# PROTECTION DES DONNÉES
# MODE D'EMPLOI

FEDIL

*The Voice of Luxembourg's Industry*

# INDEX

# *Le RGPD, c'est quoi ?*

Le RGPD vise à renforcer les droits des personnes physiques à l'égard du traitement de leurs données à caractère personnel. Pour ce faire, les entreprises se trouvent soumises à un ensemble d'obligations renforcées voire nouvelles, afin de garantir une légitimité du traitement. Le RGPD concerne uniquement les traitements de données à caractère personnel.

**25**
**MAI 2018**

***Date d'entrée en application***

### QU'EST-CE QU'UN TRAITEMENT ?

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction (article 4 RGPD).

### QU'EST-CE QU'UNE DONNÉE À CARACTÈRE PERSONNEL ?

Toute information se rapportant à une personne physique identifiée ou identifiable : est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale (article 4 RGPD).

Comme exemple on pourrait citer le nom, le prénom, le lieu de naissance, la date de naissance, l'adresse e-mail (professionnelle et personnelle), une photo, une vidéo, les données de localisation, les coordonnées bancaires, l'adresse IP, la plaque d'immatriculation d'une voiture, etc..

Uniquement les personnes physiques sont visées, sont donc exclues les données des sociétés et généralement des personnes morales.

### OÙ TROUVER LE RÈGLEMENT ?

Il est important de ne pas attendre la dernière minute : il faut être en conformité pour le 25 mai 2018.

### POURQUOI CE GUIDE ?

***Ce guide a un triple objectif :***

- vous aider à y voir plus clair dans l'implémentation de ce règlement et de la nouvelle discipline qu'il impose ;
- proposer les actions concrètes à entreprendre pour vous mettre en conformité ;
- bénéficier du support de la FEDIL dans le domaine.

***Le règlement s'applique :***

- au traitement des données à caractère personnel effectué dans le cadre des activités d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union ;
- au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union.

***Le RGPD concerne :***

- les responsables du traitement ;
- les sous-traitants.

Il est tout à fait possible d'être tour à tour responsable du traitement et sous-traitant, les deux peuvent coexister dans la même entité.

La conformité avec le RGPD vous permettra d'accroître la confiance de vos clients et des prospects dans l'entreprise lorsqu'ils vous confient leurs données personnelles.

## PAR OÙ COMMENCER ?

Avant de commencer à suivre les prescriptions de ce guide, il est fortement recommandé de désigner un référant, une personne en charge du dossier, qui puisse coordonner la mise en place du RGPD mais également devenir un référent en la matière au sein de l'entreprise.

## I. LE DPO – DATA PROTECTION OFFICER / DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Comme indiqué ci-dessus, il est vivement recommandé d'avoir une personne assignée dans l'entreprise – au besoin à côté de ses autres fonctions – à la protection des données. Étant donné que cette matière est appelée à se complexifier, la désignation d'un responsable des données devient un élément indispensable pour la compréhension du règlement et des obligations en découlant. Ce dernier sera également la personne de contact la mieux à même de dialoguer avec les autorités et ainsi réduire les risques de sanctions.

Toutefois, en dehors d'un choix tout à fait volontaire, les entreprises (à l'instar des autorités publiques) DOIVENT obligatoirement nommer un DPO si l'activité principale consiste :

- en des opérations de traitement exigeant un suivi régulier et systématique à grande échelle des personnes concernées ;
- en un traitement à grande échelle de catégories particulières de données ;
- en un traitement à grande échelle de données relatives à des condamnations pénales ou infractions.

Ce DPO peut être commun à plusieurs entités, il peut être externe, travailler à temps partiel et pour plusieurs entreprises. Or, le rôle de DPO ne peut en aucun cas être assumé par le chef d'entreprise ou par toute autre personne occupant un poste qui permet de déterminer les 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 ainsi exercer d'autres missions et tâches pour autant que celles-ci ne conduisent pas à un conflit d'intérêt.

***Le DPO aura une mission de conseil et d'accompagnement. Il devra :***

- contrôler la conformité de l'entreprise au RGPD mais aussi toute autre règlementation pertinente ;
- informer sur le contenu des obligations en matière de protection des données à caractère personnel ;
- être le point de contact de l'autorité de contrôle.

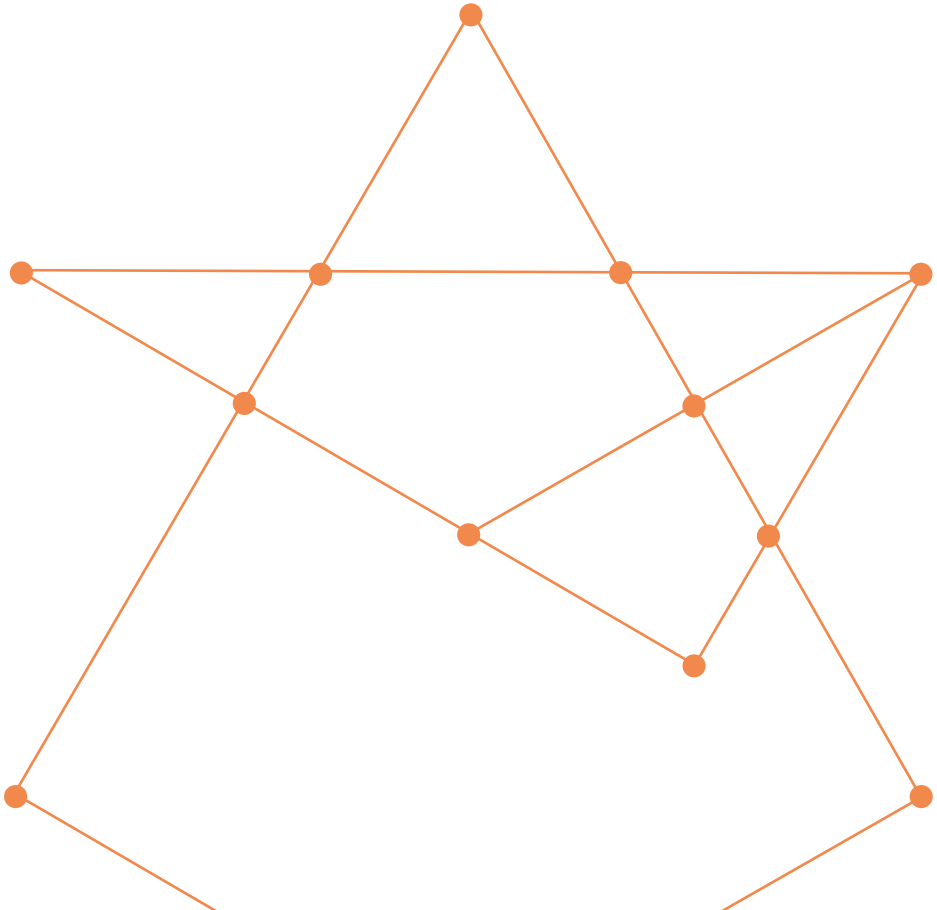
Il convient ici de mentionner qu'il appartient toujours au responsable du traitement de s'assurer qu'un registre des activités de traitement existe et est tenu à jour. On pourrait donc très bien imaginer que le DPO vérifie uniquement ledit registre qui est géré par quelqu'un d'autre. Il est aussi indispensable à relever que le délégué à la protection des données ne peut en principe pas être licencié en raison d'une violation des données à caractère personnel par le responsable du traitement. Il bénéficie donc d'une certaine protection.



Idéalement, ce dernier aura une formation juridique ou du moins sera à même de comprendre des textes légaux et règlementaires parfois complexes et aura une bonne vision de la structure de l'entreprise et de ses activités. Dans le cas d'une autorité publique ou d'un organisme public, le DPO devrait également avoir une bonne connaissance des règles et procédures administratives de l'organisme, mais tout en sachant qu'il n'existe aucune qualification professionnelle obligatoire au sens strict du terme.

Les lignes directrices du Groupe de travail « Article 29 » (qui sera remplacé à partir du 25 mai 2018 par le Comité européen de la protection des données) clarifient et illustrent d'exemples concrets le nouveau cadre juridique issu du RGPD. Il s'agit d'un organe consultatif européen indépendant traitant des questions liées à la protection des données et au respect de la vie privée.

Le texte en entier sur le délégué à la protection des données peut être consulté sur le site de la Commission Nationale pour la Protection des Données, en abrégé CNPD (www.cnpd.lu).



## II. GRANDS PRINCIPES DU RGPD

### 1. QUELLES SONT MES OBLIGATIONS EN TANT QU'ENTREPRISE ?

Pour être en conformité avec mes obligations légales, JE DOIS traiter les données :

- de manière licite, loyale et transparente ;
- pour des finalités déterminées, explicites et légitimes ;
- de manière adéquate, pertinente et limitée à ce qui est nécessaire ;
- de manière exacte et tenue à jour ;
- de manière temporaire et uniquement pour le délai nécessaire à leur traitement et suivant leur finalité ;
- avec un niveau de sécurité approprié.

La licéité du traitement n'est donnée que si certaines conditions sont remplies comme, par exemple, avoir recueilli le consentement de la personne concernée avant tout traitement, ou pouvoir justifier que le traitement est nécessaire à l'exécution d'un contrat, etc..

Une ligne directrice sur la transparence sous le RGPD a été élaborée par le Groupe de travail « Article 29 ». Cette ligne directrice est susceptible de modifications et n'est pas encore adoptée ! La version finale sera disponible sur le site de la CNPD (www.cnpd.lu).

