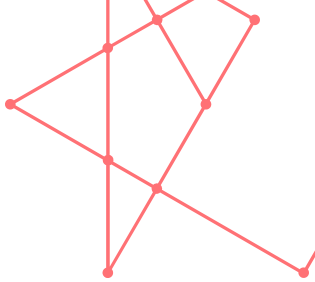
FEDIL

Publication

FAQ DANS LE CADRE DU RGPD

SUMMARY / CONTENT



QUEL RÔLE LE RESPONSABLE DU TRAITEMENT JOUE-T-IL DANS LA DÉFINITION DES MOTS DE PASSE ?

DOIS-JE AVOIR LE CONSENTEMENT DE LA PERSONNE CONCERNÉE POUR POUVOIR UTILISER SON ADRESSE E-MAIL À DES FINS PUBLICITAIRES ?

PENDANT COMBIEN DE TEMPS UN EMPLOYEUR DOIT-IL CONSERVER LES DOCUMENTS COMPTABLES ?

PENDANT COMBIEN DE TEMPS L'EMPLOYEUR DOIT-IL CONSERVER LES DOSSIERS PERSONNELS DES SALARIÉS ?

COMMENT L'EMPLOYEUR PEUT-IL INFORMER LES CANDIDATS DANS LE CADRE D'UN RECRUTEMENT DE L'UTILISATION DE LEURS DONNÉES À CARACTÈRE PERSONNEL ?

COMMENT L'EMPLOYEUR PEUT-IL INFORMER LES SALARIÉS DES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL LES CONCERNANT ? EXISTE-IL UNE CLAUSE TYPE À INSÉRER DANS LES CONTRATS DE TRAVAIL ?

POUR COMBIEN DE TEMPS L'EMPLOYEUR PEUT-IL CONSERVER DES DONNÉES À CARACTÈRE PERSONNEL DE CANDIDATS NON RETENUS APRÈS LA PHASE DE RECRUTEMENT ?

EST-CE QUE L'EMPLOYEUR EST TENU DE TRANSMETTRE LES DÉCLARATIONS D'ACCIDENT DE TRAVAIL / DE TRAJET REMPLIES À LA DÉLÉGATION DU PERSONNEL ET/OU AU DÉLÉGUÉ À LA SÉCURITÉ ET À LA SANTÉ AU REGARD DE L'ARTICLE L. 414-2. (5) DU CODE DU TRAVAIL ?

EST-CE QUE LE RESPONSABLE DU TRAITEMENT DOIT TOUJOURS AVOIR LE CONSENTEMENT DE LA PERSONNE CONCERNÉE S'IL PREND DES PHOTOS ?

L'INFORMATION QUE DES PHOTOS SOIENT PRISES À L'OCCASION D'UN ÉVÉNEMENT PEUT PRENDRE QUELLES FORMES ?

EST-CE QUE LA PUBLICATION D'UNE PHOTO PAR UN PROFESSIONNEL (ENTREPRISES, ADMINISTRATIONS, ASSOCIATIONS) NÉCESSITE-T-ELLE TOUJOURS LE CONSENTEMENT DE LA PERSONNE CONCERNÉE ?

EXISTE-T-IL D'AUTRES DOCUMENTS FACILITANT LA MISE EN CONFORMITÉ AU RGPD ?

LA SURVEILLANCE DES SALARIÉS DANS LE CADRE DES RELATIONS DE TRAVAIL

- **Qu'est-ce qu'une « surveillance » des salariés dans le cadre des relations de travail ?**
- **Quels sont les changements principaux relatifs à la surveillance des salariés dans le cadre des relations de travail après l'entrée en vigueur du RGPD ?**

Existe-il d'autres documents facilitant le respect des nouvelles dispositions en matière de surveillance des salariés dans le cadre des relations de travail ?

QU'EST-CE QUE LE PRINCIPE D'« *ACCOUNTABILITY* » ?

Il s'agit d'une des grandes nouveautés du Règlement général sur la protection des données (RGPD) par rapport à la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, transposée en droit luxembourgeois par la loi modifiée du 2 août 2002.

L'*accountability* désigne l'obligation pour les organisations de mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer que les traitements des données à caractère personnel sont effectués conformément au RGPD, et d'être en mesure de le démontrer si nécessaire (en cas de contrôle par exemple). Le système des formalités préalables (notifications et autorisations) auprès de la Commission nationale pour la protection des données (CNPD) prévu par la loi précitée n'existe plus. Tous les acteurs établis sur le territoire luxembourgeois doivent être en mesure de démontrer eux-mêmes leur conformité.

Plus d'informations :

- **Article 5 du RGPD**

QU'EST-CE QU'UN « SOUS-TRAITANT » AU SENS DU RGPD ET COMMENT CETTE QUALITÉ EST-ELLE DÉTERMINÉE ?

Un sous-traitant est défini comme une personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte et sur instruction d'un responsable du traitement. Or, pour déterminer la qualité de sous-traitant au sens du RGPD, il convient d'analyser si les 4 critères déterminés par le groupe de travail « article 29 » dans son avis 1/2010 du 16 février 2010 sont réunis pour l'acteur en question. L'avis peut toujours servir de référence même s'il a été rédigé sous l'égide de l'ancienne directive européenne du 24 octobre 1995, car les notions de « responsable de traitement » et de « sous-traitant » n'ont pas changé avec l'application du RGPD.

