Le Règlement Général sur la Protection des Données (RGPD) en 10 leçons

L'essentiel du RGPD dans un guide pratique

Janvier 2017

Par Laure LANDES-GRONOWSKI
Avocate Associée, Agil'IT
Pôle IT & data protection

Sommaire

INTRODUCTION 3

LEÇON 1 – LE REGLEMENT S'APPLIQUE A TOUS ! (OU COMMENT DETERMINER SI MON ORGANISATION EST SOUMISE AU RGPD)..... 5

LEÇON 2 – DECRYPTER LES PRINCIPES GENERAUX DU REGLEMENT 10

LEÇON 3 – RESPECTER LES DROITS DES PERSONNES CONCERNEES 15

LEÇON 4 – COMPRENDRE L'ACCOUNTABILITY ET DEPLOYER LES MESURES NECESSAIRES A UNE VERITABLE GOUVERNANCE DES DONNEES..... 22

LEÇON 5 – ORGANISER LES RELATIONS ENTRE LES ACTEURS DU TRAITEMENT..... 28

LEÇON 6 – DEPLOYER LES MESURES DE SECURITE ET DE CONFIDENTIALITE ADEQUATES .. 33

LEÇON 7 – DESIGNER UN DELEGUE A LA PROTECTION DES DONNEES..... 37

LEÇON 8 – ENCADRER LES TRANSFERTS DE DONNEES HORS UNION EUROPEENNE 42

LEÇON 9 – GERER LE SORT DES DONNEES PRESENTANT UNE CERTAINE SENSIBILITE..... 48

LEÇON 10 – ANTICIPER LES POURSUITES ET LES SANCTIONS 53

INTRODUCTION

Le règlement européen sur la protection des données à caractère personnel (RGPD) est entré en vigueur[1]. Bien que son application ait été différée au mois de **mai 2018**, il est temps de se pencher sur les implications concrètes en résultant. Les conséquences sur les processus des entreprises sont en effet considérables.

C'est l'objectif de cette série de fiches intitulée « Le RGPD en 10 leçons » !

L'idée n'est pas de faire le tour de toutes les subtilités du règlement (il faudrait plus de 10 leçons…) mais de vous permettre, de prendre conscience des obligations et enjeux résultant de l'entrée en application de cette nouvelle règlementation, et d'initier une démarche de mise en conformité.

Ces 10 leçons s'articuleront autour des thématiques suivantes :

1. Le champ d'application du RGPD
2. Les principes généraux
3. Les droits des personnes concernées
4. Le principe d'accountability
5. Les relations entre les acteurs
6. La sécurité des données
7. Le délégué à la protection des données
8. Les transferts de données hors Union européenne
9. Les données sensibles
10. Les poursuites et sanctions encourues

[1] Règlement 2016/679/UE du 27-4-2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).

Bien entendu, il demeure encore à connaître la position et l'interprétation des autorités de référence et de contrôles (G29, Cnil,…) sur différentes thématiques du RGPD. Par ailleurs, divers actes pris par la Commission européenne ou par les autorités de contrôle, ainsi que la réglementation nationale des Etats membres pourront venir compléter les dispositions du règlement. Toutefois, compte tenu de l'ensemble des actions et mesures à déployer pour se mettre en conformité avec la nouvelle règlementation, **c'est le moment ou jamais de prendre les devants**, et ce d'autant qu'une mise en conformité s'impose dans les meilleurs délais.

En effet, il y a fort à parier que les autorités de contrôle ne feront pas preuve d'indulgence dans le cadre de leur mission de vérification de l'application conforme du règlement, notamment au regard du délai de deux ans accordé aux organismes concernés pour se mettre en conformité, ainsi que du fait que les principes et obligations du règlement ne sont pas tous nouveaux…

Or, les sanctions financières encourues en cas de non-respect de ces nouvelles dispositions sont particulièrement dissuasives, à savoir une amende administrative pouvant s'élever **à 20 millions d'euros** ou, pour une entreprise, pouvant aller jusqu'à **4% du chiffre d'affaires annuel mondial total de l'exercice précédent**, le montant le plus élevé étant retenu.

Sur ce, **bonne lecture** et n'hésitez pas à nous faire connaître les sujets que vous souhaiteriez voir abordés dans le cadre de focus à développer ultérieurement !

*

* *

Leçon 1 – Le règlement s'applique à tous !
(ou comment déterminer si mon organisation est soumise au RGPD)

C'est parti pour la 1ère leçon relative au RGPD qui vise à répondre à la question que tout le monde se pose (ou devrait se poser…) : suis-je concerné par cette nouvelle règlementation ?

Et cette question n'est pas des moindre dans la mesure où, qu'on se le dise, tout le monde (ou presque) est concerné !

Voici pour s'en convaincre un décryptage des critères qui, s'ils sont réunis, font à coup sûr tomber une entité sous le joug des dispositions du règlement.

Critère 1 : Votre entité met en œuvre un (ou plusieurs) traitement(s) de données à caractère personnel…

Le RGPD a vocation à s'appliquer aux traitements de données à caractère personnel, qu'ils soient automatisés (même en partie) ou non (à condition que les données traitées soient contenues ou appelées à figurer dans un fichier).

A cet égard, il convient de préciser qu'un **traitement** de données est défini comme toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel.

Quelques exemples d'opérations considérées comme des traitements *:*
Collecte, enregistrement, organisation, structuration, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion, mise à disposition, rapprochement, interconnexion, limitation, effacement, destruction, etc.

Une **donnée à caractère personnel** est constituée par toute information qui se rapporte à une personne physique, qu'elle soit identifiée, voire simplement identifiable (même indirectement, par exemple, par un numéro identifiant ou un recoupement d'informations).

Quelques exemples de données à caractère personnel *:*
Identité, coordonnées, numéro identifiant, données de localisation, informations relatives à la vie professionnelle, habitudes de consommation, adresse IP, etc.

Il résulte de ces notions particulièrement larges qu'il y a fort à parier que votre entreprise met en œuvre des traitements de données à caractère personnel, ne serait-ce que pour gérer les membres de son personnel et les rémunérations ou encore dans le cadre de la tenue et de la mise à jour des fichiers de suivi des fournisseurs et des contacts personnes physiques qui y sont rattachés par exemple.

En effet, même dans le monde professionnel ou encore dans le cadre de relations économiques ou commerciales entre des entreprises, les personnes physiques disposent d'un droit à la protection de leurs données à caractère personnel !

Quelques illustrations de traitements coutants de données à caractère personnel :
Gestion du personnel et des rémunérations, trombinoscope et annuaire d'entreprise, gestion des fournisseurs, gestion de la comptabilité, gestion des clients et des opérations commerciales, de fidélisation et de prospection, gestion des outils informatiques, lutte contre la fraude (interne / externe), surveillance (vidéo, alarme, contrôle des accès,…), PRA/PCA/PSI, etc.

Attention, les **traitements « manuels »** de données à caractère personnel sont également concernés et soumis aux dispositions du règlement à condition que les données soient contenues ou appelées à figurer dans un fichier, défini comme un ensemble structuré de données accessibles selon des critères déterminés (que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique).

Certains traitements sont toutefois exclus de l'application du règlement. Bien qu'ils soient marginaux, il peut être opportun de savoir les identifier. Il s'agit des traitements suivants :

- les traitements mis en œuvre dans le cadre d'une **activité strictement personnelle ou domestique**, et donc sans lien avec une activité professionnelle ou commerciale (à noter que cette exception ne concerne que les personnes physiques). A titre d'exemple, sur le fondement de cette exception, le répertoire téléphonique d'un téléphone mobile personnel constitue bien un traitement de données à caractère personnel mais n'est pas soumis aux dispositions du règlement. En revanche, un téléphone utilisé à des fins professionnelles doit être géré conformément aux dispositions du règlement ;

- les traitements mis en œuvre **par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exaction de sanctions pénales** (ces traitements faisant l'objet d'une directive dédiée[2]) ;

- les traitements effectués **dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union européenne**, par exemple en matière de sécurité nationale ;

- les traitements mis en œuvre **par les Etats membres dans le cadre de leurs activités ayant trait à la politique étrangère et de sécurité commune de l'Union**.