***Et JE DOIS pouvoir démontrer la conformité de mes activités de traitement avec le règlement :***

- en tenant un registre des activités de traitement lorsque cela est nécessaire ;
- en ne traitant que les données personnelles a minima pour le traitement envisagé ;
- en rédigeant, en des termes clairs, une note d'information (« Privacy notice ») sur la manière dont sont collectées et utilisées les données personnelles ;
- en sensibilisant et en accompagnant mon personnel dans ses nouvelles obligations ;
- en effectuant une analyse d'impact relative à la protection des données pour identifier les risques pour les droits et les libertés des personnes concernées et surtout, afin de me permettre d'y apporter des solutions (humaines, informatiques, etc.) ;
- en mettant en place des procédures - techniques et organisationnelles efficaces - pour assurer le respect des dispositions légales et réglementaires et également en cas de faille.

***JE DOIS définir si j'agis en tant que :***

- responsable du traitement ou
- sous-traitant, sachant que suivant les données traitées, je peux être les deux à la fois.

Par exemple : je suis responsable du traitement en tant qu'employeur mais je peux être sous-traitant si je gère des données pour le compte d'un client.

***En tant que responsable du traitement*, JE DOIS :***

- examiner toutes mes activités de traitement de données et les consigner dans un registre des activités de traitement quand cela est obligatoire (ou base volontaire) ;
- m'assurer que j'ai mis en œuvre des mesures techniques et organisationnelles appropriées pour assurer la sécurité nécessaire des données à caractère personnel traitées dans mon entreprise ;
- respecter le principe de responsabilisation et coopérer avec la CNPD ;
- m'assurer que je dispose de procédures et de modèles appropriés pour surveiller, identifier, examiner et signaler rapidement des violations de données à la CNPD.

**Le responsable du traitement détermine les finalités et les moyens du traitement de données à caractère personnel.*

***En tant que sous-traitant*, JE DOIS :***

- examiner mes contrats existants et pouvoir garantir et assurer la sécurité et la confidentialité adéquates des données personnelles confiées ;
- traiter uniquement les données conformément aux instructions du responsable du traitement ;
- m'assurer que je dispose de procédures et de modèles appropriés pour surveiller, identifier, examiner et signaler rapidement les violations de données au responsable du traitement concerné ;
- obtenir l'accord du responsable du traitement pour désigner des sous-sous-traitants.

**Le sous-traitant agit pour le compte et sous les directives d'un responsable du traitement.*

### 2. QUELLES SONT MES RESPONSABILITÉS ?

Le RGPD change le paradigme habituel : il n'y a plus de demande préalable à effectuer auprès de la CNPD, mais cette dernière contrôlera a posteriori des traitements opérés. En cas de non-respect des dispositions légales, je m'expose à des amendes pouvant aller jusqu'à 4 % du chiffre d'affaires annuel mondial de l'exercice précédent ou 20 millions d'euros.

***JE DOIS :***

- rester pragmatique et gérer les priorités, c'est-à-dire identifier les risques les plus élevés compte tenu de la sensibilité des informations ou d'une protection insuffisante des données, etc. ;
- mettre en œuvre des mesures proportionnées au type de données traitées et à la finalité du traitement ;
- démontrer avoir rempli mes obligations afin de voir ma responsabilité minorée voire exclue.

Une ligne directrice sur l'application et la fixation des amendes administratives sous le RGPD a été adoptée par le Groupe de travail « Article 29 » et peut être consultée sur le site de la CNPD (www.cnpd.lu).

## III. L'APPLICATION EN ENTREPRISE : LE CHEMIN VERS LA CONFORMITÉ

### 1. CARTOGRAPHIE DES DONNÉES PERSONNELLES DÉTENUES PAR L'ENTREPRISE : OÙ SONT MES DONNÉES PERSONNELLES ?

***JE DOIS :***

- Identifier quels traitements de données contiennent des données personnelles.

***Est-ce que je traite des données personnelles ?***

Généralement, toutes les entreprises traitent des données personnelles, ne serait-ce que celles de leurs salariés.

Dans le cadre de cette identification des données personnelles, il convient de faire attention à une pseudonymisation non effective, où il serait facile de retrouver le titulaire des données par « croisement ».

Le règlement définit la « pseudonymisation » dans l'article 4 comme le « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable. ».

Ainsi, les données simplement pseudonymisées doivent être considérées comme des données à caractère personnel soumises au règlement si elles peuvent être attribuées à une personne physique identifiée, considération faite de l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour une telle identification.

***Où se trouvent les données personnelles que l'entreprise détient ?***
***JE DOIS :***

- avoir un aperçu clair des données dont je dispose et où elles se trouvent ;
- recenser ces données et les consigner afin de les rattacher à un traitement.

**UN EFFORT DE RECHERCHE :**

Deux approches peuvent être combinées pour plus d'efficacité : approche « bottom up » (ou ascendante) et/ou « top down » (descendante).

**A. APPROCHE DESCENDANTE :**

Je regarde la structure de mon entreprise, ses départements, ses sous-départements et quelles sont les données personnelles traitées par ces départements.

Je vais à la rencontre des personnes clefs pour appréhender au mieux les données personnelles et leur gestion.

- l'organigramme de la société permet d'identifier des personnes clefs et de discerner le contour des grandes catégories de traitement ;
- le support du management est indispensable. Les enjeux doivent être compris par le chef d'entreprise et les managers afin que les ressources nécessaires à la bonne exécution du processus soient mises à disposition.

**B. APPROCHE ASCENDANTE :**

La structure du réseau informatique, la base de données ainsi que son arborescence sont généralement de bons indicateurs.

Je demande à mon fournisseur informatique de m'aider à établir l'arborescence des traitements opérés au sein de mon entreprise afin de définir où les données sont stockées pour constituer une cartographie précise.

Cela permet de cibler des données moins usitées ou auxquelles personne n'avait pensé. Les deux approches doivent être complémentaires et ainsi couvrir toutes les données détenues par mon entreprise ainsi que tous les traitements y relatifs.

**UN EFFORT DE CLASSEMENT :**

***JE DOIS :***

- avoir une vision claire des données personnelles présentes dans mon entreprise ;
- classer les données « flottantes » ou non assignées.

Beaucoup de données et notamment personnelles, ne sont pas « classées » ou ne sont pas liées à un traitement déterminé. Il convient, dès lors, de les classer, respectivement de les rattacher à un traitement, mais en gardant à l'esprit que le RGPD ne s'applique uniquement aux données à caractère personnel.

*Exemples : cartes de visite, liste des enfants des salariés, etc..*

Si je ne sais pas affecter ces données, alors je dois me demander si ces dernières sont toujours utiles et s'il convient de les conserver.

Cet audit ne permet pas seulement de connaître les données personnelles présentes dans votre entreprise, il vous permettra de jeter les bases de l'élaboration d'un registre des activités de traitement (si nécessaire). Dès lors, il est important de faire cet exercice consciencieusement pour élaborer non seulement ledit registre, en identifiant les données traitées, leurs finalités et la durée d'utilisation nécessaire au traitement, mais aussi pour apporter des réponses aux dysfonctionnements éventuellement constatés comme par exemple l'oubli qu'on traite une certaine catégorie de données à caractère personnel.

Le résultat est un catalogue des données personnelles traitées :
- elles sont identifiées ;
- elles sont classées ;
- elles sont assignées à un traitement.

### 2. POURQUOI AI-JE CES DONNÉES PERSONNELLES ?

***JE DOIS :***
- assigner les données à un traitement déterminé ;
- savoir précisément pourquoi je collecte les données (exemple : fichier de prospects) ;
- savoir précisément pourquoi je les traite (exemple : en vue d'un démarchage commercial ciblé) ;
- supprimer toutes les données devenues obsolètes ;
- m'assurer que je ne conserve que des données strictement nécessaires à la poursuite de mes objectifs.

Il faut distinguer les données personnelles externes (exemples : clients, fournisseurs, prospects) et les données personnelles internes (exemple : salariés de l'entreprise).

Je pourrai ainsi déterminer si j'agis comme responsable du traitement ou sous-traitant, élément fondamental dans la détermination du contour de mes obligations.

> *Exemples : gestion des clients, gestion d'accès, recrutement et gestion du personnel, événementiel, etc..*

Le recensement des données et leur affectation à un traitement permet dès lors :
- de supprimer toutes les données à caractère personnel devenues obsolètes ou inutiles et de ne conserver que l'utile et le nécessaire ;
- de définir le juste niveau de confidentialité et d'accès alors que toutes les données n'ont pas à être connues de toute l'organisation.

***Combien de temps dois-je garder des données et à quel moment les effacer ?***
***JE DOIS :***
- prévoir une durée de conservation des données personnelles pour chaque catégorie de traitement ;
- renseigner cette durée dans le registre des activités de traitement (quand ce dernier est obligatoire) et la communiquer à la personne concernée ;
- pouvoir justifier les objectifs et finalités de la durée de cette conservation.

« L'accumulation » de données personnelles est proscrite par le règlement. Par conséquent, il est important, au moyen de l'analyse précédemment opérée, de les gérer de manière adéquate mais surtout de les effacer lorsqu'elles sont obsolètes ou lorsque le traitement pour lequel elles ont été recueillies est terminé.



Cela ne veut pas dire que toutes les données doivent être effacées sitôt qu'un projet/traitement s'arrête, mais leur quantité doit être réduite au strict minimum, si possible anonymisées et leur accès doit être limité.

Généralement, les durées de prescription sont un bon indicateur, sauf si on peut justifier une durée de conservation plus longue.

L'anonymisation concerne des informations ne pouvant pas être rattachées à une personne identifiée. Ainsi, les données à caractère personnel rendues anonymes font que la personne concernée ne soit pas ou plus identifiable.

Pour déterminer si une personne physique est identifiable, le RGPD précise qu'il convient de « prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. ».

Lorsque la personne physique n'est pas identifiable, le règlement ne s'applique pas.