Les 4 critères sont les suivants :

- le niveau d'instruction donné par le client au prestataire ;
- le degré de contrôle de l'exécution de la prestation ;
- la valeur ajoutée fournie par le prestataire ;
- le degré de transparence sur le recours à un prestataire.

À noter que les 4 critères doivent être cumulativement remplis pour avoir la qualité de sous-traitant, à défaut, l'organisation est à considérer comme responsable du traitement pour le traitement en question. Il est possible qu'une entreprise d'un groupe soit sous-traitant d'une entreprise appartenant au même groupe.

Ont souvent la qualité de sous-traitant les prestataires de *payroll*, les fournisseurs de logiciel ERP, les fournisseurs de prestations *de cloud computing*, les sociétés de sécurité informatique ou encore les agences de marketing ou de communication.

Plus d'informations :

- **Article 4 du RGPD**
- **Avis 1/2010 du 16 février 2010 du groupe de travail « article 29 »**
- **Note relative aux notions de responsable de traitement et de sous-traitant de l'autorité de contrôle belge (Autorité de protection des données, APD)**

FAUT-IL CONCLURE UN CONTRAT AVEC TOUS LES SOUS-TRAITANTS, ET SI OUI, QUEL EST SON CONTENU MINIMAL ?

Oui, le traitement des données à caractère personnel par un sous-traitant doit être régi par un contrat ou un autre acte juridique au titre de l'Union européenne ou du droit d'un État membre, liant le sous-traitant au responsable du traitement, définissant l'objet et la durée du traitement, la nature et les finalités du traitement, le type de données à caractère personnel et les catégories de personnes concernées, en tenant compte des tâches et responsabilités spécifiques du sous-traitant dans le cadre du traitement à effecteur et du risque pour les droits et libertés de la personne concernée.

Tous les éléments devant figurer dans le contrat sont décrits à l'article 28 du RGPD. Il est encore important à relever que cela nécessite, selon le cas, une mise à jour active et continuelle des contrats.

Plus d'informations :

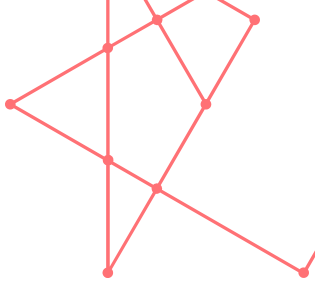
- **Article 28 du RGPD**
- **Considérant 81 du RGPD**
- **Guide pratique de l'autorité de contrôle française (Commission Nationale de l'Informatique et des Libertés, CNIL) sur la relation responsable du traitement – sous-traitant**

QU'EST-CE QU'UN « REGISTRE DES ACTIVITÉS DE TRAITEMENT » ?

Le registre des activités de traitement est censé regrouper tous les traitements de données à caractère personnel que l'entreprise est amenée à faire. Ce registre fait partie de l'*accountability* de chaque organisation et sert donc à prouver la conformité au RGPD. En effet, cette cartographie en mode continu de ses activités doit permettre à toute organisation de bien veiller à toujours respecter les règles du RGPD. La tenue de ce registre est nécessaire pour les responsables du traitement pour avoir une connaissance suffisamment documentée de leurs activités de traitement des données à caractère personnel. Il doit constamment être tenu à jour en fonction du développement et de l'évolution des activités de l'entreprise.

Plus d'informations :

- **Article 30 du RGPD**
- **Considérant 82 du RGPD**
- **Recommandation relative au registre des activités de traitement du 14**



juin 2017 de l'autorité de contrôle belge (Autorité de protection des données, APD)

EST-CE QUE MON ENTREPRISE DOIT TENIR UN TEL REGISTRE ?

En tant que responsable du traitement, vous devez tenir un registre des activités de traitement effectuées sous votre responsabilité. De même, chacun de vos sous-traitants doit tenir un registre de toutes les catégories d'activités de traitement effectuées pour votre compte.

Néanmoins, cette obligation ne s'applique pas si les conditions cumulatives suivantes sont remplies :

- l'entreprise ou l'organisation concernée compte moins de 250 employés ;
- le traitement qu'elle effectue n'est pas susceptible de comporter un risque pour les droits et les libertés des personnes concernées ;
- le traitement qu'elle effectue est occasionnel ;
- le traitement qu'elle effectue ne porte pas sur des données dites « sensibles » visées à l'article 9, paragraphe 1, du RGPD ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 du RGPD.

Or, vu que le registre des activités de traitement permet de mesurer concrètement l'impact du RGPD sur l'activité de l'entreprise, la tenue de ce dernier se révèle ainsi souvent nécessaire pour les responsables du traitement afin d'avoir une connaissance suffisamment documentée de leurs activités de traitement des données à caractère personnel et donc pour en assurer une protection efficace. C'est la raison pour laquelle le registre des activités de traitement est en tout état de cause recommandé par la Commission nationale pour la protection des données (CNPD) et le comité européen de la protection des données dans les démarches de mise en conformité au RGPD.