[2] Directive 2016/680/UE du 27-4-2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

Anonymisation ou pseudonymisation ?
Enfin, il convient de préciser que les traitements de données réellement anonymisées n'entrent pas dans le champ d'application du règlement dans la mesure où ces données ne permettent pas, même indirectement, d'être rattachées à une personne physique identifiable. Toutefois, seule une réelle anonymisation irréversible peut permettre de se prévaloir d'une telle exception à l'application du règlement. A l'inverse, les données simplement pseudonymisées (même si une telle pratique est encouragée et réduit les risques pour les personnes concernées) 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 utilisé pour une telle identification.

Critère 2 : … Qu'elle soit responsable de traitement ou qu'elle agisse comme sous-traitant…

Le RGPD prévoit des obligations à la charge des organismes **responsables de traitement**, définis comme toute personne physique ou morale, autorité publique, service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Notion centrale et faisceau d'indices
S'agissant de l'identification du responsable de traitement, une analyse au cas par cas, in concreto, doit être menée pour tout traitement mis en œuvre dans la mesure où cette notion est centrale : il s'agit de l'entité sur laquelle repose les principales obligations en matière de protection des données à caractère personnel.
A cet égard, divers critères et indices doivent être pris en compte afin de déterminer l'entité devant être qualifiée de responsable de traitement[3] : initiative du traitement et définition de la finalité / des objectifs, influence de droit ou de fait sur le traitement et degré d'influence, autonomie et pouvoir décisionnaire, image donnée aux personnes concernées et attentes raisonnables que cette visibilité peut susciter chez ces dernières, détermination des moyens matériels, humains, techniques et organisationnels du traitement, etc.

Mais le règlement est également applicable aux entités qui traitent les données en qualité de **sous-traitant**, c'est-à-dire qui traitent les données pour le compte d'un tiers, lui-même responsable de traitement.

En effet, si le sous-traitant agit par définition uniquement pour le compte (et donc sur instruction) du responsable de traitement, certaines obligations spécifiques, voir stratégiques, sont tout de même mises à sa charge par le règlement.

Le sous-traitant : un responsable de traitement « par ailleurs »
En tout état de cause, le fait pour une entité d'agir comme sous-traitant dans le cadre d'un traitement de données n'exclut pas sa qualité de responsable de traitement par ailleurs, pour les traitements mis en œuvre pour son propre compte…

[3] G29, Avis 1/2010 du 16-2-2010 sur les notions de responsable de traitement et de sous-traitant.

Ainsi, qu'une entité agisse en qualité de responsable de traitement ou de sous-traitant dans le cadre d'un traitement de données à caractère personnel, le règlement lui est applicable.

Critère 3 : … Et les traitements ont un lien géographique avec l'Union européenne

L'application du RGPD d'un point de vue territorial dépend en premier lieu du **lieu de l'établissement de l'entité** : le règlement s'applique aux traitements de données mis en œuvre dans le cadre de l'activité d'un établissement d'une entité situé sur le territoire de l'Union européenne, que l'entité en question dispose de la qualité de responsable de traitement ou de sous-traitant, et que le traitement ait lieu ou non dans l'Union européenne.

A noter : si un responsable de traitement n'est pas établi dans l'Union européenne mais tout de même dans un lieu où le droit d'un Etat membre de l'Union européenne s'applique, alors le règlement lui est également applicable.

Notion d'établissement :
Si la notion d'établissement suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable, la forme juridique de cet établissement n'est pas déterminante (il peut s'agir d'une simple succursale ou au contraire d'une filiale disposant de la personnalité juridique).

En second lieu, si le responsable de traitement ou le sous-traitant n'est pas établi en Union européenne, alors le RGPD peut tout de même s'appliquer en fonction du **lieu où se trouvent les personnes concernées** par le traitement, c'est-à-dire les personnes dont les données sont traitées.

En effet, dans cette hypothèse, le règlement s'applique si les personnes concernées se trouvent sur le territoire d'un Etat membre de l'Union européenne, et si le traitement est lié :

- soit à une offre de biens ou de services à destination desdites personnes concernées ;

Notion d'offre de biens ou services à des personnes concernées au sein de l'Union
Sur ce point, il est précisé que la simple accessibilité du site internet de l'entité depuis le territoire de l'Union européenne ne suffit pas pour considérer que celui-ci offre des biens ou des services à des personnes concernées se trouvant dans l'Union européenne. En revanche, des facteurs tels que l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs pays de l'Union européenne, avec la possibilité de commander des biens ou services dans cette langue, ou la référence sur le site internet à des clients ou utilisateurs établis dans l'Union européenne, peuvent indiquer clairement que des biens ou services sont proposés à des personnes concernées en Union européenne.

- soit au suivi du comportement de ces personnes dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union européenne.

Notion de suivi du comportement
A titre d'exemple, un suivi des internautes dans le cadre de leur navigation sur le web, couplé avec des techniques de traitement visant à déterminer un profil, notamment afin de prendre des décisions ou d'analyser leurs préférences de consommation, leurs comportements, etc. répond à la notion de suivi du comportement de ces personnes.

* *
*

Le constat est sans appel : le nouveau règlement européen sur la protection des données s'applique à la majorité des entreprises et il est plus que temps d'envisager de se mettre en conformité !

Votre entité réunit tous les critères ? Alors rendez-vous aux prochaines leçons qui s'attacheront à faire le point sur les obligations en résultant…

Références textuelles
Considérants 14) à 30)
Articles premier, 2, 3 et 4

Leçon 2 – Décrypter les principes généraux du règlement

La leçon 1 vous a fait prendre conscience que le RGPD est applicable à votre entité, soit! Il convient désormais de se pencher sur les principes applicables en matière de traitement des données à caractère personnel à l'aune de ce règlement.

Le respect de ces principes est un préalable nécessaire à tout traitement de données à caractère personnel. Ils se répartissent en deux groupes : les principes applicables aux données et les principes applicables aux traitements en tant que tels[4].

Il ne s'agit pas de grandes déclarations de principe mais bien de dispositions qui doivent présider à la mise en œuvre et au maintien en conformité des traitements de données à caractère personnel par toute entité soumise au règlement. C'est pourquoi il convient de déterminer concrètement ce à quoi ils correspondent ainsi que les incidences en résultant.

1/ Principes concernant les données

S'agissant des données qui ont vocation à être traitées, les **principes applicables** sont les suivants :

- **principe de transparence** : les données doivent être traitées de manière loyale, licite et transparente ;

En pratique
Cela signifie que les données ne doivent être collectées, utilisées, consultées ou traitées qu'après communication aux personnes concernées d'une information complète sur le traitement, aisément accessible (par exemple : sur les formulaires de collecte, dans les documents contractuels, dans une politique « privacy » en ligne, etc.), facile à comprendre, et formulée en des termes clairs et simples[5].

- **principe de limitation des finalités** : les données ne doivent être collectées que pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ;

En pratique
Cela signifie que les données doivent être collectées pour une finalité précise et ne pas être réutilisées ultérieurement pour une finalité qui serait incompatible avec la finalité initiale prévue lors de la collecte.

[4] Seuls les principes généraux seront ici abordés. Les dispositions spécifiques applicables aux traitements de données particulières notamment (origines raciales ou ethniques, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques, données biométriques, données concernant la santé, données relatives à la vie sexuelle ou à l'orientation sexuelle, condamnations pénales / infractions / mesures de sûreté) seront abordées dans le cadre de la leçon 9.
[5] Sur le contenu de l'information à délivrer, voir leçon 3.