### 3. QUELS SONT MES FLUX DE DONNÉES ?

***JE DOIS :***
- absolument connaître mes flux de données : savoir d'où elles proviennent et où elles vont.

#### 1. D'OÙ PROVIENNENT MES DONNÉES ?

***Sont-elles importées ?***

Est-ce que je vais moi-même rechercher des données personnelles et est-ce que je procède à leur traitement : réseaux sociaux, enregistrement de données de mails, recherches spécifiques, ... ?

> *Exemple : un recruteur cherchant des profils de candidats intéressants sur les réseaux sociaux.*

***Sont-elles fournies ?***

Ces données sont-elles volontairement fournies ?

> *Exemples : CV, formulaire d'adhésion, etc..*

Cette question est également importante pour la recherche du consentement et déterminera par la suite le droit à l'information des personnes concernées.

## 2. OÙ VONT MES DONNÉES ?

***Où sont-elles susceptibles d'être exportées/transférées ?***
***JE DOIS :***

- savoir exactement à qui mes données sont susceptibles d'être transférées.

Par exemple, un recruteur transfèrera des données personnelles de candidats (CV) à des sociétés clientes ou pouvant le devenir. Dans le cadre d'un fichier client, ce dernier peut servir à plusieurs entités du groupe et sera donc transféré entre différentes entités.

***JE DOIS :***

- savoir exactement dans quels pays seront transférées mes données, car des règles différentes peuvent s'appliquer ;
- choisir des prestataires informatiques pouvant garantir le niveau de protection exigé par le RGPD.

***Que dois-je faire si je transfère mes données hors de l'UE ?***
***JE DOIS :***

- vérifier si le pays hors UE possède un niveau de protection équivalent à celui de l'Union européenne en matière de protection des données (pays listés ci-dessous) ;
- si le pays hors UE ne possède un niveau de protection adéquat, entourer le transfert de garanties appropriées (clauses contractuelles types, règles contraignantes d'entreprises (BCR), codes de conduite ou certifications) ou, à défaut, recourir aux dérogations de l'article 49 du RGPD (parmi lesquelles le consentement explicite et informé de la personne concernée).

Un graphique très intéressant peut être consulté sur la page 11 du document suivant :

À ce stade, on pourrait également s'inspirer du modèle à minima d'information des destinataires des données établi par la Commission Nationale de l'Informatique et des Libertés (CNIL), homologue français de la CNPD :

Certains de ces destinataires sont situés en dehors de l'Union européenne, et en particulier les destinataires suivants :

***Destinataires / pays***

Les garanties suivantes ont été prises pour s'assurer d'un niveau de protection suffisant des données personnelles :



{type de garantie}{référence} (clause contractuelle type, règle contraignante d'entreprise, code de conduite, certification)

Conformément au Règlement général sur la protection des données (RGPD), vous pouvez exercer votre droit à la rectification ou à l'effacement des données, à la limitation du traitement, s'opposer au traitement et à la portabilité des données. Si votre traitement est basé sur le consentement, vous disposez également du droit de retirer ce consentement à tout moment en contactant {service en charge du droit d'accès} ».

***Qu'est-ce qu'on entend par « pays à niveau de protection équivalent » ?***

Par pays à niveau de protection équivalent on entend : les pays de l'Espace Économique Européen (EEE), Principauté d'Andorre, Argentine, Canada, Iles Féroé, Ile de Man, Guernesey, Jersey, Nouvelle-Zélande, Israël, Uruguay, Suisse, et dans certains cas seulement les États-Unis.

En effet, il convient ici de rechercher sur le site www.privacyshield.gov si l'entreprise destinataire des données adhère à l'accord "*Privacy Shield*" qui a été négocié entre 2015 et 2016 entre l'Union européenne et les États-Unis.

## 3. QUI A ACCÈS À MES DONNÉES ?

- dans mon entreprise ?

***JE DOIS :***

- identifier qui a accès aux données et dans quelle mesure ;
- prévoir des limitations si l'accès est trop général.
- en externe ?

***JE DOIS :***

- établir une liste claire de mes fournisseurs et de mes sous-traitants ;
- m'assurer que les sous-traitants/partenaires connaissent leurs nouvelles obligations et leurs responsabilités, à l'aide d'un document contractuel ;

  *Exemple 1 : la gestion des salaires par une société externe.*

  *Exemple 2 : l'hébergement et l'opération d'un système IT.*
- savoir où sont stockées les données détenues par mon entreprise afin de pouvoir vérifier le niveau de protection dont elles bénéficient contre des accès non autorisés notamment.

La relation contractuelle avec le sous-traitant (partenaires, clients, fournisseurs) doit être clairement encadrée. Il est indispensable d'insérer des clauses contractuelles reprenant les obligations de chacun relatives à la protection des données personnelles (telles que reprise sous l'article 28 (3) du RGPD).

## 4. COMMENT MES DONNÉES SONT-ELLES SÉCURISÉES ?

***JE DOIS :***

- évaluer le risque lié aux données personnelles conservées ;
- réaliser une analyse d'impact pour les données personnelles et/ou traitements susceptibles d'engendrer des risques élevés pour les droits et libertés de la personne concernée ;
- sécuriser l'accès à mes données pour minimiser les risques d'accès non autorisés et donc limiter les risques de fuites de données et l'impact sur la vie privée des personnes concernées ;
- définir le niveau adéquat de protection en fonction des risques liés aux données : pseudonymisation, chiffrement, limitation de droits d'accès, ...

Plus la donnée et/ou le traitement sera sensible, plus le niveau d'assurance devra être important.

Exemples de traitements nécessitant une analyse d'impact relative à la protection des données :

- traitement à grande échelle (exemple : laboratoire d'analyse) ;
- surveillance systématique à grande échelle d'une zone accessible au public (exemple : vidéosurveillance) ;
- traitement de données sensibles (données concernant la santé, données biométriques, données génétiques, opinions politiques, orientation sexuelle, appartenance syndicale, etc.) ;
- l'évaluation ou la notation basée sur des données personnelles y compris le profilage et la prédiction (exemple : politique de cookies ou de recueil de l'adresse IP pour des offres ciblées).

***Je DOIS réaliser cette analyse d'impact :***

- avant de collecter des données et de procéder au traitement ;
- sur tout traitement susceptible d'engendrer des risques élevés pour les droits et libertés des personnes physiques.

***Cette analyse comprend :***

- une description du traitement et de ses finalités ;
- une évaluation de la nécessité et de la proportionnalité du traitement ;
- une appréciation des risques sur les droits et libertés des personnes concernées ;
- les mesures envisagées pour traiter ces risques et se conformer au règlement.

***Que faire pour protéger les données que je traite ?***

Le risque ne doit pas simplement être vu au niveau de l'organisation mais du point de vue des droits de la personne concernée.

Il sera question d'analyser ou de mettre en place des systèmes de protection notamment pour surveiller et contrôler le flux de données ainsi que les données stockées et leur accès. Les risques doivent également être évalués du côté des fournisseurs/clients ou encore de tiers afin de permettre la mise en place de solutions informatiques et juridiques adéquates.

Il est fondamental dans ce contexte d'identifier les risques les plus élevés, respectivement, de voir où sont conservées les informations personnelles les plus sensibles afin d'y apporter en premier lieu les solutions adéquates.

À noter que les numéros IBAN, les arrêts de maladie, les listes d'absence et les listes d'allergènes ne sont en principe pas considérés comme sensibles au sens du RGPD.

***Qu'est-ce qui se passe-t-il si, malgré mes précautions, une faille se produit ?***
***JE DOIS :***

- être proactif et avoir mis en place un mécanisme de gestion de crise / avertissement ;
- être en mesure d'apporter les preuves de la mise en place de mesures de protection des données appropriées et de démontrer cette conformité à tout moment ;
- avoir une procédure d'information à l'égard de la CNPD et de la personne concernée.

Le délai de notification à la CNPD est extrêmement bref : La violation doit être notifiée dans les meilleurs délais et, si possible, au plus tard 72 heures après en avoir pris connaissance. Lorsque la notification à l'autorité de contrôle concernée n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

Un responsable du traitement a « pris connaissance d'une violation » lorsqu'il a une certitude raisonnable qu'il y a eu un incident de sécurité impliquant des données à caractère personnel. Cela variera au cas par cas, mais si un tel incident a eu lieu, il est important de vérifier immédiatement si des données à caractère personnel ont été violées et, dans l'affirmative, de prendre des mesures et de notifier la violation si nécessaire.

- en cas de faille, il est important de prévoir des schémas de transmission et des procédures permettant d'activer la transmission d'informations ;
- obligation d'information des personnes concernées dans les meilleurs délais lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

La notification doit indiquer aussi bien la nature de la violation ainsi que des recommandations sur la manière dont la personne concernée peut limiter les conséquences négatives potentielles (par exemple, en changeant le mot de passe individuel). En principe, les personnes concernées doivent être informées individuellement, à moins que cela ne soit disproportionné. Dans ce cas, les personnes concernées peuvent être informées au moyen d'un message général, par exemple par une mention sur le site web, une newsletter ou un e-mail général.

Il est fortement conseillé de prévoir des évaluations régulières de la sécurité des installations (au minimum 1 fois par an) et des procédures automatisées au niveau de l'entreprise.