Plus d'informations :

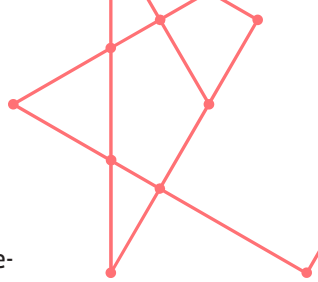
- **Article 30 du RGPD**
- **Considérant 82 du RGPD**
- **Recommandation relative au registre des activités de traitement du 14 juin 2017 de l'autorité de contrôle belge (Autorité de protection des données, APD)**

EST-CE QUE CE REGISTRE DOIT ÊTRE PUBLIÉ OU ENVOYÉ À L'AUTORITÉ DE CONTRÔLE ?

Non, le registre n'est pas destiné au public, mais l'entreprise a l'obligation de mettre le registre des activités de traitement à la disposition de la Commission nationale pour la protection des données (CNPD) si celle-ci en fait la demande.

SOUS QUELLE FORME DOIT SE PRÉSENTER LE REGISTRE DES ACTIVITÉS DE TRAITEMENT ?

Le RGPD précise que ce registre peut se présenter sous une forme écrite y compris la forme électronique. En principe, il ne devra pas être spécialement réalisé dans une des trois langues officielles du Luxembourg. Toutefois, lors de la mise à disposition à une autorité de contrôle, celle-ci pourrait exiger sa traduction dans une des langues nationales. Selon l'Autorité de protection des



données (APD), l'autorité de contrôle belge, cette traduction se fait aux frais de l'entreprise. L'autorité de contrôle française, la Commission Nationale de l'Informatique et des Libertés (CNIL), a mis à disposition aux acteurs un modèle-type d'un tel registre qui est aussi reconnu par l'autorité de contrôle luxembourgeoise, la Commission nationale pour la protection des données (CNPD). Il convient de mentionner que pas toutes les cases sont à remplir, mais uniquement celles qui sont concernées par le traitement en question.

Plus d'informations :

- **Article 30 du RGPD**
- **Considérant 82 du RGPD**
- **Recommandation relative au registre des activités de traitement du 14 juin 2017 de l'autorité de contrôle belge (Autorité de protection des données, APD)**
- **Modèle d'un registre des activités de traitement, CNIL**

QUELS SONT LES TRAITEMENTS HABITUELS DE DONNÉES À CARACTÈRE PERSONNEL ?

Des traitements souvent rencontrés en pratique sont notamment la gestion du personnel et des rémunérations, l'annuaire d'entreprise, la gestion des fournisseurs, la gestion de la comptabilité, la gestion des clients, la lutte contre la fraude (interne/externe) ou encore la surveillance (vidéosurveillance, dispositifs de géolocalisation, systèmes biométriques, contrôle des accès, ...).

DOIS-JE DOCUMENTER LES VIOLATIONS DES DONNÉES À CARACTÈRE PERSONNEL ?

Oui, chaque responsable du traitement est tenu de documenter dans un registre dédié à cette fin toute violation de données à caractère personnel (quel que soit le degré de gravité de la violation), en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permettra à l'autorité de contrôle de vérifier le respect des obligations du responsable du traitement. Des exemples concrets sont la perte d'un laptop, d'un CD-Rom ou d'une clé USB contenant des données à caractère personnel d'un collaborateur, une faille informatique, un stockage non-sécurisé des données ou encore un accès non-autorisé à un certain type de données. Selon la gravité de la violation des données à caractère personnel, le responsable du traitement doit la notifier à l'autorité de contrôle compétente dans un délai de 72 heures au plus tard après en avoir pris connaissance. Pour des raisons de simplification et d'harmonisation, il est recommandé d'utiliser le modèle de registre élaboré par la Commission nationale pour la protection des données (CNPD).

Plus d'informations :

- **Articles 33 et 34 du RGPD**
- **Considérants 85-88 du RGPD**
- **Registre des violations de données à caractère personnel, CNPD**
- **Formulaire de notification de violation de données, CNPD**

QUI PEUT ÊTRE DATA PROTECTION OFFICER (DPO) ?

Le DPO est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions qui lui sont assignées par le RGPD. Il peut être un membre du personnel (DPO interne) ou exercer ses missions sur la base d'un contrat de service (DPO externe). Sa tâche, qui peut être à temps plein ou à temps partiel, est essentiellement pédagogique au sein de l'entreprise afin que chacun connaisse les enjeux de la nouvelle règlementation et l'applique au quotidien en particulier pour l'ensemble des traitements des données à caractère personnel à venir. Son rôle sera donc avant tout la sensibilisation des collaborateurs.

Il est à noter que le rôle de DPO ne peut en aucun cas être assumé par le chef d'entreprise ou par toute autre personne occupant un poste permettant de déterminer le moyens et les finalités du traitement des données à caractère personnel (par exemple le chef des finances, le chef de l'exploitation, le responsable du département marketing, le responsable des ressources humaines, le responsable du département informatique, etc.). Les délégués peuvent exercer d'autres missions pour autant que celles-ci ne conduisent pas à un conflit d'intérêt. Un groupe d'entreprises peut désigner un seul DPO.

Même si la désignation d'un DPO n'est dans la majorité des cas pas obligatoire pour les PME, elle est cependant fortement recommandée par la Commission nationale pour la protection des données (CNPD) et par le comité européen de la protection des données.

Des organisations où la désignation d'un DPO est obligatoire sont notamment les autorités publiques (quelle que soit la nature des données traitées), mais aussi les compagnies d'assurance, les banques, les services de santé, les hôpitaux ou encore les professionnels du recrutement.