Afin de déterminer si le traitement ultérieur envisagé est ou non compatible avec la finalité initiale, il convient notamment de tenir compte des facteurs suivants : existence d'un lien entre les finalités initiale et ultérieure, contexte de la collecte, relation entre la personne concernée et le responsable de traitement, nature des données traitées, conséquences du traitement pour la personne concernée, existence de garanties appropriées à l'égard de cette dernière, attentes raisonnables de la personne concernée.
Pour une illustration, des données collectées et traitées par un établissement bancaire dans le cadre de son activité de tenue des comptes bancaires (par exemple, ensemble des informations disponibles sur un relevé de compte : typologie des retraits et des paiements, bénéficiaires, fréquence, etc.) ne peuvent être réutilisées pour effectuer des opérations de ciblage et de prospection sans précautions préalables sous peine de « détournement » de finalité. En revanche, les traitements ultérieurs à des fins archivistiques dans l'intérêt public, de recherche scientifique ou historique, ou de statistiques ne sont en principe pas considérés comme incompatibles avec les finalités initiales.

- **principe de minimisation des données** : les données traitées doivent être pertinentes, adéquates et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ;

En pratique
Cela signifie que les données à caractère personnel ne doivent être traitées que si la finalité du traitement ne peut pas être atteinte pas d'autres moyens. A titre d'illustration, une entreprise qui propose sur son site internet aux internautes de recevoir gratuitement un devis ou toute autre documentation, peut recueillir l'identité et les coordonnées du demandeur pour répondre à sa demande, mais ne doit en aucun cas collecter ses coordonnées bancaires même s'il s'agit uniquement d'anticiper des relations futures.

- **principe d'exactitude des données** : les données traitées doivent être exactes et mises à jour régulièrement (rectification, voire effacement) ;

En pratique
Cela signifie que des mesures raisonnables doivent être prises pour s'assurer que les données inexactes sont rectifiées ou effacées (par exemple : prise en compte effective et sans délai des demandes de rectification ou d'effacement[6], mise en place de processus permettant d'effectuer une revue régulière des données afin de déterminer si elles sont encore pertinentes ou au contraire devenues obsolètes, etc.).

- **principe de limitation de la conservation des données** : les données ne peuvent être conservées que pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;

En pratique
Cela signifie que la durée de conservation des données doit être limitée au strict minimum. Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais doivent notamment être fixés pour leur effacement ou leur examen périodique. Des aménagements peuvent

[6] Sur les droits des personnes concernées, voir leçon 3.

être prévus pour certaines données ou pour certaines finalités. D'un point de vue pragmatique, une véritable politique de conservation, d'archivage et de purge des données doit être formalisée.

- **principe de sécurité, d'intégrité et de confidentialité des données** : les données doivent être traitées de façon à garantir une sécurité appropriée desdites données au moyen de mesures techniques ou organisationnelles appropriées ;

En pratique
Cela nécessite que des mesures de sécurité soient prises, en particulier afin de protéger les données contre le traitement non autorisé ou illicite, la perte, la destruction, les dégâts d'origine accidentelle, la divulgation à des personnes non autorisées, etc.
La mise en œuvre de ces mesures doit notamment passer par la formalisation d'une politique de sécurité des données, d'actions de sensibilisation des membres du personnel, etc.[7]

En tout état de cause, le responsable de traitement doit être en mesure de démontrer le respect de ces principes. C'est **le principe d'accountability** qui désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes propres à permettre la protection des données à caractère personnel et d'être prêtes à démontrer qu'elles respectent le règlement.

En pratique
*Les entreprises vont devoir **agir** et être en mesure de **prouver**, de **tracer**, ce qui a été fait. Cela passera notamment par l'implémentation de documentations adaptées et de politiques de traitement des données écrites et contraignantes, ou encore de procédures de vérifications pour s'assurer de l'effectivité et de l'efficacité des mesures mises en œuvre pour le respect des dispositions applicables*[8].

2/ Principes concernant les traitements

Outre les principes applicables aux données, un traitement ne peut être mis en œuvre que s'il respecte le **principe de licéité**. Pour ce faire, il doit remplir au moins une des conditions alternatives suivantes :

- la personne concernée a consenti au traitement ;

En pratique
Si le consentement est le fondement du traitement, alors le responsable de traitement doit être en mesure de prouver que la personne concernée a effectivement consenti à l'opération de traitement.
Par ailleurs, le consentement doit être recueilli de manière éclairée (c'est-à-dire après information claire et complète de la personne concernée sur les caractéristiques et modalités du traitement) mais également librement (c'est-à-dire que la personne concernée doit disposer d'une véritable liberté de choix et être en mesure de refuser ou de retirer librement son consentement sans subir de préjudice). A titre d'illustration, le consentement ne peut être considéré comme libre et valable s'il existe un déséquilibre significatif entre la personne concernée et le responsable de traitement (par exemple, autorité publique, employeur, etc.).

[7] Sur les obligations en matière de sécurité et de confidentialité des données, voir leçon 6.
[8] Sur les obligations du responsable de traitement et la gouvernance Informatique et libertés (cf. principe d'accountability), voir leçon 4.

- le traitement est nécessaire à l'exécution d'un contrat ou de mesures précontractuelles ;

En pratique
La licéité du traitement ne peut être fondée sur cette exception que si la personne concernée est partie au contrat ou que les mesures précontractuelles sont prises à la demande de celle-ci. Par ailleurs, seule une connexion réelle et substantielle, un lien direct et objectif avec le contrat peut justifier que la licéité du traitement repose sur ce fondement.

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable de traitement est soumis ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont il est investi ;

En pratique
Le traitement doit avoir un fondement dans le droit de l'Union européenne ou dans le droit d'un Etat membre. Sur ce point, les Etats membres pourront d'ailleurs prévoir des dispositions visant à déterminer plus précisément les exigences spécifiques applicables à ces traitements (conditions du traitement, types de données pouvant être traitées, personnes concernées, destinataires pouvant se voir communiquer les données, durées de conservation, etc.).

- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

En pratique
Le traitement ne peut être fondé sur l'intérêt vital d'une personne que s'il est motivé par l'urgence de la situation médicale et qu'il est nécessaire à l'administration de soins correspondants : un diagnostic vital conditionné par le traitement doit être en cause. A contrario, ce fondement ne peut être utilisé par exemple si le traitement a uniquement pour finalité des recherches médicales d'ordre général qui ne porteraient leurs fruits que dans les années à venir.

- le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable de traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données ;

En pratique
L'existence d'un intérêt légitime doit faire l'objet d'une évaluation attentive : il convient de procéder au test de la ***balance des intérêts***[9]*.*
La question qui doit présider à la vérification de la validité de ce fondement est « l'intérêt légitime du responsable de traitement à mettre en œuvre le traitement prévaut-il sur l'intérêt de la personne concernée à ce que ses données ne soient pas traitées dans le cadre dudit traitement ? ».
Un faisceau d'indices et de critères doivent alors être analysés, tels que la réalité et la pertinence des intérêts en présence, la typologie et le volume de données traitées, les incidences négatives ou positives du traitement sur les personnes concernées, le nombre de personnes concernées ainsi que les attentes raisonnables de ces dernières, les modalités du traitement (partage des données, mutualisation,

[9] G29, Avis 6/2014 du 9-4-2014 sur la notion d'intérêt légitime du responsable de traitement.

sécurité, etc.), les garanties offertes aux personnes concernées (notamment chiffrement ou pseudonymisation), etc.
Si le règlement donne des exemples de finalités pouvant être considérées comme répondant à un intérêt légitime du responsable de traitement (telles que la prévention de la fraude, la prospection commerciale ou encore la sécurité du réseau et des informations), une analyse au cas par cas doit en tout état de cause être menée pour chaque traitement ayant vocation à être mis en œuvre du ce fondement.

* *
*

C'est donc une véritable politique « Informatique et libertés » qu'il convient de déployer pour mettre et maintenir ses traitements de données à caractère personnel en conformité avec le règlement.

En tout état de cause, l'analyse du respect de ces principes doit être un préalable à la mise en œuvre de chaque traitement de données : elle doit être intégrée dès l'origine dans les processus métiers et déployée pour chaque nouveau projet.