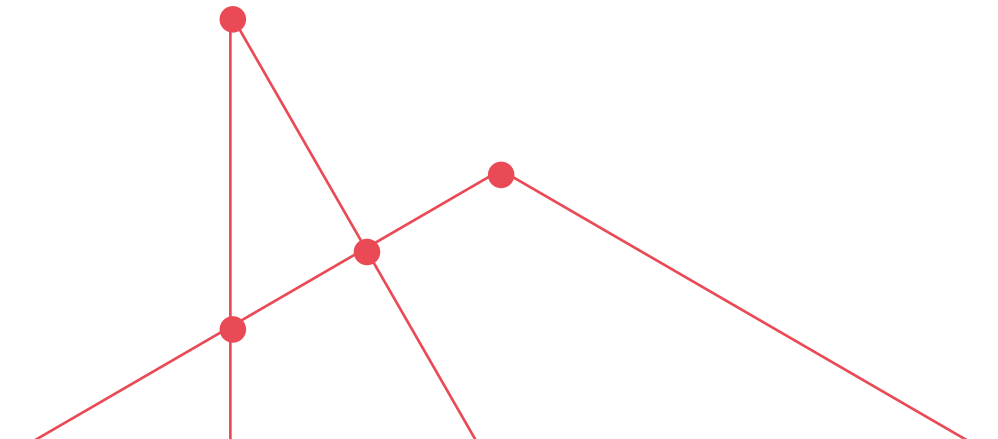
## 5. NÉCESSITÉ D'UNE PRISE DE CONSCIENCE DE L'ENSEMBLE DES COLLABORATEURS ET SURTOUT DES PERSONNES INVESTIES D'UN POUVOIR DE DÉCISION

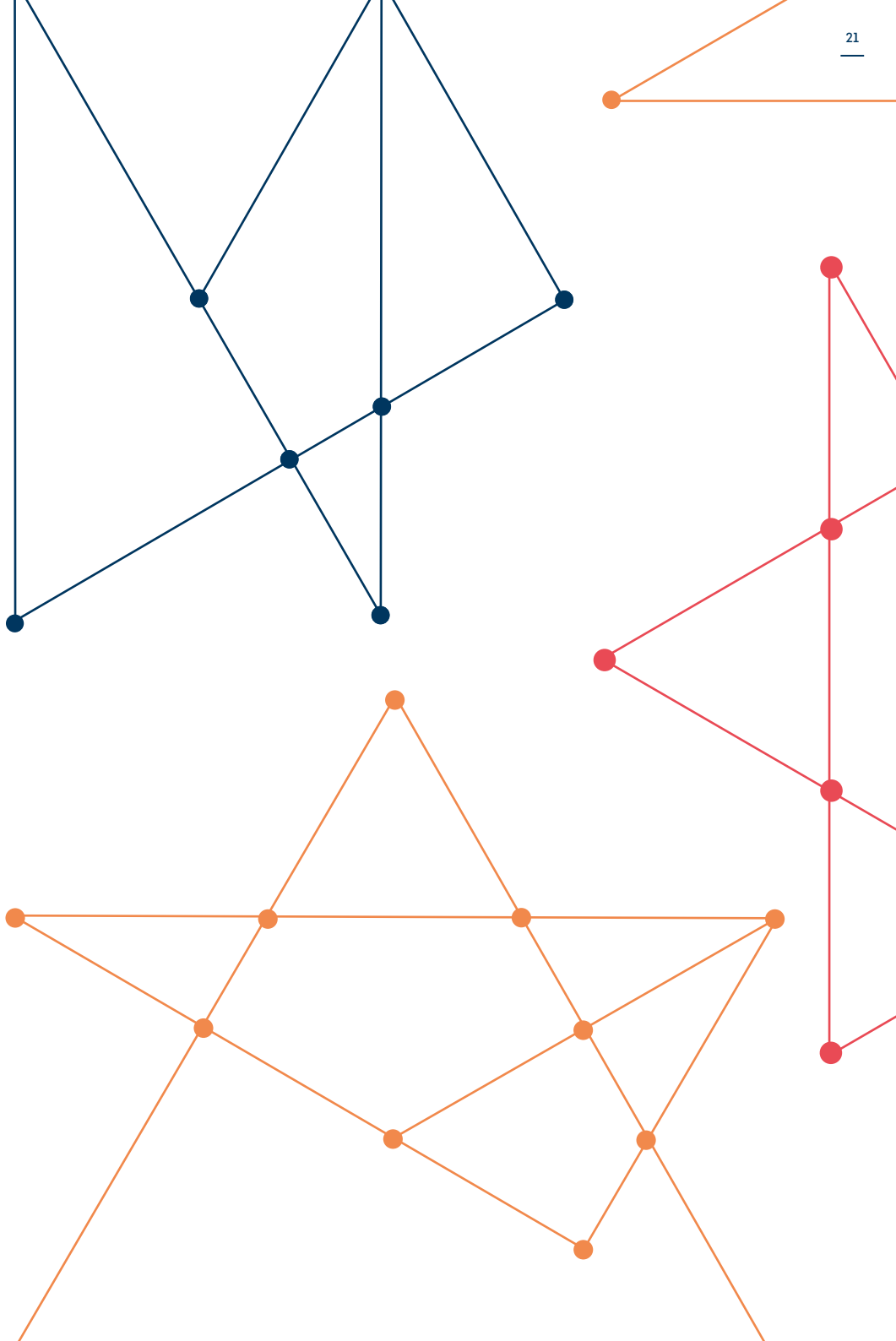
***JE DOIS :***

- sensibiliser et former mes collaborateurs sur les enjeux de la protection des données à caractère personnel ;
- m'assurer régulièrement que ces derniers maîtrisent le concept de protection des données ;
- m'assurer que mes collaborateurs et moi-même pensons au traitement des données à caractère personnel dès la conception d'un nouveau projet :
  - principe de protection des données dès la conception (« privacy by design ») ;
  - principe de protection des données par défaut, donc les paramètres sont mis tels que le mode le plus « privacy friendly » soit assuré, par exemple un browser n'accepte par défaut pas de cookies – sauf si l'utilisateur change ce paramètre (« privacy by default »).

Tous les salariés de l'entreprise doivent connaître les implications du RGPD et les nouvelles obligations en découlant. De la même manière, une attention particulière devra être portée à la protection des données à caractère personnel lorsque de nouveaux traitements seront mis en place (par exemple : nouvelle étude de marché). En effet, le RGPD a notamment introduit les concepts-clés indiqués ci-dessous qui participent à l'organisation et au respect du principe de responsabilisation (« accountability ») :

« Privacy by design and by default » : Le responsable du traitement doit dès le commencement du projet, au moment même de la détermination des moyens de traitement et pendant le traitement lui-même, envisager la protection des données à caractère personnel. Pour cela, il doit mettre en place un ensemble de mesures visant à garantir la protection des données à caractère personnel (restrictions, anonymisation, ...). Sans cette rigueur, tous les efforts entrepris précédemment n'auront qu'un intérêt limité et la mise en conformité ne pourra être pérenne.





## IV. EST-CE QUE LE TRAITEMENT OPÉRÉ EST LICITE ?

***Pour qu'un traitement soit licite, il doit :***

- soit être effectué sur base du consentement de la personne concernée ;
- soit être nécessaire pour :
  - l'exécution d'un contrat (exemple : la livraison d'un bien, ...) ;
  - l'exécution d'une obligation légale (exemple : déclaration d'entrée et de sortie auprès du CCSS, ...) ;
  - la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne (exemple : personne traitée aux urgences d'un hôpital, ...) ;
  - l'exécution d'une mission d'intérêt public (exemple : enquête du STATEC, ...) ;
  - des intérêts légitimes poursuivis par le responsable du traitement (exemple : mettre à disposition un annuaire interne avec les contacts des salariés d'une entreprise, ...).

***JE DOIS :***

- identifier dans quelle catégorie se situe mon traitement ;
- déterminer si je suis dans l'exécution d'un contrat ou dans un des autres cas de figure ;
- me rappeler que le consentement n'est requis que s'il n'entre pas dans un des cas précédemment mentionnés ;
- m'assurer que même en l'absence de consentement, le titulaire des données personnelles est aussi averti de tout traitement dont il ferait l'objet (fenêtre automatique, mention au contrat, mail d'information, ...).

Il convient donc de clarifier qu'un traitement des données parfaitement sécurisé ne sert à rien, s'il n'est pas licite (donc s'il ne satisfait à aucune des conditions énumérées ci-dessus).

### 1. LE CONSENTEMENT DU TITULAIRE DES DROITS

***Si le consentement est requis (donc s'il constitue la base juridique sur laquelle se fonde le traitement), JE DOIS :***

- déterminer comment est recueilli, enregistré et géré le consentement du titulaire du droit ;
- rédiger des procédures de recueil du consentement ;
- ne pas procéder au traitement en l'absence de consentement exprès.

***Ai-je recueilli un consentement pour l'utilisation de ces données ? Qu'est-ce que le consentement ?***

Il s'agit de 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.

Le consentement est un acte volontaire de la part de la personne concernée (mécanisme de l'« opt-in »). Le silence ou l'absence de réaction ne peut pas être considéré comme un consentement.

Le consentement doit être donné de manière claire, non équivoque, spécifique pour un traitement défini et sans contrainte.



La contrainte se manifeste notamment lorsque la personne doit donner son consentement sans quoi il ne peut plus poursuivre le processus (exemple : consentement nécessaire à la consultation d'un site Internet, ...).

***JE DOIS DONC :***

- mettre en place un mécanisme de recueil du consentement et de rétractation ;
- préciser les principales caractéristiques du traitement (objet, finalité, durée, etc.) afin que la personne sache clairement à quoi elle consent ;
- démontrer avoir obtenu le consentement de la personne ;
- consigner et conserver la charge de la preuve du consentement dans le registre des activités de traitement (date, heure, etc.) ou en l'absence de ce dernier, tout autre support aisément consultable par l'autorité de contrôle me dispensant du consentement exprès.

Lors de chaque nouveau traitement, il est impératif de se demander si un consentement est requis ou non.

En revanche, si le consentement a été donné avant l'entrée en application du RGPD et s'il répond aux nouvelles exigences, il n'est pas nécessaire de l'obtenir à nouveau.

***Est-ce que l'information relative au traitement était simple et claire ?***

Le libellé de la demande de consentement doit être clair et parfaitement compréhensible. Le détenteur des données doit savoir pour quelle raison et de quelle manière ses données personnelles seront traitées.