Plus d'informations :

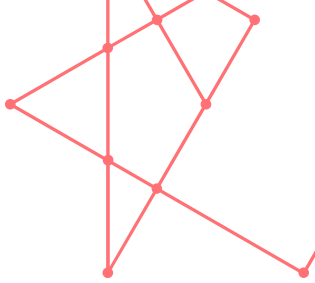
- **Articles 37-39 du RGPD**
- **Considérant 97 du RGPD**
- **Recommandation relative au DPO du 24 mai 2017 de l'autorité de contrôle belge (Autorité de protection des données, APD)**
- **Ligne directrice de l'ancien groupe de travail « article 29 » relative au DPO du 5 avril 2017**

EST-CE QUE LE DPO DOIT ÊTRE AGRÉÉ PAR LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES (CNPD) ?

Non, la CNPD ne délivre pas d'agrément aux DPO (contrairement aux chargés de la protection des données dans le cadre de l'ancienne directive). Le responsable du traitement ou le sous-traitant doivent simplement communiquer les coordonnées du DPO à la CNPD et sont invités d'utiliser le formulaire prévu à cette fin qui est mis à disposition par la CNPD. Le responsable du traitement (ou le sous-traitant) est en plus obligé de publier les coordonnées de son DPO (par exemple sur son site Internet).

La CNPD peut contrôler si les articles 37 à 39 du RGPD règlementant la désignation, la fonction et les missions du DPO sont respectés.

Plus d'informations :



- **Articles 37-39 du RGPD**
- **Considérant 97 du RGPD**
- **Formulaire de déclaration de DPO établi par la CNPD**

QU'EST-CE QU'UNE « ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES » ET QUI DOIT LA MENER ?

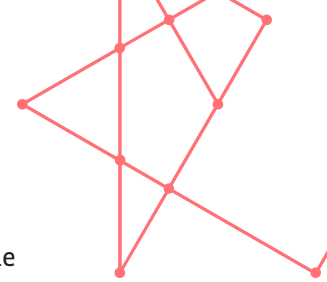
Les analyses d'impact relatives à la protection des données (AIPD) sont un outil aidant à identifier et à minimiser les risques de protection des données de nouveaux projets. Elles font partie des obligations du responsable du traitement et contribuent fortement à l'approche de protection des données dès la conception et protection des données par défaut. De plus, elles aident à identifier et à traiter les problèmes à un stade précoce, à démontrer la conformité avec les obligations de protection des données, répondre aux attentes des individus en matière de vie privée et aide à éviter les atteintes à la réputation qui pourraient se produire. L'obligation de procéder à une telle analyse incombe au responsable du traitement et pas au DPO en tant que tel. C'est le responsable du traitement qui sera responsable en vertu de l'article 35 du RGPD si elle n'a pas été réalisée alors qu'elle aurait dû l'être, si elle n'a pas été correctement réalisée ou si le responsable du traitement n'a pas consulté la CNPD lorsque c'était nécessaire. Elle doit obligatoirement être effectuée avant la mise en œuvre du traitement des données à caractère personnel concerné.

- **Articles 35-36 du RGPD**
- **Lignes directrices de l'ancien groupe de travail « article 29 » concernant l'AIPD du 4 octobre 2017**
- **Recommandation concernant l'AIPD du 28 février 2018 de l'autorité de contrôle belge** (Autorité de protection des données, APD)
- **Formulaire de la CNPD pour une consultation préalable dans le cadre d'une AIPD**

À PARTIR DE QUEL MOMENT CETTE ANALYSE EST-ELLE OBLIGATOIRE ET QUELS SONT LES CRITÈRES À PRENDRE EN COMPTE ?

Le RGPD précise que lorsque des traitements de données à caractère personnel considérés comme particulièrement risqués sont envisagés par un responsable du traitement, celui-ci devra réaliser, préalablement à ces traitements, une AIPD. L'article 35 du RGPD renvoie à une catégorie particulière de risques à savoir les risques, non pas vis-à-vis de l'entreprise, mais vis-à-vis des droits et libertés des personnes physiques. Selon les lignes directrices de l'ancien groupe de travail « article 29 » concernant l'AIPD, les termes « pour les droits et libertés des personnes physiques » de l'article 35 du RGPD concernent notamment le droit au respect de la vie privée mais ils peuvent également se rapporter à d'autres droits et libertés fondamentaux comme la liberté d'expression, la liberté de pensée, de conscience et de religion, l'interdiction de discrimination et le droit à la liberté de mouvement.

Les lignes directrices de l'ancien groupe de travail « article 29 » concernant l'AIPD précisent les 9 critères qui doivent être pris en considération lorsqu'un responsable du traitement doit se décider sur la réalisation ou non d'une AIPD. Si au moins 2 critères sont remplis, l'AIPD est obligatoire. Si le traitement de données à caractère personnel envisagé nécessite une AIPD, mais que le responsable du traitement décide de ne pas en réaliser une, il devra documenter cette décision ainsi que l'opinion de son DPO (lorsqu'un DPO a été



désigné).