Mais une vérification de l'existant doit également être réalisée pour une conformité globale.

Rendez-vous aux prochaines leçons pour découvrir les autres subtilités du règlement.

Références textuelles
Considérants 39) à 50)
Articles 5, 6 et 7

Leçon 3 – Respecter les droits des personnes concernées

Lorsqu'une entité met en œuvre des traitements de données à caractère personnel, elle se doit de déployer les process appropriés pour respecter les droits des personnes concernées.

Petit décryptage pratique des principaux droits dont il convient de tenir compte et des mesures à mettre en place !

1/ Avant le traitement : informer les personnes concernées

Le RGPD prévoit que **les personnes concernées doivent être informées** du traitement de leurs données à caractère personnel et liste un ensemble d'informations devant leur être obligatoirement communiquées.

Les modalités et le contenu de cette information diffèrent en fonction de si la collecte de données a été effectuée directement auprès de la personne concernée ou de manière indirecte, par l'intermédiaire d'un tiers (par exemple, en cas de location de fichier).

Le tableau ci-dessous propose un récapitulatif synthétique de ces éléments :

<table>
<tr><th></th><th>Collecte directe</th><th>Collecte indirecte</th></tr>
<tr><td rowspan="12">Quelles informations ?</td><td colspan="2">Identité et coordonnées du responsable de traitement et de son représentant</td></tr>
<tr><td colspan="2">Coordonnées du délégué à la protection des données</td></tr>
<tr><td colspan="2">Finalités et fondement juridique du traitement</td></tr>
<tr><td>/</td><td>Catégories de données à caractère personnel concernées</td></tr>
<tr><td colspan="2">Intérêt légitime poursuivi par le responsable de traitement (si le traitement est fondé sur « l'intérêt légitime »[10])</td></tr>
<tr><td colspan="2">Existence du droit de retirer son consentement (lorsque le traitement est fondé sur un tel consentement)</td></tr>
<tr><td>Caractère règlementaire ou contractuel de l'exigence de la fourniture des données et conséquence de la non-fourniture de ces données</td><td>/</td></tr>
<tr><td colspan="2">Destinataires des données</td></tr>
<tr><td colspan="2">Existence de transferts de données hors Union européenne et référence aux garanties associées</td></tr>
<tr><td colspan="2">Durée de conservation des données</td></tr>
<tr><td colspan="2">Existence des droits d'accès, de rectification, d'effacement, de limitation et d'opposition au traitement et du droit à la portabilité</td></tr>
<tr><td colspan="2">Existence du droit d'introduire une réclamation auprès d'une autorité de contrôle (cf. Commission Nationale de l'Informatique et des Libertés, dite « CNIL », en France)</td></tr>
</table>

[10] Sur la licéité du traitement, voir leçon 2.

<table>
<tr><td rowspan="2"></td><td colspan="2">Existence d'une prise de décision automatisée (notamment profilage), ainsi que la logique, l'importance et les conséquences de ce traitement</td></tr>
<tr><td>/</td><td>Source d'où proviennent les données et mention indiquant qu'elles sont issues ou non de sources accessibles au public.</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>S'agissant de quels traitements ?</td><td colspan="2">Traitement initial et éventuel traitement ultérieur</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>Quand ?</td><td>Au moment où les données sont obtenues</td><td>Dans un délai raisonnable après avoir obtenu les données, et ne dépassant pas un mois.

Si les données doivent être utilisées à des fins de communication avec la personne concernée, au plus tard lors de la première communication.

S'il est envisagé de communiquer des informations à un autre destinataire, au plus tard lors de cette première communication.</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td rowspan="4">Comment ?</td><td colspan="2">Information concise, transparente, compréhensible, aisément accessible, en des termes clairs et simples
<u>Attention</u> : l'information sur le droit d'opposition doit en outre être portée à la connaissance de la personne concernée lors de la première communication avec cette dernière, et être présentée clairement et séparément de toute autre information.</td></tr>
<tr><td colspan="2">Information accompagnée d'icônes normalisées pour une meilleure vue d'ensemble (cf. voir les actes ultérieurs qui pourront être pris par la Commission sur ce point)</td></tr>
<tr><td colspan="2">Par écrit ou autre moyen approprié, notamment par voie électronique</td></tr>
<tr><td colspan="2">A l'oral si la personne concernée en fait la demande</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td rowspan="4">Hypothèses dans lesquelles l'obligation d'information ne s'applique pas ?</td><td colspan="2">Si la personne concernée dispose déjà de ces informations</td></tr>
<tr><td>/</td><td>Si la fourniture de ces informations se révèle impossible ou exige des efforts disproportionnés.
<u>Attention</u> : cette notion est interprétée de manière restrictive par les autorités de contrôle.</td></tr>
<tr><td>/</td><td>Si l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union européenne ou par le droit d'un Etat membre.</td></tr>
<tr><td>/</td><td>Si les données doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union européenne ou d'un Etat membre, y compris une obligation légale de secret professionnel.</td></tr>
</table>

Aussi, afin de s'assurer qu'une information exhaustive et conforme est bien (a bien été) communiquée à l'ensemble des personnes concernées, une **vérification** doit être effectuée :

- Comment sont collectées les données ?
- Par quel moyen ?
- Auprès de qui ?
- Une information figure-t-elle dans les documents ?
- Est-elle communiquée à l'ensemble des personnes concernées, quel que soit le mode de collecte des données ?
- Que contient cette information ?
- Etc.

Ces questions devront en tout état de cause se poser pour **tout nouveau projet** impliquant une collecte de données (ou une réutilisation de données préalablement obtenues) et une information des personnes concernées effectivement réalisée dans le respect des dispositions du règlement.

L'astuce : j'anticipe !

Pour aider les responsables de traitement dans cette tâche, il peut notamment être opportun de déployer, par anticipation, les actions suivantes :

***1/ Formaliser un process** imposant, pour tout nouveau projet nécessitant une collecte / utilisation de données à caractère personnel, de vérifier l'existence, les modalités et le contenu de l'information des personnes concernées ;*

***2/ Rédiger une bibliothèque de mentions d'information type**, qui tiendrait compte des divers types de traitement pouvant être mis en œuvre au sein de l'entité, des finalités poursuivies, des caractéristiques de ces traitements, des modalités de collecte des données, etc. afin de disposer de modèle harmonisés et réutilisables ;*

***3/Identifier les supports permettant de communiquer l'information aux personnes concernées**, étant précisé à titre d'exemple que les mentions obligatoires peuvent notamment figurer :*
- sur les formulaires de collecte de données (papier, en ligne) ;
- dans les documents contractuels (contrat avec les fournisseurs, contrat de travail, etc.) ;
- dans un livret de présentation de l'entité ou encore un livret d'accueil ;
- dans un courrier (papier ou électronique) dédié ;
- au sein de la « politique de protection des données » ou « privacy policy » d'un site web ;
- dans le script des téléconseillers (doublée par l'envoi d'un écrit) ;
- etc.

2/ Une fois le traitement mis en œuvre, répondre aux demandes des personnes concernées

Outre le droit à l'information, les personnes dont les données à caractère personnel font l'objet d'un traitement disposent du **droit de demander** au responsable de traitement d'effectuer certaines actions à leur profit.