***Ai-je donné l'explication de l'utilisation de ces données :***

- de manière concise ?
- de manière transparente (utilisation à cette seule fin) ?
- de manière compréhensible et facilement accessible par l'utilisateur ?
- dans des termes simples et clairs ?

***JE DOIS :***

- proscrire les cases pré-cochées ou les formulaires préremplis ;
- proscrire les descriptions indigestes et les renvois à des documents ;
- faire un résumé synthétique du traitement opéré et de ses finalités.

***S'agissait-il d'un enfant ?***

Auquel cas, le consentement des parents est nécessaire au Luxembourg jusqu'à 16 ans révolus. Les autres pays de l'Union européenne peuvent déterminer par la loi nationale un âge inférieur pour autant que cet âge ne soit pas en-dessous de 13 ans. Ainsi, il faudra vérifier l'âge requis au cas par cas suivant le lieu où les données sont traitées et recueillies.

***Mentions devant figurer dans une clause type***

Il est impossible de rédiger une clause type pouvant convenir à toutes les situations, mais les éléments suivants doivent y figurer :

***JE DOIS :***

- m'identifier en tant que responsable du traitement (nom de l'entreprise et coordonnées) ;
- expliquer pourquoi les données sont collectées ;
  - les explications doivent être données de manière claire et compréhensible ;
  - les finalités du traitement doivent être expliquées ;
  - l'explication de la finalité du traitement doit être succincte et exhaustive ;
- si un traitement connexe est envisagé, alors je dois le signaler et l'expliquer pour recueillir le consentement de la personne concernée ;
- m'assurer qu'il n'y ait aucune dépendance (économique, sociale, professionnelle) et pas de contrainte dans le recueil du consentement qui limiterait la liberté de consentir (il faut toujours garder en arrière-tête que le consentement, s'il est requis, doit être libre, spécifique, éclairé et univoque) ;
- indiquer où la personne peut trouver des informations plus détaillées sur le traitement et sur le responsable du traitement ;
- indiquer la durée de conservation des données ;
- indiquer qui aura accès à ces données ;
- mentionner les droits dont le titulaire dispose (effacement, rectification, ...) ;
- mettre en place un système d'adhésion actif, comme par exemple des cases à cocher.

Les acceptations par défaut ou les cases préremplies sont désormais exclues. Il faut donc un consentement exprès, une manifestation positive : le silence ne constitue pas une acceptation.

Une ligne directrice sur le consentement a été élaborée par le Groupe de travail « Article 29 ». Cette ligne directrice est susceptible de modifications et n'est pas encore adoptée! La version finale sera disponible sur le site de la CNPD (www.cnpd.lu).

## 2. DIFFÉRENTS CAS DE FIGURE QUI NE RENDENT PAS NÉCESSAIRE LE CONSENTEMENT

***L'exécution d'un contrat***

***JE DOIS :***

- regarder s'il s'agit d'un contrat ou d'une phase précontractuelle ;
- informer la personne concernée que ses données personnelles sont traitées.

Le traitement est considéré comme licite lorsqu'il est nécessaire dans le cadre d'un contrat ou de l'intention de conclure un contrat (exemple : procédure d'embauche, ...).



Il faut cependant que le traitement soit effectivement nécessaire au contrat et à son exécution sinon le consentement doit être recueilli.

*Exemple 1 : Le consentement n'est pas requis lorsque le traitement de l'adresse postale d'un client est opéré pour lui faire parvenir une commande.*

Par contre, l'utilisation de l'adresse collectée à des fins de démarchage publicitaire doit avoir fait l'objet d'un consentement – ou d'une autre base de licéité - puisque cela est non directement lié à l'exécution d'un contrat principal.

*Exemple 2 : Le traitement des données des salariés par l'employeur pour opérer les justes retenues fiscales et sociales n'est pas soumis à consentement – car ce traitement est une obligation légale.*

***L'obligation légale ou l'exécution d'une mission d'intérêt public***

***JE DOIS :***

- vérifier si le traitement se fait en vue d'une obligation légale.

Le traitement sera considéré comme licite lorsqu'il est effectué pour répondre à une obligation légale à laquelle le responsable du traitement est soumis ou lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'autorité publique.

*Exemple : Communication des rémunérations des salariés de l'entreprise à l'Administration des Contributions Directes (ACD) afin d'établir la correcte retenue.*

***L'intérêt vital***

Le traitement sera considéré comme licite lorsqu'un intérêt vital de la personne concernée ou d'une autre personne est en jeu.

*Exemple : communication de données de santé nécessaire dans l'urgence.*

***L'intérêt légitime***

***JE DOIS :***

- justifier la poursuite d'un intérêt légitime afin de procéder au traitement sans le consentement d'un salarié.

Le RGPD met en balance les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, et les droits et libertés fondamentaux de la personne concernée. Le responsable du traitement devra ainsi démontrer que ses intérêts prévalent sur ceux de la personne concernée. (exemple : acquittement d'une facture, ...)

*Exemple : une entreprise utilise les données de ses clients afin de les contacter pour mettre en conformité une installation ou encore pour déterminer si ces derniers ont acheté un produit se révélant défectueux.*

## V. LE REGISTRE DES ACTIVITÉS DE TRAITEMENT

***JE DOIS tenir un registre des activités de traitement si :***

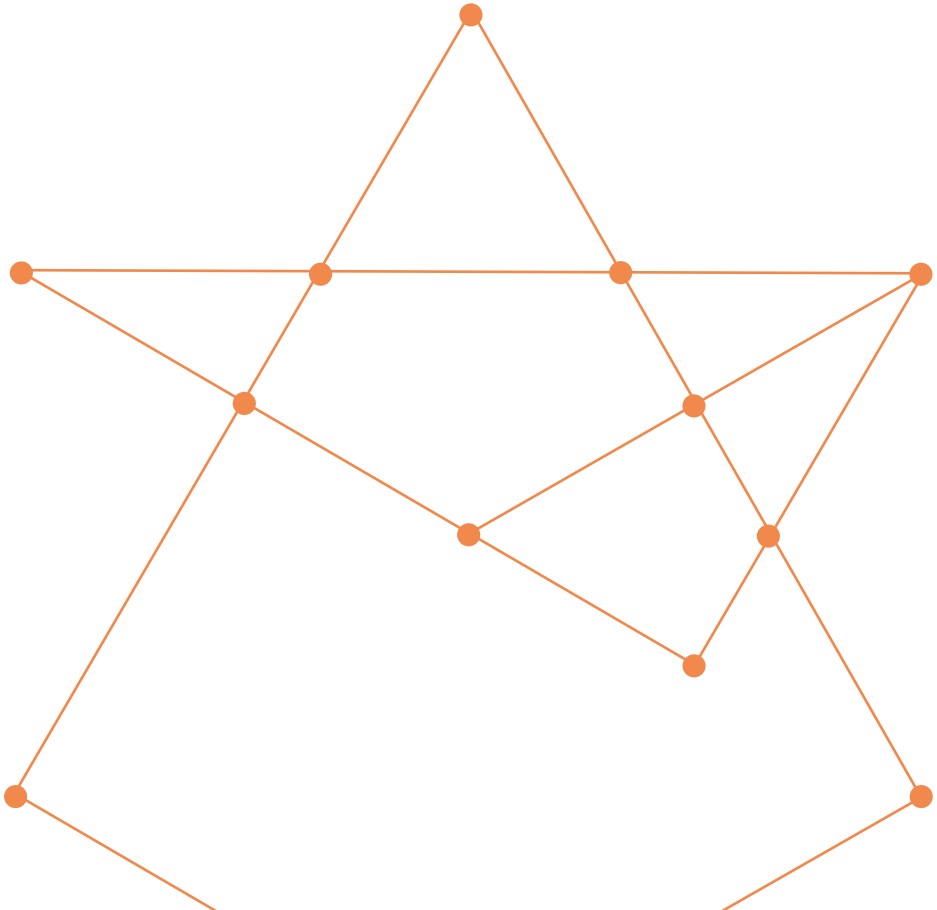
- mon entreprise compte plus de 250 salariés ;
- mon entreprise compte moins de 250 salariés et si je me trouve dans un des cas suivants :
  - le traitement est susceptible de comporter un risque pour les droits et des libertés des personnes concernées ;
  - le traitement porte notamment sur les catégories particulières de données (origine raciale ou ethnique, opinions politiques ou philosophiques, condamnations pénales, infractions, ...) ;
  - le traitement n'est pas occasionnel – donc habituel (exemple : système de vidéosurveillance visant à surveiller certains comportements/installations ou gestion habituelle de données personnelles en très grand nombre : fiduciaire, recruteurs, agences d'intérim, etc., il est indispensable de clarifier que la gestion du personnel n'est pas considérée comme un traitement occasionnel).

Que le registre des activités de traitement au sens strict du terme soit obligatoire ou non, il est conseillé de disposer d'un registre (cartographie) afin de pouvoir visualiser rapidement les différentes informations sur les traitements opérés et de pouvoir fournir rapidement l'information en cas de contrôle. En outre, la tenue d'un tel registre reste préconisée afin de permettre de documenter la mise en conformité aux autres obligations imposées par le RGPD.

Ce registre n'est pas soumis à un formalisme particulier, mais il doit impérativement reprendre certaines dispositions obligatoires (voir glossaire de fin). Il peut donc être sous format Excel, un programme informatique ou tout autre support facilement accessible par l'autorité de contrôle.