De plus, la CNPD a élaboré, conformément à l'article 35 (4) du RGPD, une liste de traitements pour lesquels une AIPD est requis. Le projet de liste avait été soumis pour avis au Comité européen de la protection des données (CEPD), successeur du groupe de travail « article 29 », dans le cadre de la mise en œuvre d'une cohérence et d'une homogénéité de l'application du RGPD au niveau européen. La liste publiée prend en compte les remarques de l'avis du CEPD. Il convient cependant de souligner que la liste actuelle n'est pas une liste exhaustive de tous les types d'opération de traitement nécessitant la réalisation d'une AIPD. Ainsi, l'absence d'un type d'opération de traitement sur cette liste ne signifie pas nécessairement qu'une AIPD n'est pas requise.

- **Articles 35-36 du RGPD**
- Considérants **72**, **84**, **89-95** du RGPD
- **Lignes directrices de l'ancien groupe de travail « article 29 » concernant l'AIPD du 4 octobre 2017**
- **Recommandation concernant l'AIPD du 28 février 2018 de l'autorité de contrôle belge** (Autorité de protection des données, APD)
- **Délibération n° 34/2019 du 6 mars 2019 de la CNPD portant adoption de la liste des types d'opérations de traitement pour lesquelles une AIPD est requise**
- **Formulaire de la CNPD pour une consultation préalable dans le cadre d'une AIPD**

QUEL RÔLE LE RESPONSABLE DU TRAITEMENT JOUE-T-IL DANS LA DÉFINITION DES MOTS DE PASSE ?

Suivant l'article 32 du RGPD, il appartient au responsable du traitement de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Ainsi, ces mesures doivent assurer un niveau de sécurité approprié, y compris en matière de confidentialité, compte tenu de l'état des connaissances techniques et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger. Dans ce contexte, l'utilisation du mot de passe associé à un identifiant afin de procéder au contrôle des accès à des données à caractère personnel est l'une des mesures susceptibles d'être définie par le responsable du traitement.

Selon la Commission Nationale de l'Informatique et des Libertés (CNIL), l'autorité de contrôle française, le responsable du traitement doit notamment fixer la taille et la complexité du mot de passe à définir par les personnes concernées. Ces dernières doivent être informées des règles applicables à la définition du mot de passe (taille et complexité, p. ex. au moyen d'une jauge). En outre, aucun mot de passe ne peut être communiqué en clair aux personnes concernées, notamment par courrier électronique. Le renouvellement du mot de passe de la personne concernée doit être imposé par le responsable du traitement selon une périodicité qu'il définit. Enfin, la personne doit avoir la possibilité de pouvoir modifier son mot de passe en conformité avec les règles de création de mot de passe.

Plus d'informations :

- **Article 32 du RGPD**
- **Considérant 83 du RGPD**
- **Délibération n° 2017-012 de la CNIL du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe**

DOIS-JE AVOIR LE CONSENTEMENT DE LA PERSONNE CONCERNÉE POUR POUVOIR UTILISER SON ADRESSE E-MAIL À DES FINS PUBLICITAIRES ?

La réponse varie si une relation contractuelle est déjà existante ou non. En effet, de façon générale, le RGPD confère aux personnes concernées un droit de s'opposer (« opt-out ») au traitement des données à caractère personnel la concernant à des fins de prospection (p.ex. aux courriers de prospection envoyés par la poste). La loi luxembourgeoise modifiée du 30 mai 2005, qui continue à s'appliquer aux communications électroniques, dispose que le responsable du traitement (i.e. l'entreprise) est autorisé, dans le cas d'une base contractuelle déjà existante (vente ou services), à utiliser l'adresse e-mail de son client ou abonné à des fins publicitaires sans consentement préalable. En contrepartie, le client ou abonné doit avoir le droit de s'y opposer à tout moment (et être informé de ce droit lorsque les données sont recueillies et lors de chaque message de prospection).

Dans le cas où il n'existe aucun lien entre un responsable du traitement et un utilisateur, le consentement préalable doit être demandé avant l'envoi de courriers électroniques (« opt-in »).

Plus d'informations :

- **Communication de la Commission nationale pour la protection des données (CNPD) du 25 mai 2018**

PENDANT COMBIEN DE TEMPS UN EMPLOYEUR DOIT-IL CONSERVER LES DOCUMENTS COMPTABLES ?

Aux termes de l'article 16 du Code de commerce, les documents ou informations relatifs à la comptabilité d'un commerçant doivent être conservés pendant 10 ans à partir de la clôture de l'exercice auquel ils se rapportent.

Il apparaît indispensable de citer l'article 5 (1) (e) du RGPD précisant que les données ne peuvent être conservées que pour une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées.

Par conséquent, les documents comptables doivent être conservés pendant une période minimale de 10 ans. À noter qu'une période de rétention plus longue pour ces documents est possible, sous condition que cela soit raisonnable et justifié (et spécifié, le cas échéant, dans le registre des activités de traitement).

Plus d'informations :

- **Article 16 du Code de commerce**
- **Article 5 du RGPD**

PENDANT COMBIEN DE TEMPS L'EMPLOYEUR DOIT-IL CONSERVER LES DOSSIERS PERSONNELS DES SALARIÉS ?

En dehors de la question de la conservation des documents comptables, il n'y a pas de réponse précise à la question générale de la durée de conservation des dossiers personnels des salariés. Effectivement, la durée de conservation d'un document dépendra du type de document dont il est question et de la finalité

de la conservation de ce document.