Il s'agit des droits suivants :

- le ***droit d'accès*** à ses données par la personne concernée, c'est-à-dire le droit d'obtenir du responsable de traitement la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que, si elles le sont, l'accès auxdites données (communication d'une copie) et aux informations relatives aux caractéristiques du traitement (le règlement fixe la liste précise desdites informations) ;

- le ***droit d'obtenir la rectification*** des informations inexactes et que les données incomplètes soient complétées ;

- le ***droit d'obtenir l'effacement*** de ses données dans plusieurs hypothèses (énumérées par le RGPD), notamment lorsque les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées, si la personne concernée retire son consentement (et qu'il n'existe pas d'autre fondement au traitement), si la personne concernée exerce son droit d'opposition au traitement, si le traitement est illicite, etc. Il convient toutefois de garder à l'esprit que certaines exceptions à ce droit à l'effacement existent ;

- le ***droit à la limitation*** du traitement dans certaines hypothèses précisément visées par le règlement. A titre d'exemple, une telle limitation doit être mise en place lorsque l'exactitude des données est contestée par la personne concernée, pendant une durée permettant au responsable de traitement d'effectuer les vérifications adéquates. Il en est de même lorsque le responsable de traitement n'a plus besoin des données mais qu'elles sont encore nécessaires à la personne concernée pour la défense d'un droit en justice. Lorsqu'une telle limitation, par principe temporaire, est mise en place, alors les données ne peuvent être traitées, sauf pour leur conservation, qu'avec le consentement de la personne concernée ou pour des motifs spécifiques (défense d'un droit en justice, protection des droits d'une personne physique ou morale, motifs importants d'intérêt public de l'Union européenne ou d'un Etat membre). La personne concernée doit en tout état de cause être informée par le responsable de traitement avant que la limitation du traitement ne soit levée ;

- le ***droit à la portabilité*** : la personne concernée a le droit d'obtenir les données qu'elle a fournie à un responsable de traitement, dans un format structuré, couramment utilisé et lisible par machine, et a le droit de transmettre ces données à un autre responsable de traitement sans que le responsable de traitement initial ne puisse y faire obstacle. La personne concernée peut même demander que ces données soient transmises directement d'un responsable de traitement à l'autre lorsque cela est techniquement possible. Ce droit est toutefois subordonné au fait que (i) le traitement soit fondé sur le consentement ou sur un contrat et que (ii) le traitement est effectué à l'aide de procédés automatisés[11] ;

- le ***droit d'opposition*** : la personne concernée dispose, sous certaines conditions prévues par le règlement, d'un droit d'opposition au traitement qui lui permet de demander au responsable de traitement de ne plus traiter ses données et, en tout état de cause, d'un droit d'opposition à la prospection ;

[11] Sur le droit à la portabilité, voir les guidelines et FAQ du G29 adoptées le 13-12-2016.

- le ***droit de ne pas faire l'objet d'une décision*** fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative. Si ce droit est assorti d'exceptions, le responsable de traitement doit en tout état de cause, par principe, permettre à la personne concernée d'obtenir une intervention humaine pour l'analyse du traitement, d'exprimer son point de vue et de contester la décision.

L'astuce : j'évite les pièges !

Dans la mesure où il s'agit de droits dont bénéficie toute personne concernée, si les conditions sont remplies, le responsable de traitement doit bien entendu par principe accéder à la demande et procéder aux opérations nécessaires en résultant (communication d'informations, rectification, effacement, limitation, arrêt du traitement, etc.).

Mais attention, certaines demandes induisent des actions complémentaires :
- en cas de demande d'effacement, si le responsable de traitement a rendu publiques les données, il doit prendre les mesures raisonnables (compte tenu des technologies disponibles et des coûts de mise en œuvre) pour informer les responsables de traitement qui traitent ces données que la personne concernée a demandé l'effacement par ces derniers de toute copie ou de toute reproduction de ces données, ainsi que de tout lien vers lesdites données ;
- en cas de demande d'effacement, de rectification ou de limitation, le responsable de traitement doit notifier chaque destinataire cette demande (à moins qu'une telle notification se révèle impossible ou exige des efforts disproportionnés).

En cas de demande, une **<u>réponse</u>** doit par principe être apportée. Ci-après quelques pistes issues du règlement s'agissant des modalités de réponse à déployer :

Délais	Dans les meilleurs délais et en tout état de cause dans le délai d'**un mois** à compter de la réception de la demande. Possibilité de prolongation du délai dans certaines hypothèses mais nécessité d'informer la personne concernée. Si le responsable de traitement ne donne pas suite à la demande, nécessité d'informer la personne concernée dans un délai d'un mois des motifs du refus de réponse ainsi que de la possibilité pour cette dernière d'introduire une réclamation auprès d'une autorité de contrôle ou de former un recours juridictionnel.
Modalités	Information concise, transparente, compréhensible, aisément accessible, en des termes clairs et simples.
	Par écrit ou autre moyen approprié, notamment par voie électronique (à cet égard, si la demande est effectuée par voie électronique, alors la réponse est effectuée par voie électronique sauf demande contraire expresse de la personne concernée).
	A l'oral si la personne concernée en fait la demande, à condition que l'identité de la personne soit démontrée.
	<u>Attention</u>

	S'agissant du droit d'accès et du droit à la portabilité, l'exercice de ces droits et les réponses apportées ne doivent pas porter atteinte aux droits d'autrui. *Notamment, la copie des données communiquée à la personne concernée ne doit contenir que des données qui lui sont propres et aucune donnée sur des tiers, cette communication ne doit pas non plus porter atteinte au secret des affaires ou encore à la propriété intellectuelle d'un tiers.*
Paiement	Aucun paiement ne peut être exigé. Exception : - si les demandes sont manifestement infondées ou excessives (il appartient au responsable de traitement de le prouver), notamment en raison de leur caractère répétitif : possibilité de refuser de répondre ou d'exiger le paiement des frais administratifs supportés en conséquence. - pour le droit d'accès, le responsable de 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).

En tout état de cause, l'exercice de ces droits ainsi que les obligations en résultant pour les responsables de traitement sont chacun conditionnés à la réunion de divers critères et souffrent d'exceptions. Le droit de l'Union européenne ou de l'Etat membre pourront également limiter la portée de ces droits et obligations dans certaines hypothèses.

Aussi, chaque demande émanant d'une personne concernée doit faire l'objet d'une attention particulière afin de vérifier si les conditions requises sont réunies, de préparer les réponses appropriées, de procéder au déploiement des actions nécessaires, etc.

Et ce d'autant que l'absence de prise en compte et de réponse à ce type de demandes conduit fréquemment à l'introduction d'une réclamation ou d'un recours juridictionnel.

L'astuce : je formalise !

Il est recommandé de formaliser et de mettre en œuvre une procédure de gestion et de traitement des demandes d'exercice de leurs droits par les personnes concernées.

Cette procédure devra notamment intégrer les points suivants :

- identification des demandes (cf. procédure « courrier ») ;
- modalités de traitement des demandes (service ou cellule dédié(e) en charge de la réponse, délais, contenu, formalisme, destinataire, vérification de l'identité du demandeur et du bien-fondé de la demande, etc.) en tenant compte des spécificités de chaque droit et des conséquences et actions en résultant, des diverses typologies de personnes concernées, etc. ;
- vérification de la cohérence des mentions d'information s'agissant de ces droits ;
- élaboration d'une bibliothèque de courriers / réponses-types ;

- déploiement de fonctionnalités d'extraction, notamment pour les réponses aux demandes d'accès et de portabilité (cf. requêteur et formatage / paramétrage des réponses).

3/ Dans tous les cas, tenir compte de l'articulation entre le droit de l'Union européenne et le droit local des Etats membres

Si cette précision vaut pour l'ensemble des dispositions du règlement, elle trouve une résonnance encore plus particulière en matière de respect du droit des personnes concernées.

A titre d'exemple, en droit français, à ce jour, outre l'information « générale » devant d'ores et déjà être portée à la connaissance des personnes concernées s'agissant des caractéristiques du traitement préalablement à la mise en œuvre de celui-ci, une information spécifique (certes plus limitée que l'information « générale » précitée) doit figurer, en sus, **sur** tout questionnaire ou formulaire de collecte de données. Or, cette disposition pourrait éventuellement subsister en complément des dispositions précitées du RGPD.

De même, le règlement ne s'applique pas aux données à caractère personnel des personnes décédées, les Etats membres pouvant néanmoins prévoir des règles spécifiques relatives au traitement des données à caractère personnel des personnes décédées. Or, de telles règles sont prévues en droit français (à titre d'illustration, droit pour les personnes concernées de définir des directives générales et particulières pour le traitement de leurs données post-mortel notamment).