Pour chaque traitement, JE DOIS me poser les questions suivantes et les renseigner dans le registre :

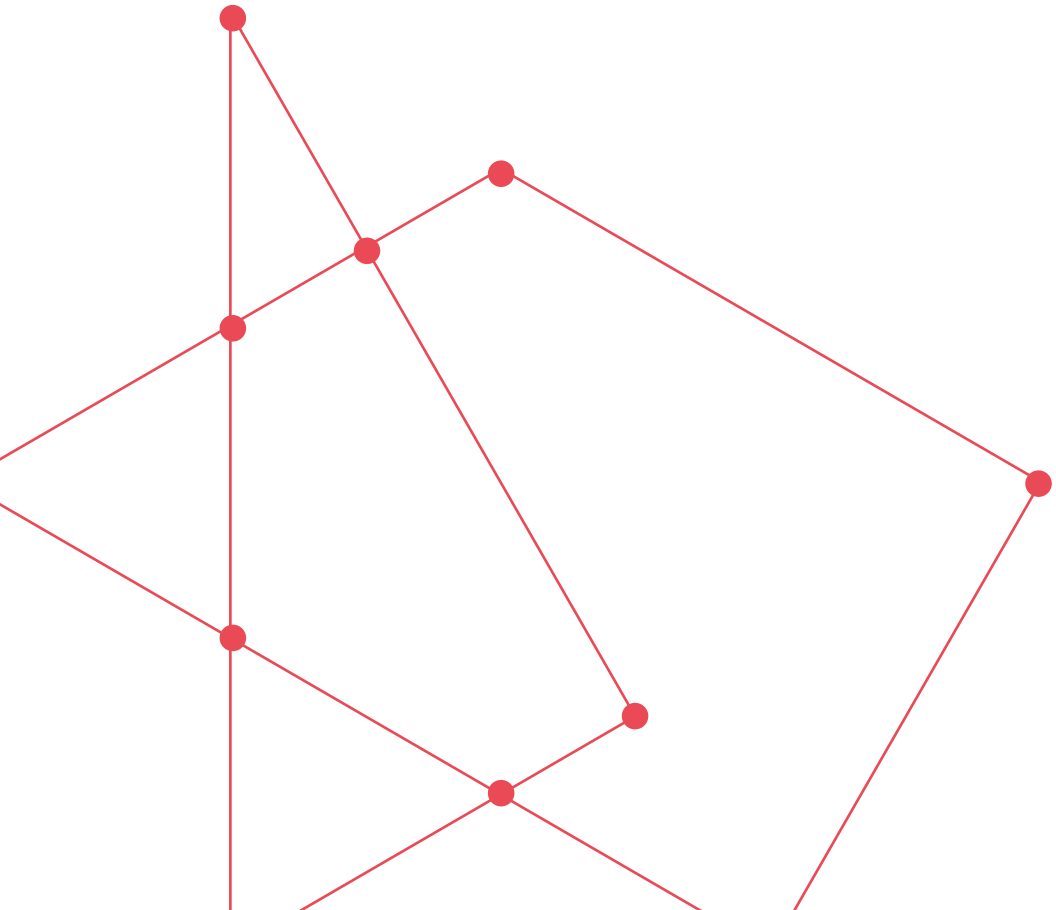
- qui est en charge du traitement ?
  - j'indique le nom et les coordonnées du responsable du traitement (et de son représentant légal) et, le cas échéant, du délégué à la protection des données,
  - j'établis une liste des sous-traitants.
- qu'est-ce qui est traité ?
  - j'identifie les catégories de données traitées,
  - j'identifie les données « sensibles » entraînant des risques accrus (exemples : les données relatives à la santé ou les infractions, les orientations sexuelles, etc.).
- pourquoi cela est traité ?
  - je communique la ou les finalité(s) pour laquelle ou lesquelles je collecte et traite ces données (exemples : gestion de la relation commerciale, gestion RH, ...).
- où est-ce que cela est traité ?
  - j'indique où les données sont hébergées,
  - j'indique vers quels pays les données seront éventuellement transférées.
- pendant quelle durée ces données seront-elles conservées ?
  - pour chaque catégorie de données, j'indique la durée de conservation.
- comment cela est protégé ?
  - je précise les mesures de sécurité mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc l'impact sur la vie privée des personnes concernées,
  - je cible prioritairement les données sensibles (données concernant la santé, données, biométriques, données génétiques, appartenance syndicale, les convictions religieuses ou philosophiques, etc.).



## VI. LES NOUVEAUX DROITS DES PERSONNES CONCERNÉES RESPECTIVEMENT LES NOUVEAUX DEVOIRS DE L'ENTREPRISE

***JE DOIS adapter mes traitements conformément aux nouvelles dispositions :***
***Droit à l'information :***

Les informations relatives au traitement des données personnelles doivent être fournies de façon concise, transparente et aisément accessible. Ces informations doivent être gratuites, sauf si les demandes sont manifestement infondées ou excessives (il appartient dans ce cas au responsable du traitement de prouver ce caractère manifestement infondé ou excessif), notamment en raison de leur caractère répétitif : possibilité de refuser de répondre ou d'exiger le paiement des frais administratifs supportés en conséquence. Quant au droit d'accès, le responsable du traitement peut exiger le paiement de frais raisonnables sur la base des coûts administratifs supportés pour toute copie complémentaire qui serait demandée (c'est-à-dire pour tout exemplaire supplémentaire demandé en sus de l'exemplaire initial).





***JE DOIS :***

- respecter le délai d'un mois pour répondre à toute demande sauf demande de prolongation (maximum 2 mois) ;
- dans tous les cas de figure informer la personne que des données à caractère personnel la concernant sont traitées et l'informer sur ses droits (que les données soient ou non collectées auprès de la personne concernée).

À nouveau, on pourrait se référer au modèle à minima d'information établi par la Commission Nationale de l'Informatique et des Libertés (CNIL) :

« Les informations recueillies sur ce formulaire sont enregistrées dans un fichier informatisé par {responsable de traitement} pour {finalités du traitement}. Elles sont conservées pendant {durée de conservation} et sont destinées à {destinataires des données}.

Conformément au Règlement général sur la protection des données (RGPD), vous pouvez exercer votre droit d'accès aux données vous concernant et les faire rectifier en contactant : {service en charge du droit d'accès} »

***Droit à la portabilité des données :***

***JE DOIS :***

- pouvoir restituer les données collectées sur un support « habituel », c'est-à-dire structuré, couramment utilisé et lisible à la personne concernée qui en fait la demande dans un délai de 1 mois après réception de la demande. Ce délai peut être prolongé à un maximum de trois mois pour les affaires complexes, à condition que la personne concernée ait été informée des motifs de cette prolongation dans un délai d'un mois à compter de la réception de la demande initiale ;
- pouvoir démontrer avoir supprimé les données des personnes ayant requis la portabilité de leurs informations ;
- mettre en place un règlement et des procédures permettant la garantie de ces droits.

La personne concernée peut demander le transfert de ses données personnelles d'un environnement informatique à un autre d'une manière sûre et sécurisée, mais il n'existe pas d'obligation du responsable du traitement de faire cela, c'est encouragé. Seules les données personnelles qu'un individu a fournies à un responsable du traitement (sur la base du consentement ou du contrat) sont concernées.

Des lignes directrices sur le droit à la portabilité des données ont été adoptées par le Groupe de travail « Article 29 » et peuvent être consultées sur le site de la CNPD (www.cnpd.lu).

***Droit d'accès et de rectification :***

***JE DOIS :***

- permettre aux personnes concernées d'accéder à leurs données ;
- mettre en place des mesures effectives de rectifications lorsque cela est demandé.

***Droit d'opposition :***

Les personnes peuvent (dans certains cas) s'opposer au traitement de leurs données à caractère personnel. Dans ce cas, les intérêts légitimes du responsable du traitement sont mis en balance avec les intérêts, droits et libertés de la personne concernée.

***Décision individuelle automatisée, y compris le profilage :***

Je réfléchis à ma politique de « cookies » et de profilage. Est considéré comme profilage « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données {...} pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique » (considérant 71 du règlement).

***JE DOIS :***

- avertir la personne concernée d'un tel traitement ;
- mettre en place des mécanismes d' « opt-out » permettant de sortir de traitements automatisés.

Des lignes directrices sur le profilage ont été adoptées par le Groupe de travail « Article 29 » et peuvent être consultées sur le site de la CNPD (www.cnpd.lu).