Ici, il convient à nouveau de citer l'article 5 (1) (e) du RGPD précisant que les données ne peuvent être conservées que pour une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées. L'employeur est ainsi conseillé à opérer une distinction entre les différents documents composant les dossiers personnels de ses salariés et de procéder au cas par cas. Pour les documents rentrant dans la comptabilité de l'employeur, le délai légal de 10 ans prévu à l'article 16 du Code de commerce s'impose.

Pour tous les documents relatifs à la relation de travail avec le salarié (contrat de travail, avenants, avertissements, évaluations), il est recommandé aux employeurs de les garder au moins jusqu'à l'expiration du délai légal endéans lequel le salarié pourrait contester la résiliation de son contrat de travail, et pendant toute la durée de la procédure judiciaire, en cas de litige porté devant les juridictions.

Plus d'informations :

- **Article 16 du Code de commerce**
- **Article 5 du RGPD**

COMMENT L'EMPLOYEUR PEUT-IL INFORMER LES CANDIDATS DANS LE CADRE D'UN RECRUTEMENT DE L'UTILISATION DE LEURS DONNÉES À CARACTÈRE PERSONNEL ?

En pratique, cette information préalable obligatoire peut notamment se faire à l'aide d'un wording sur la plateforme de recrutement (souvent le cas pour les grandes entreprises) ou grâce à un e-mail de réponse automatique contenant l'information nécessaire. Pour la réception des candidatures par la poste, l'employeur est libre soit de répondre via e-mail soit par courrier. Le plus important est qu'il prenne des mesures appropriées afin que la communication se fasse d'une façon concise, transparente, compréhensible et aisément accessible. Elle doit se faire en des termes clairs et simples. Dans chaque situation, tous les points de l'article 13 du RGPD sont à respecter.

Il paraît également indispensable de clarifier que l'employeur est déjà à ce stade obligé de respecter le principe de la minimisation des données résultant de l'article 5 (1) (c) du RGPD. Ainsi, il doit veiller à ce que les données à caractère personnel soient adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. La demande du numéro de matricule d'un candidat pendant la phase du recrutement est par exemple à éviter.

Plus d'informations :

- **Article 5 du RGPD**
- **Article 12 du RGPD**
- **Article 13 du RGPD**
- **Considérants 39, 58-63 du RGPD**

COMMENT L'EMPLOYEUR PEUT-IL INFORMER LES SALARIÉS

DES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL LES CONCERNANT ? EXISTE-IL UNE CLAUSE TYPE À INSÉRER DANS LES CONTRATS DE TRAVAIL ?

L'employeur peut satisfaire à son obligation d'information vis-à-vis de ses salariés par différents moyens. Ainsi, il peut par exemple envoyer un courrier à tous les salariés les informant des traitements de données à caractère personnel qui les concernent ou envoyer une note interne via courriel à son personnel.

Un autre moyen est une clause y relative au contrat de travail. La FEDIL peut vous proposer le modèle de clause suivant :

« En vue de l'exécution du présent contrat de travail et des diverses obligations légales qui incombent à l'employeur en vertu du présent contrat de travail, l'employeur, responsable du traitement, procède au traitement de diverses données à caractère personnel du salarié (p. ex. nom, prénom, adresse postale, adresse e-mail, matricule, date de naissance, sans que cette liste ne soit limitative) conformément au règlement (UE) n° 2016/679 du 27 avril 2016 relatif à la protection des données à caractère personnel, ci-après désigné « RGPD ».

Les personnes travaillant dans le département des ressources humaines et (veuillez préciser un autre service si tel est le cas) sont destinataires des données à caractère personnel des salariés.

La base juridique au sens du RGPD des traitements de données à caractère personnel est l'exécution du contrat de travail, sans le traitement des données à caractère personnel, le contrat de travail ne peut pas être exécuté. Le traitement des données à caractère personnel répond, selon le cas, également à une obligation légale à laquelle l'employeur est soumis (p. ex. communication à l'administration des contributions directes pour la fixation d'impôts, déclaration d'entrée/de sortie auprès du Centre commun de la sécurité sociale, etc.)

Certaines données à caractère personnel (veuillez préciser lesquelles) sont transférées à (...), sous-traitant au sens du RGPD pour le paiement des salaires (si tel est effectivement le cas).

Les données à caractère personnel seront conservées aussi longtemps que nécessaire à l'exécution du contrat de travail, à l'accomplissement par l'employeur de ses obligations légales et réglementaires et à l'exercice des prérogatives lui étant reconnues par la loi et la jurisprudence. La durée de conservation des données à caractère personnel dépend essentiellement du type de donnée concernée. À titre d'exemple, les données à caractère personnel pouvant être qualifiées de « données comptables » doivent être conservées pendant une durée maximale de 10 années. Les données à caractère personnel des salariés pouvant servir comme éléments de preuve en cas de contestations, revendications ou réclamations émanant des salariés sont conservées pendant 3 années après la fin des relations de travail (cette durée de conservation correspondant aux dispositions de l'article 2277 du Code civil, selon lesquelles les actions en paiement des rémunérations de toute nature dues au salarié se prescrivent par 3 ans). Pendant toute la durée de conservation des données à caractère personnel, l'employeur s'engage à mettre en place tous les moyens nécessaires à assurer leur confidentialité et leur sécurité, de manière à empêcher leur endommagement, effacement ou accès par des tiers non autorisés.