Par conséquent, il conviendra dans le cadre du déploiement par les responsables de traitements de leur procédure de gestion des droits des personnes, de tenir compte de l'ensemble de ces dispositions.

* *
*

Cette leçon vous a permis d'entrevoir un aperçu des obligations et process à déployer aux fins de mise en conformité s'agissant du respect des droits des personnes. Et ce n'est qu'un début !

Rendez-vous à la prochaine leçon pour découvrir d'autres obligations résultant du règlement et astuces pour s'y conformer !

Références textuelles
Considérants 27) et 58) à 73)
Articles 12 à 23

Leçon 4 – Comprendre l'*accountability* et déployer les mesures nécessaires à une véritable gouvernance des données

Un principe essentiel et primordial issu du règlement doit guider l'entité qui met en œuvre des traitements de données à caractère personnel : le principe d'accountability.

L'accountability désigne l'obligation pour les entreprises 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 règlement, et être en mesure de le démontrer.

Aussi, l'accountability implique la mise en place d'une véritable gouvernance des données, et notamment :

- **de déployer un processus permanent et dynamique de mise en conformité** de son entreprise à la réglementation « Informatique et libertés », notamment grâce à un ensemble de règles contraignantes, d'outils et de bonnes pratiques correspondantes ;

- **d'apporter la preuve que les mesures appropriées ont été prises** (cf. mécanisme permettant de démontrer l'efficacité et l'effectivité des mesures prises) : en pratique, les entreprises vont devoir faire et être en mesure de prouver, de tracer, ce qui a été fait ;

- **d'auditer les mesures prises dans le cadre d'un contrôle continu**, pour d'une part, vérifier l'efficacité desdites mesures et d'autre part, les actualiser le cas échéant pour assurer leur maintien en conformité au règlement au regard de l'évolution des traitements, de leurs finalités, des exigences réglementaires ou tout simplement du retour d'expérience.

Méthode d'évaluation du caractère approprié des mesures
Le caractère approprié des mesures prises doit être évalué, de manière objective, au regard de la nature, de la portée, du contexte et des finalités du traitement, ainsi que du degré de probabilité et de la gravité des risques encourues pour les droits et libertés des personnes physiques.

En tout état de cause, le respect du principe d'accountability doit se traduire par le déploiement de diverses mesures concrètes.

1/ Documentation et organisation générale « Informatique et libertés »

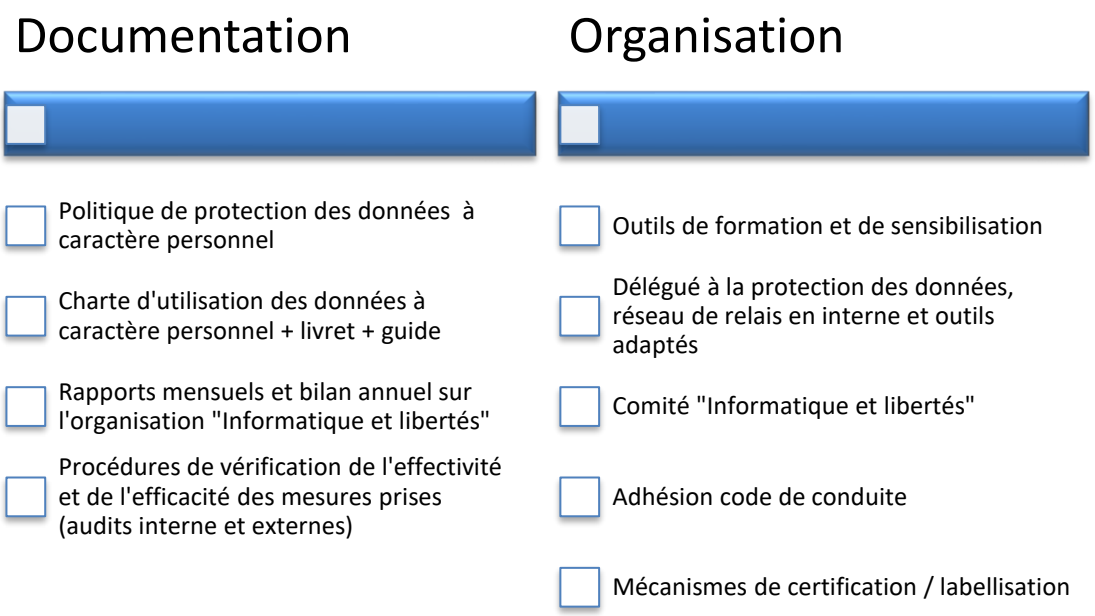
Il est indispensable de prévoir l'implémentation d'une **organisation** « Informatique et libertés » au sein de l'entreprise, de **documentations** adaptées et de politiques de traitement des données écrites et contraignantes, ou encore de procédures de vérification pour s'assurer de l'effectivité et de l'efficacité des mesures mises en œuvre.

A titre d'exemple, le RGPD fait notamment référence à la mise en œuvre de politiques en matière de protection des données par l'entité qui procède à la mise en œuvre de traitements de données à caractère personnel. Il est également renvoyé à la possibilité de faire application de codes de conduites ou de mécanismes de certifications.

Codes de conduite et certifications « approuvés »
Lorsqu'il est envisagé de se soumettre à un code de conduite ou à une certification, il est recommandé de choisir ceux « approuvés », c'est-à-dire « validés » par l'autorité de contrôle compétente, qui permettent selon le règlement de servir d'élément attestant du respect des obligations en matière de protection des données. En tout état de cause, quel que soit le mécanisme retenu, il convient de porter une attention particulière au respect des règles et principes qu'ils édictent dans la mesure où des vérifications peuvent être effectuées par l'autorité de contrôle, mais également par des organismes dédiés disposant d'un niveau d'expertise approprié ou par les organismes de certification.

Dans cette même optique, la désignation d'un délégué à la protection des données, outre le fait qu'elle devient avec le règlement obligatoire dans un certain nombre d'hypothèses, a aussi vocation à venir renforcer la gouvernance « Informatique et libertés » au sein des entreprises et à offrir un gage complémentaire de confiance s'agissant de la protection des données[12].

Les principaux éléments à prévoir peuvent donc être ainsi synthétisés :



[12] Sur le délégué à la protection des données, voir leçon 8.

2/ Privacy by design et privacy by default

La privacy by design et la privacy by default sont des concepts nouveaux introduits par le RGPD et qui participent à l'organisation et au respect de l'accountability.

La **privacy by design** consiste en la nécessité de prendre les mesures appropriées pour concrètement tenir compte de la protection des données dans les projets depuis leur origine, et de s'assurer de la conformité des produits et services proposés aux dispositions « Informatique et libertés » tout au long de leur cycle de vie.

L'objectif est d'anticiper les contraintes « Informatiques et libertés » lors de la détermination du traitement pour que ces contraintes soient intégrées de manière effective lors de la mise en œuvre du traitement.

Notamment, il est fortement recommandé de formaliser un cahier des charges traduisant les contraintes juridiques en matière de protection des données à caractère personnel (minimisation des données pouvant être traitées, durées proportionnées de conservation des données, limitation des personnes pouvant y accéder, etc.), en contraintes techniques devant être respectées, et qui serait impératif pour tout nouveau projet de programme informatique, de logiciel, d'application.

Les obligations résultant de ce principe de privacy by design peuvent se traduire ainsi :

La **privacy by default** consiste à prendre les mesures techniques et organisationnelles appropriées pour garantir que par défaut seules les données qui sont nécessaires au regard de la finalité spécifique du traitement sont collectées et utilisées.

En pratique
Ce principe s'applique en particulier à la quantité de données collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité, qui doivent par défaut être limitées au strict minimum au regard de la finalité du traitement.

3/ Le registre des activités

Toujours pour répondre à la contrainte d'accountability, les traitements mis en œuvre doivent être répertoriés dans un registre des activités de traitement.