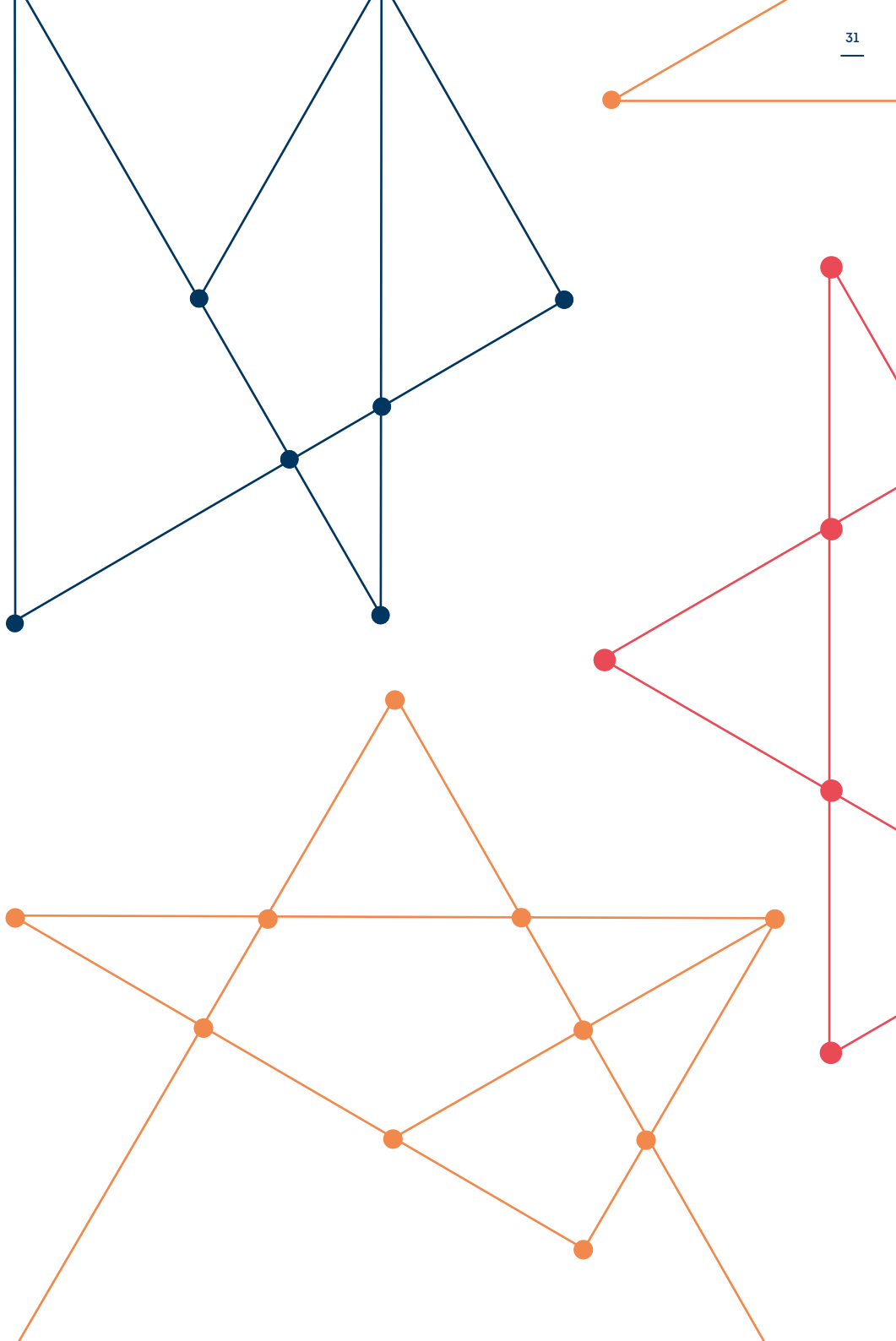
***Droit à l'oubli :***

Le RGPD prévoit, pour le titulaire d'un droit, l'effacement de ses données personnelles sur simple demande. Ce droit n'est toutefois pas absolu et peut par exemple se heurter à l'intérêt légitime du responsable du traitement – ou aux obligations légales dont ce dernier est soumis. Ainsi, par exemple, une personne devant acquitter une facture ne pourra demander purement et simplement l'effacement de ses données pour échapper à sa dette, la conservation des données de son débiteur étant pour le responsable du traitement légitime au moins jusqu'au paiement.

***JE DOIS EFFACER LES DONNEES lorsque :***

- elles ne sont plus nécessaires au traitement ;
- la personne a retiré son consentement ;
- la personne a fait jouer son droit à l'effacement ;
- le traitement est illicite.





## VII. COMMENT EFFECTUER UN PLAN D'ACTION POUR LA MISE EN ŒUVRE DU RGPD ?

Au cours des processus précédents, je me suis aperçu que je n'étais pas conforme aux prescriptions du RGPD. Dès lors, je dois mettre en place un plan d'action pour pallier à mes carences. Il est important de rester pragmatique dans l'approche. Les solutions et leurs coûts doivent être pondérés avec la nature des données à protéger (plus une donnée est sensible, plus elle mérite protection).

***JE DOIS DONC :***

- remédier aux lacunes constatées ;
- prioriser les actions à mener au regard des risques ;
- idéalement, rassembler une équipe pluridisciplinaire pour permettre de confronter les points de vue mais aussi les réalités du terrain.

Ce plan d'action devra contenir les mesures permettant d'/de :

1. identifier / cerner les problèmes relatifs au traitement des données personnelles ;
2. identifier la ou les solutions et opérer un arbitrage entre les solutions quand cela est nécessaire, exemples : Pseudonymisation, formation des salariés, suppression de données, etc. ;
3. éduquer les collaborateurs au traitement des données personnelles ;
4. concevoir le traitement de données dès la conception (« privacy by design ») et réaliser des études d'impact pour chaque traitement opéré ;
5. adapter les traitements pour que ces derniers deviennent conformes aux prescriptions du RGPD ;
6. rédiger des informations quant à la gestion des données personnelles (« privacy notice ») pour les différents traitements, afin de donner aux personnes un ensemble d'informations relatives aux traitements opérés ;
7. prévoir des délais stricts mais réalistes, toujours dans l'idée que les solutions devront être implémentées avant le 25.05.2018 ;
8. revoir les contrats avec l'ensemble des sous-traitants opérant avec des données personnelles de l'entreprise et les modalités de la collaboration pour assurer une application effective et efficiente du RGPD :
   i. objet du contrat, nature, durée, finalité de traitement ;
   ii. fin de la relation contractuelle ;
   iii preuves de garanties suffisantes pour être conforme avec le RGPD ;
   iv. encadrement strict du traitement des données ;
      1. valable pour tous les sous-traitants même étrangers ;
      2. auditer le sous-traitant : véritable audit ou feuille de renseignement ;
      3. engagement contractuel indispensable.
9. gérer la relation contractuelle dans sa globalité et notamment quant aux éventuels sous-traitants du sous-traitant ;



10. réfléchir quant à l'opportunité de mettre en place des solutions informatiques spécifiques pour permettre d'automatiser certains processus et permettre une certaine fluidité dans la gestion des données personnelles ;
    - purge automatique de certains dossiers contenant des données personnelles suivant des critères à établir (durée, mission terminée, etc.) ;
    - effacement automatique de documents après plusieurs mois/années, etc. ;
    - cryptage automatique de certaines informations avec degré d'accessibilité ;
    - ....

Il faut insister sur le fait que pas toutes les entreprises ou organismes avec lesquels on entretient des relations contractuelles sont à considérer comme sous-traitant au sens du RGPD. Ainsi, il convient de se référer à l'avis 1/2010 du 16 février 2010 du groupe de travail « G29 » ayant établi un faisceau d'indices pour bien définir la qualité de sous-traitant. Il faut notamment prendre en considération les questions suivantes :

- niveau d'instruction donné par le client au prestataire : quelle est l'autonomie du prestataire dans la réalisation de sa prestation ?
- degré de contrôle de l'exécution de la prestation : quel est le degré de « surveillance » du client sur la prestation ?
- valeur ajoutée fournie par le prestataire : le prestataire dispose-t-il d'une expertise approfondie dans le domaine ?
- degré de transparence sur le recours à un prestataire : l'identité du prestataire est-elle connue des personnes concernées qui utilisent les services du client ?

L'avis est disponible dans son intégralité sur le site de la CNPD (www.cnpd.lu).

***Être conforme, c'est une action sur la durée !***

Veuillez encore noter que la CNPD a développé, avec le soutien de Digital Luxembourg, ensemble avec le Luxembourg Institute of Science and Technology (LIST), un « GDPR Compliance Support Tool » afin d'aider les acteurs dans leur tâche d'intégration des dispositions du RGPD dans leur politique interne.

Ainsi, l'objectif de cet outil est d'offrir une solution innovante et intuitive aux utilisateurs permettant de vérifier le niveau de maturité de leurs organisations en matière de protection des données. L'outil permettra aux utilisateurs non seulement de gérer un registre de traitement et tous les autres documents nécessaires à démontrer leur responsabilité, mais aussi de réaliser un suivi sur l'évolution du niveau de maturité de leurs organisations.

Le « GDPR Compliance Support Tool » peut être consulté sous le lien suivant :

https://cst.cnpd.lu/portal/

## GLOSSAIRE DE FIN

*Analyse d'impact relative à la protection des données*, selon les lignes directrices du Groupe de travail « Article 29 », la mise en œuvre d'une analyse d'impact relative à la protection des données est nécessaire si plusieurs des critères suivants s'appliquent au traitement de données à caractère personnel :

- le traitement effectue une évaluation ou notation, y compris le profilage et la prédiction ;
- le traitement effectue des décisions automatiques résultant en des implications légales ou similaires pour les personnes concernées ;
- le traitement consiste en une surveillance systématique des personnes concernées (traitements utilisés pour observer, surveiller ou contrôler les personnes concernées, y compris les données collectées à partir d'une surveillance systématique des lieux accessibles au public) ;
- des données sensibles (suivant la définition de la règlementation) font l'objet du traitement ;
- le traitement est un traitement à grande échelle :
  - le nombre de personnes concernées est élevé ou proportionnellement élevé par rapport à une population ;
  - le volume de données traitées est important ;
  - la durée ou la permanence de l'activité de traitement est importante ;
  - l'étendue géographique du traitement est importante.
- les jeux de données à caractère personnel ont été combinés d'une manière qui pourrait dépasser les attentes raisonnables des personnes concernées ;
- les données traitées concernent des personnes vulnérables (exemple : situation de déséquilibre des pouvoirs entre les personnes concernées et le responsable du traitement comme c'est le cas pour une entreprise mettant en place un contrôle de l'activité de ses salariés) ;
- le traitement se rapporte à l'usage ou l'application de solutions technologiques ou organisationnelles innovantes ;
- le traitement de données ne permet pas aux personnes concernées d'exercer leur droit ou les empêche d'accéder à un service ou un contrat (exemple : une banque qui analyse le profil de ses clients pour décider de leur offrir un crédit ou pas).

Le texte en entier peut être consulté sur le site de la CNPD (www.cnpd.lu).

*Autorité de contrôle concernée*, une autorité de contrôle qui est concernée par le traitement de données à caractère personnel parce que :

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

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

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

*Binding Corporate Rules (BCR)*, instrument juridique européen auquel une société multinationale ou un groupe d'entreprises peut recourir afin de garantir un niveau adéquat de protection des données à caractère personnel lors du transfert de ces données, au sein du groupe, au départ d'un pays situé dans l'Union européenne (UE) ou dans l'Espace économique européen (EEE) vers un pays tiers. Ces règles nécessitent d'être approuvées au préalable par l'autorité de contrôle nationale.