Le salarié dispose d'un droit d'accès aux données lui concernant ainsi que d'un

droit à la rectification des données à caractère personnel lui concernant. Le salarié dispose du droit à l'effacement de ses données à caractère personnel lorsque celui-ci n'est pas en contradiction avec une obligation légale à laquelle l'employeur est soumis. Il peut exercer ses droits à tout moment en envoyant un courriel à (...) ou en envoyant un courrier à (...).

Le salarié dispose du droit d'introduire une réclamation auprès de la Commission nationale pour la protection des données (CNPD) s'il considère qu'un traitement de données à caractère personnel le concernant constitue une violation du RGPD. ».

La FEDIL tient à rappeler que ce modèle de clause doit évidemment être adapté et complété selon les spécificités de l'entreprise.

- **Article 13 du RGPD**

POUR COMBIEN DE TEMPS L'EMPLOYEUR PEUT-IL CONSERVER DES DONNÉES À CARACTÈRE PERSONNEL DE CANDIDATS NON RETENUS APRÈS LA PHASE DE RECRUTEMENT ?

Il n'existe pas de disposition officielle, mais conformément à l'article 5 (1) (e) du RGPD, les données à caractère personnel ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée qui n'excède pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées.

La position de la CNPD est de dire que les données à caractère personnel des candidats non retenus (volontaire ou non) doivent en principe être détruites de manière sécurisée après la période d'essai du candidat embauché vu que le traitement n'ait plus aucune finalité claire et précise, donc plus de base légale d'après l'article 6 du RGPD. Selon la recommandation n° 02-017 de la Commission Nationale de l'Informatique et des Libertés (CNIL), l'autorité de contrôle française, cette durée de conservation est de 2 ans maximum à compter du dernier contact avec le candidat.

Or, le responsable du traitement pourrait les garder plus longtemps sous condition d'avoir le consentement informé, libre et clair de la personne concernée, mais dans cette hypothèse le responsable du traitement doit opter pour un délai précis et raisonnable.

D'après la loi du 23 juillet 2016, les casiers judiciaires pour les candidats non retenus après la phase de recrutement doivent être détruits de manière sécurisée sans délai tandis que ceux des candidats retenus doivent être détruits de manière sécurisée 1 mois après la conclusion du contrat de travail.

Plus d'informations :

- **Article 5 du RGPD**
- **Loi du 23 juillet 2016 relative à l'organisation du casier judiciaire**
- **Délibération n°02-017 de la CNIL du 21 mars 2002 portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives lors d'opérations de recrutement**

EST-CE QUE L'EMPLOYEUR EST TENU DE TRANSMETTRE LES

DÉCLARATIONS D'ACCIDENT DE TRAVAIL / DE TRAJET REMPLIES À LA DÉLÉGATION DU PERSONNEL ET/OU AU DÉLÉGUÉ À LA SÉCURITÉ ET À LA SANTÉ AU REGARD DE L'ARTICLE L. 414-2. (5) DU CODE DU TRAVAIL ?

Non, à notre avis, la transmission des déclarations des accidents de travail / de trajet à la délégation du personnel et/ou au délégué à la sécurité et à la santé n'est pas nécessaire afin d'atteindre la finalité prévue à l'article L. 414-2. (5) point 3 du Code du travail qui se limite à prévoir que l'employeur est tenu de communiquer aux acteurs concernés toutes les informations nécessaires pour les informer quant à l'évolution du taux d'absence des salariés au sein de l'entreprise.

Or, transmettre (peu importe le support, papier ou électronique) le formulaire rempli en cas d'un accident de travail / de trajet à la délégation du personnel et/ou au délégué à la sécurité et à la santé (sur demande ou d'office) est à notre sens disproportionné, voire trop intrusif à la vie privée de la personne concernée du fait que ledit formulaire contient des données n'étant pas nécessaires pour atteindre la finalité claire et précise citée en haut qui se limite à une simple information relative à l'évolution du taux d'absence des salariés dans l'entreprise.

- **Article L. 414-2. (5) du Code du travail**
- **Formulaire de déclaration d'un accident de travail / de trajet à envoyer à l'Association d'assurance accident (AAA)**
- **Article 5 du RGPD**

EST-CE QUE LE RESPONSABLE DU TRAITEMENT DOIT TOUJOURS AVOIR LE CONSENTEMENT DE LA PERSONNE CONCERNÉE S'IL PREND DES PHOTOS ?

Non. Ici, la jurisprudence différencie entre les photos ciblées et les photos non-ciblées. Les photos ciblées sont celles dans lesquelles une personne est le sujet principal, en y figurant seul, en y étant mise à l'avant-plan ou en y prenant une pose (même en groupe). Les photos non-ciblées reflètent l'ambiance générale sans avoir une ou plusieurs personnes en tant que sujet principal. Le consentement (même tacite) est nécessaire pour les photos ciblées. En général, le fait de prendre une pose, individuellement ou en groupe, peut être considéré comme un consentement tacite à la prise de vue. Pour les photos non-ciblées, il suffit en général d'informer les personnes concernées. Lors d'événements publics (par exemple concerts, manifestatives sportives, spectacles culturels, marchés de Noël, ...), le consentement des personnes présentes peut être présumé à la prise de vue, en particulier si les conditions générales de l'évènement le précisent.

Plus d'informations :

- **Lignes directrices sur le droit à l'image établies par la Commission nationale pour la protection des données (CNPD)**

L'INFORMATION QUE DES PHOTOS SOIENT PRISES À

L'OCCASION D'UN ÉVÉNEMENT PEUT PRENDRE QUELLES FORMES ?