Ce registre doit être mis à jour régulièrement, au fur et à mesure de la mise en œuvre de nouveaux traitements ou de la modification de traitements existants. Il doit être tenu sous forme écrite, y compris sous forme électronique. Il doit également être mis à disposition de l'autorité de contrôle en cas de demande de cette dernière.

Le piège à éviter
Le règlement prévoit que la tenue du registre n'est pas obligatoire pour les entités comptant moins de 250 salariés. La tentation serait grande pour les TPE/PME de s'en tenir à cette exception pour échapper à cette obligation. Toutefois, cette exception est réduite à peau de chagrin dans la mesure où elle ne s'applique pas si le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées, s'il porte notamment sur des données dites « particulières » ou relatives à des infractions ou condamnations pénales, ou encore s'il n'est pas occasionnel.
Aussi, tout traitement mis en œuvre qui présente une certaine pérennité (par opposition au caractère occasionnel visé dans le règlement) doit en tout état de cause faire l'objet d'une insertion dans un registre des activités de traitement, que l'entité compte plus ou moins de 250 salariés etc.

Les informations devant être contenues dans ce registre diffèrent en fonction qu'il s'agit du registre des activités de traitement d'un responsable de traitement ou d'un sous-traitant :

Responsable de traitement	Sous-traitant
Identité et coordonnées du responsable de traitement et de son représentant et du délégué à la protection des données	Identité et coordonnées du sous-traitant et de son représentant, de chaque responsable de traitement et de leur représentant, et du délégué à la protection des données
Finalités du traitement	Catégories de traitements
Catégories de personnes concernées	/
Catégories de données traitées	/
Catégories de destinataires des données	/
Existence de transferts de données hors Union européenne et référence aux garanties associées	
Durée de conservation des données	
Description générale des mesures de sécurité techniques et organisationnelles mises en œuvre	

Anticiper l'élaboration du registre
Afin d'élaborer un tel registre, il convient de procéder dès à présent à une démarche de mise en conformité incluant notamment les actions suivantes :
- cartographie et audit des traitements mis en œuvre au sein de l'entité ;
- réalisation d'une trame de registre ;
- définition d'une méthodologie interne pour la tenue du registre ;
- détermination de la (ou des) personne(s) en charge de la tenue du registre ;
- formalisation d'une « aide utilisateur » en vue de la rédaction du registre ;
- insertion de chaque traitement identifié dans le registre ;
- mise à jour régulière du registre.

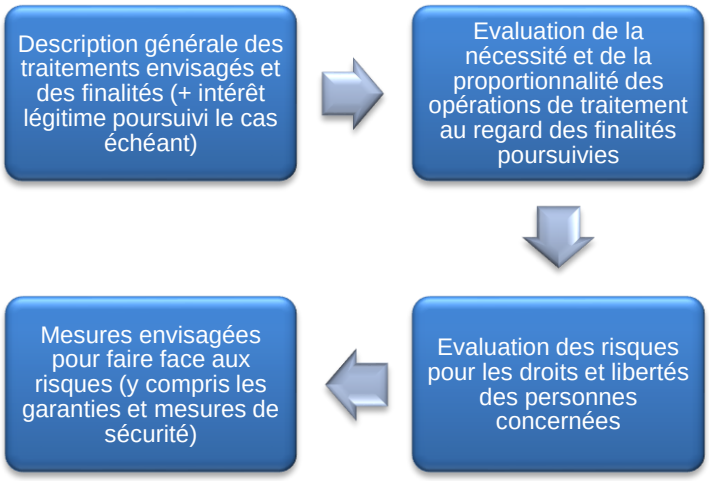
4/ L'analyse d'impact

Enfin, le règlement prévoit que lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes, alors une analyse d'impact des opérations de traitement sur la protection des données à caractère personnel doit être effectuée afin de déterminer les mesures appropriées à prendre afin de démontrer que le traitement des données respecte le règlement.

Le règlement liste également certains traitements soumis d'office à une telle analyse d'impact et les autorités de contrôle seront amenées à publier une liste des types d'opérations qui devront également y être soumises. Les traitements concernés pourraient donc être synthétisés comme suit :

Traitements concernés		
Traitements présentant des risques particuliers du fait de leur nature, de leur portée, de leur contexte ou de leurs finalités	Traitements présentant des risques particuliers selon le règlement (exemple, traitement d'informations dites "particulières" ou relatives à des infractions ou condamnations pénales, évaluations automatisées, systématiques et approfondies d'aspects personnels en vue de prendre une décision produisant des effets juridiques, surveillances systématiques à grande échelle d'une zone accessible au public)	Traitements considérés par l'autorité de contrôle comme étant susceptibles de présenter des risques spécifiques pour les droits et libertés des personnes concernées

Le règlement prévoit également ce que doit contenir une étude d'impact. Il s'agit *a minima* des points suivants :



Attention, si l'analyse conclut au fait que le traitement présente un risque élevé pour les droits et libertés des personnes, si le responsable ne prend pas de mesures pour atténuer le risque, alors une consultation préalable de l'autorité de contrôle est nécessaire.

Formaliser l'analyse d'impact
Il convient de formaliser un process visant à :
- analyser pour chaque traitement, avant sa mise en œuvre, ou avant toute modification, pour déterminer si une étude d'impact est nécessaire ;
- déterminer les modalités de l'analyse d'impact ;
- élaborer une procédure ou une méthode pour la réalisation de cette analyse d'impact, ainsi qu'une trame d'analyse associée ;
- déterminer les conséquences induites par cette analyse, en fonction du résultat obtenu, et prendre les mesures adaptées.

* *
*

L'accountability est sans conteste la clé de voûte du RGPD en ce qu'un nombre important de contraintes en résultent. Ces contraintes doivent dès à présent être anticipées afin que l'ensemble des mesures appropriées soient déployées et effectives au moment de l'entrée en application du règlement.

Mais de nombreux autres processus doivent être mis en œuvre ou ajustés afin de se conformer à l'ensemble des dispositions du règlement. Rendez-vous aux prochaines leçons pour les découvrir…

Références textuelles
Considérants 74 à 78, 82 à 84, 89 à 96 et 98 à 100
Articles 24, 25, 30, 35, 36 et 40 à 43

Leçon 5 – Organiser les relations entre les acteurs du traitement

Plusieurs acteurs peuvent intervenir dans la mise en œuvre d'un traitement de données à caractère personnel, principalement le (ou les) responsable(s) de traitements et le (ou les) sous-traitant(s).

Or, le RGPD prévoit que les relations entre ces acteurs doivent être encadrées, l'objectif avoué de ce texte étant une répartition claire des rôles et responsabilités en matière de protection des données à caractère personnel.

1/ Les relations entre les responsables de traitements

Plusieurs responsables de traitements peuvent intervenir dans le cadre d'un traitement de données à caractère personnel. En effet, le règlement prévoit l'hypothèse dans laquelle plusieurs responsables déterminent conjointement les finalités et les moyens du traitement : ils sont alors désignés comme « **responsables conjoints** du traitement ».

Or, la probabilité de voir de multiples acteurs participer à un traitement de données à caractère personnel est à ce jour naturellement liée à la multiplicité et à la complexité des activités qui peuvent constituer un traitement. Il s'agit donc de tenir compte de la possibilité que différents acteurs participent à la détermination de plusieurs opérations ou ensembles d'opérations appliquées à des données à caractère personnel au sein d'un même traitement. Ces opérations peuvent se dérouler simultanément ou en différentes étapes

Dans un environnement aussi complexe que notre environnement actuel, il importe que les rôles et les responsabilités puissent facilement être attribués, pour éviter que les complexités de la responsabilité conjointe n'aboutissent à un partage des responsabilités impossible à mettre en œuvre, qui compromettrait l'efficacité de la règlementation sur la protection des données.

