizz et des évaluations.

Le MOOC est structuré en 4 modules avec une durée moyenne de 5h :

- Module 1 : le RGPD et ses notions clés
- Module 2 : les principes de la protection des données
- Module 3 : les responsabilités des acteurs
- Module 4 : le DPO et les outils de la conformité

Le premier module donne les *notions clés* du RGPD en précisant dans son dernier point à qui s'adresse ce règlement. Le second module revient sur les principes de la protection des données en donnant notamment *8 règles d'or*. Le troisième fait le point sur les responsabilités des acteurs. Enfin, le dernier module détaille les attributions du *DPO* et les outils de la conformité.

Adresse Internet : https://atelier-rgpd.cnil.fr

Fiche B Cadre juridique

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (*règlement général sur la protection des données*) applicable dans tous les pays européens depuis le 25 mai 2018

- Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil

- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles

- Décret n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles

Fiche C Glossaire

Analyse d'impact	Document d'analyse des risques en matière de protection des données. Il permet de définir les mesures appropriées lorsqu'un risque élevé est susceptible d'exister pour les droits et les libertés des personnes concernées
Consentement	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 : - s'il est donné par écrit, le consentement ne doit pas avoir été noyé sous d'autres questions ; - la personne concernée a le droit de retirer son consentement à tout moment ; - concernant les services en ligne adressés aux enfants, le traitement est licite s'il est consenti par un mineur de plus de 15 ans ou par le titulaire de l'autorité parentale ; - le responsable de traitement doit pouvoir prouver que la personne concernée a donné son consentement
Données à caractère personnel (ou données personnelles)	Toute information se rapportant à une personne physique identifiée ou identifiable. Cette identification peut être directe ou indirecte, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, une photo, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale
Données sensibles	Données à caractère personnel, qui, par nature, sont particulièrement sensibles du point de vue des libertés et des droits fondamentaux et méritent donc une protection spécifique. Il s'agit des données qui révèlent : - l'origine (*raciale, ethnique*) ; - des convictions ou pratiques (*les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, la vie sexuelle*) ; - l'état de santé (*données génétiques, données concernant la santé, données biométriques*).
Droit à la limitation du traitement	- lorsque l'exactitude des données personnelles est contestée (*pendant une durée permettant la vérification par le responsable de traitement*) ; - lorsque le traitement est illicite et la personne concernée s'oppose à leur effacement ; - lorsque le responsable de traitement n'a plus besoin des données personnelles qui sont toujours nécessaires à la personne concernée ; - lorsque la personne concernée a fait valoir son droit d'opposition, pendant la période de vérification de l'existence motifs légitimes dans l'intérêt public.
Droit à la portabilité des données	Droit de récupérer et/ou de transmettre les données personnelles à un autre responsable de traitement quand le traitement est fondé sur le consentement et qu'il est effectué à l'aide de procédés automatisés.
Droit à l'effacement	Possibilité pour la personne concernée d'obtenir l'effacement de ses données lorsqu'elles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées : - lorsque la personne concernée retire son consentement (*et qu'il n'existe pas d'autres fondements juridiques au traitement*) ; - lorsque la personne concernée s'oppose au traitement de ses données personnelles dans l'intérêt public en l'absence de motif légitime impérieux ; - lorsque les données personnelles ont fait l'objet d'un traitement illicite ; - lorsque les données personnelles ont été collectées auprès d'un enfant dans le cadre de l'offre de services de la société de l'information.
Limitation de la conservation	Les données personnelles doivent être conservées sous une forme permettant l'identification pendant une durée n'excédant pas celle nécessaire au regard des

	finalités pour lesquelles elles sont traitées sauf finalité archivistique, de recherche, statistique.
Objet du traitement	Le fichier a pour finalité la gestion clients, la gestion de ressources humaines et de lutter contre la fraude.
Personne concernée	Personne dont les données sont recueillies à des fins de traitement.
Registre des activités de traitement	Outil permettant aux responsables du traitement et sous-traitants de recenser sous forme écrite y compris électronique, les traitements effectués et de prouver, le cas échéant, le respect des obligations imposées par le RGPD. Il doit être mis à disposition de l'autorité de contrôle sur demande.
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. Il peut s'agir d'un représentant légal de l'entreprise qui prend l'initiative de constituer un fichier
RPD	Le Responsable (*ou Délégué*) à la protection des données est la personne chargée de s'assurer que les dispositions du RGPD sont bien mises en œuvre dans l'entreprise qui l'a désignée. Il peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service
Traitement de données à caractère personnel	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, contenues ou destinées à être contenues dans un fichier 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. Les procédés utilisés peuvent être très sophistiqués (*un progiciel spécifique destiné à gérer les ressources humaines ou lutter contre la fraude, par exemple*) ou rudimentaires (*un tableur ou même la constitution de dossiers papier pour autant qu'ils soient structurés selon des critères déterminés*).
Violation des 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

Pour plus d'informations, contactez un avocat du Cabinet RIERA via l'adresse Internet cabinet.riera@avocatem.com

Les dessins sont prêtés avec l'aimable autorisation de Dobritz
« Le placard a horreur du vide »
Editions Bruno Leprince, 2010