L'information des personnes présentes à un évènement peut être effectué par l'intermédiaire d'un renvoi vers un site web, par une information figurant sur l'invitation ou sur le billet d'entrée ou alors par un affichage approprié sur place.

Plus d'informations :

- **Lignes directrices sur le droit à l'image établies par la Commission nationale pour la protection des données (CNPD)**

EST-CE QUE LA PUBLICATION D'UNE PHOTO PAR UN PROFESSIONNEL (ENTREPRISES, ADMINISTRATIONS, ASSOCIATIONS) NÉCESSITE-T-ELLE TOUJOURS LE CONSENTEMENT DE LA PERSONNE CONCERNÉE ?

Non. Le droit à l'image et le droit à la protection des données à caractère personnel sont deux droits fondamentaux qui ne sont pas soumis aux mêmes conditions : ainsi, si, en matière de droit à l'image, le consentement tacite est admis pour la capture de l'image, tel n'est pas le cas en matière de droit à la protection des données. Dès lors, en absence d'un consentement explicite ou d'acte positif clair à la prise de vue, un responsable de traitement devra fonder son analyse sur une autre condition de licéité prévue par le RGPD. Un responsable de traitement pourra par exemple invoquer ses « intérêts légitimes ». Cette condition de licéité présuppose que le responsable du traitement prenne dûment en compte les « *libertés et droits fondamentaux de la personne concernée* ».

Plus d'informations :

- **Lignes directrices sur le droit à l'image établies par la Commission nationale pour la protection des données (CNPD)**

EXISTE-T-IL D'AUTRES DOCUMENTS FACILITANT LA MISE EN CONFORMITÉ AU RGPD ?

Oui, il existe notamment des guides pratiques élaborés par les autorités de contrôle belge et française.

Le premier guide, réalisé par l'autorité française, porte sur la sécurité des données à caractère personnel qui constitue un volet essentiel de la conformité au RGPD. Ainsi, il rappelle les précautions élémentaires à mettre en œuvre de façon systématique dans chaque organisation.

Le deuxième guide est élaboré par l'autorité belge et vise à donner un aperçu succinct des principaux droits et obligations qui découlent du RGPD et qui sont pertinents pour les PME. Ce guide offre une assistance utile et efficace aux PME dans la mise en œuvre de cette nouvelle règlementation. À noter que le document n'a pas l'ambition d'aborder de manière exhaustive toute la législation applicable en matière de protection des données à caractère personnel.

Plus d'informations :

- **Guide de la sécurité des données personnelles, édition 2018 de la Commission Nationale de l'Informatique et des Libertés (CNIL)**
- **Vade-mecum pour les PME de l'Autorité de protection des données (APD)**

LA SURVEILLANCE DES SALARIÉS DANS LE CADRE DES RELATIONS DE TRAVAIL

QU'EST-CE QU'UNE « SURVEILLANCE » DES SALARIÉS DANS LE CADRE DES RELATIONS DE TRAVAIL ?

La surveillance inclut toute activité qui, opérée au moyen d'instruments techniques, consiste en l'observation, la collecte ou l'enregistrement de manière non occasionnelle des données d'une ou plusieurs personnes relatives à des comportements, des mouvements, des communications ou à l'utilisation d'appareils électroniques et informatisés. Comme exemple on pourrait citer la vidéosurveillance, les contrôles électroniques des accès (par exemple les badges), les contrôles électroniques des horaires de travail, le traçage des communications et/ou l'enregistrement d'entretiens téléphoniques, le contrôle de l'utilisation d'internet ou des courriers électroniques, les dispositifs de géolocalisation (GPS) ou encore les systèmes biométriques. Contrairement à la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (abrogée par la loi du 1ier août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, le RGPD ne définit pas la notion de « surveillance ».

Plus d'informations :

- **Avis 02/2017 du groupe de travail « article 29 » du 8 juin 2017 sur le traitement des données à caractère personnel sur le lieu de travail**

QUELS SONT LES CHANGEMENTS PRINCIPAUX RELATIFS À LA SURVEILLANCE DES SALARIÉS DANS LE CADRE DES RELATIONS DE TRAVAIL APRÈS L'ENTRÉE EN VIGUEUR DU RGPD ?

Les changements majeurs en matière de surveillance des salariés dans le cadre des relations de travail peuvent être consultés dans la note d'information élaborée par la FEDIL. La loi du 1ier août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du RGPD au Luxembourg a été publiée le 16 août au Mémorial du Grand-duché de Luxembourg. Elle est applicable depuis le 20 août 2018.

Plus d'informations :

- **Note d'information de la FEDIL**

EXISTE-IL D'AUTRES DOCUMENTS FACILITANT LE RESPECT DES NOUVELLES DISPOSITIONS EN MATIÈRE DE SURVEILLANCE DES SALARIÉS DANS LE CADRE DES RELATIONS DE TRAVAIL ?

Oui, la Commission nationale pour la protection des données (CNPD) a publié le 14 août 2018 des lignes directrices en matière de vidéosurveillance. Elles s'adressent aux responsables du traitement souhaitant avoir ou ayant recours à des dispositifs de vidéosurveillance.

- **Lignes directrices élaborées en matière de vidéosurveillance par la CNPD**