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

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

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

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

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

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

*Groupe d'entreprises*, une entreprise qui exerce le contrôle et les entreprises qu'elle contrôle.

*Etablissement principal*,

a) en ce qui concerne un responsable du traitement établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement a le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal.

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

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

*Identifiable*, pouvant être identifié, directement ou indirectement.

*Identifiants*, nom, prénom, date de naissance, numéro de sécurité sociale, adresse, plaque d'immatriculation, ...

*Limitation du traitement*, le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur.

*Personne concernée*, titulaires des données personnelles et donc des droits afférents. Personne identifiée ou identifiable.

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

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



*Responsable du traitement*, la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

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

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

*Registre des activités de traitement*,

1. Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes :

   a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;

   b) les finalités du traitement;

   c) une description des catégories de personnes concernées et des catégories de données à caractère personnel;

   d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales;

   e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;

   f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;

   g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

2. Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant :

   a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données;

   b) les catégories de traitements effectués pour le compte de chaque responsable du traitement;

   c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;

   d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

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

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

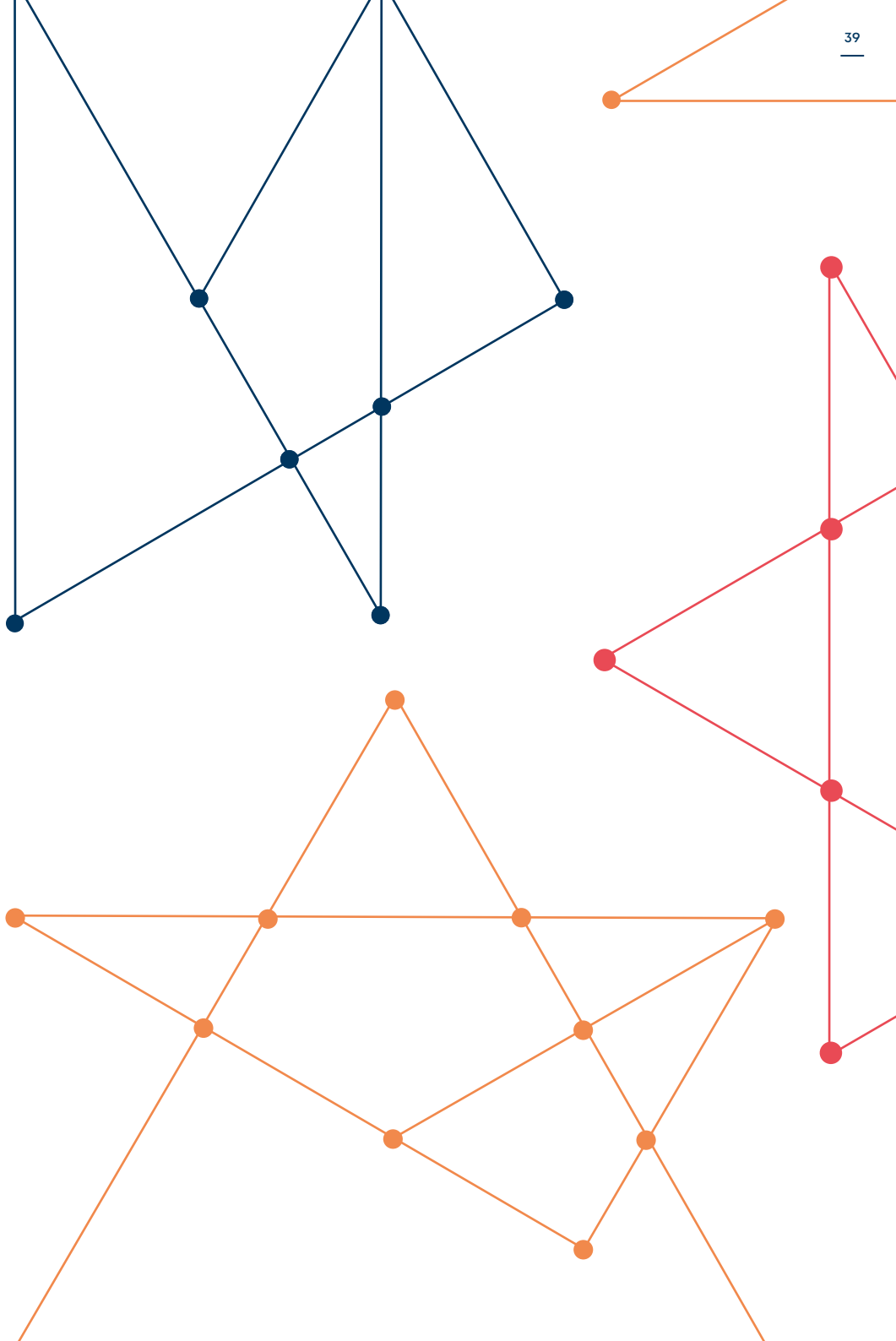
*Violation de données à caractère personnel*, une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé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

*Traitement transfrontalier*,

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

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





# GDPR TERRITORIAL SCOPE – SUBJECTS, CONTROLLERS AND PROCESSORS

### DATA SUBJECT

*An identified or identifiable natural person*

### DATA CONTROLLER

*Natural or legal person, public authority, agency or other body which, alone or jointly, with others, determines the purposes and means of the processing of personal data*

### DATA PROECESSOR

*Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*

## 1

### CONTROLLER / PROCESSOR IN THE EU

*The processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not.*

## 2

### DATA SUBJECTS IN EU, CONTROLLER / PROCESSOR NOT

*Processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where processing activities related to:*

*1) The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU.*

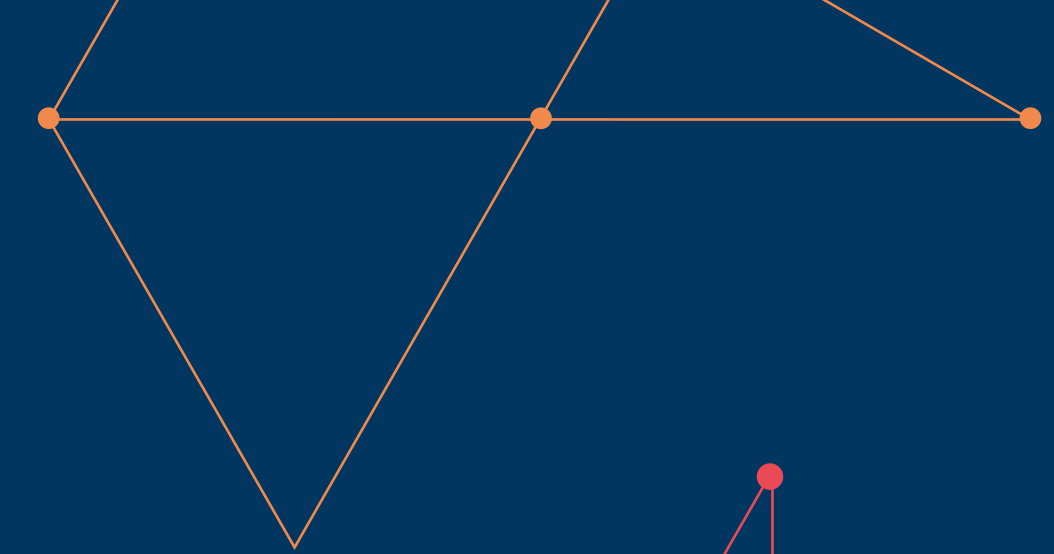
*2) The monitoring of their behaviour as far as their behaviour takes place within the EU.*

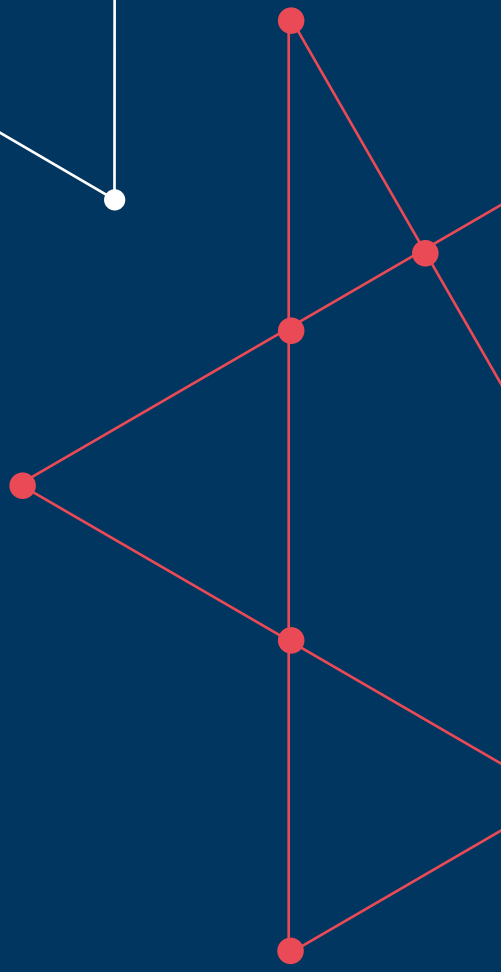
## 3

### CONTROLLER OUTSIDE THE EU

*The processing of personal data by a controller not established in the EU but in a place where Member State law applies by virtue of public international law.*

*texte repris par une illustration de i-scoop.eu*





**PUBLISHED BY:**
*FEDIL - The Voice of Luxembourg's Industry*

**PRINTED BY:**
*Victor Buck Services*

**GRAPHICS BY:**
*cl'ff*

# FEDIL

**Office**
*7, rue Alcide de Gasperi*
*Luxembourg-Kirchberg*

*fedil@fedil.lu*
**T** *+352 43 53 66-1*
**F** *+352 43 23 28*
**W** *fedil.lu*

**Postal Address**
*P.O. Box 1304*
*L-1013 Luxembourg*