Notion de « responsables conjoints »

Il n'est pas nécessaire que les responsables de traitements participent de façon égale à la détermination des finalités et moyens du traitement pour être considérés comme responsables conjoints du traitement : la participation des parties à la détermination conjointe d'un traitement peut revêtir différentes formes et n'est pas nécessairement partagée de façon égale. En effet, lorsqu'il y a pluralité d'acteurs, ils peuvent entretenir une relation très proche (en partageant, par exemple, l'ensemble des finalités et des moyens d'une opération de traitement) ou, au contraire, plus distante (en ne partageant que les finalités ou les moyens, ou une partie de ceux-ci). Dès lors, l'éventail de typologies de responsables conjoints est particulièrement large.

Attention : le simple fait que différents acteurs coopèrent dans le traitement de données à caractère personne ne signifie pas nécessairement qu'ils sont responsables conjoints.
En effet, un échange de données entre deux parties, sans partage des finalités ou des moyens dans un ensemble commun d'opérations, doit être considéré uniquement comme un transfert de données entre des responsables distincts.

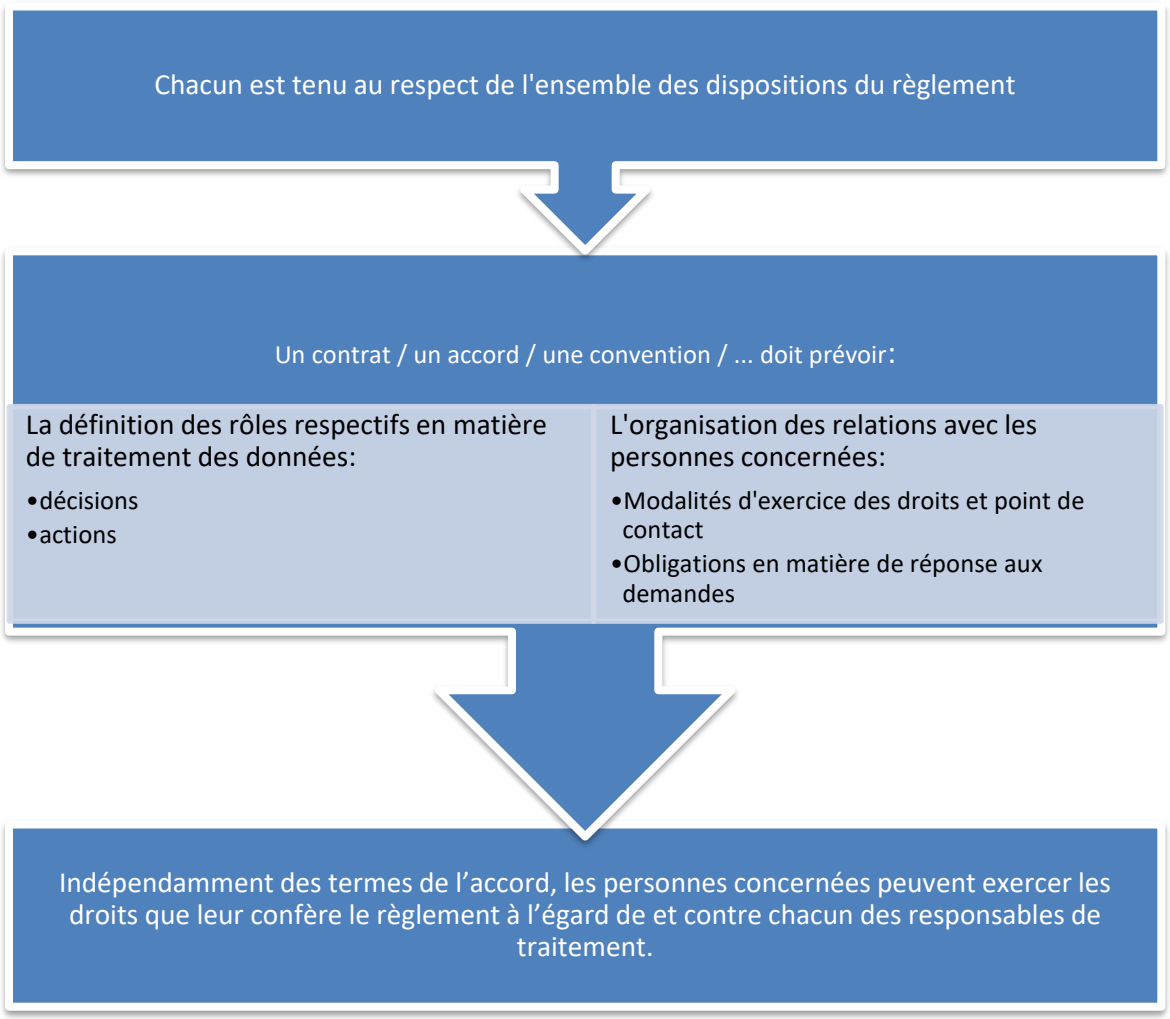
Il pourrait également s'agir d'opérations successives sur les données mais qui ne poursuivraient pas la même finalité d'un point de vue global. Une analyse au cas par cas doit donc être effectuée pour chaque situation qui pourrait éventuellement relever d'une responsabilité conjointe afin de déterminer les rôles de chacun et d'adapter leurs relations en conséquence.

Dans une hypothèse de responsabilité conjointe, le règlement prévoit que les obligations respectives des responsables conjoints de traitements en matière de protection des données doivent être définies de manière transparente par voie d'accord entre ces derniers, sauf si lesdites obligations respectives sont définies par le droit de l'Union européenne ou par le droit de l'Etat membre.

Il s'agit donc de **contractualiser les relations** entre les responsables conjoints de traitements, notamment s'agissant de leurs rôles respectifs et de leurs relations vis-à-vis des personnes concernées.

Toutefois, en tout état de cause, et indépendamment des termes contractuels, chaque responsable conjoint demeure **tenu au respect de l'ensemble des dispositions** du règlement, et les personnes concernées doivent pouvoir exercer leurs droits à l'égard de, et contre, chacun d'entre eux.

Schématiquement, l'organisation des relations entre les responsables conjoints de traitements peuvent être résumée comme suit :



2/ Les relations entre le responsable de traitement et le sous-traitant

Lorsqu'un responsable de traitement a recours à un sous-traitant pour la réalisation d'un traitement de données à caractère personnel, des précautions doivent également être prises et les relations entre ces acteurs encadrées.

Dans un premier temps, le responsable de traitement doit s'assurer que le sous-traitant auquel il a recours présente les **garanties nécessaires et suffisantes** s'agissant de la mise en œuvre de mesures techniques et organisationnelles appropriées pour répondre aux exigences du règlement et garantir la protection des droits des personnes concernées.

L'astuce : le cahier des charges « Informatique et libertés »
Le respect de cette exigence peut opportunément passer par la rédaction d'un cahier des charges ad hoc en matière de protection des données en vue du recrutement d'un sous-traitant.
Par ailleurs, l'application par le sous-traitant d'un code de conduite ou d'un mécanisme de certification approuvé peut servir à attester des obligations incombant au responsable de traitement dans le choix du sous-traitant.

Dans un second temps, **les relations entre le responsable de traitement et le sous-traitant doivent être contractualisées** sous forme écrite, le format électronique étant considéré comme valable. Le règlement liste les éléments devant obligatoirement figurer dans le contrat ou l'acte juridique liant ces acteurs, à savoir[13] :

[13] Sur la sécurité et la confidentialité des données, voir leçon 6.

Enfin, le responsable de traitement comme le sous-traitant est **responsable à l'égard des personnes concernées** de la réparation du préjudice éventuellement subi par ces dernières : toute personne ayant subi un dommage matériel ou moral du fait d'une violation du règlement peut en obtenir réparation en totalité auprès du responsable de traitement ou du sous-traitant, l'objectif étant que la personne concernée puisse obtenir une réparation complète et effective.

Néanmoins, si vis-à-vis de la personne concernée, le responsable de traitement et le sous-traitant peuvent, tant l'un que l'autre, être attraits en justice pour la réparation d'un préjudice subi, le partage des responsabilités dans les relations entre le responsable de traitement et le sous-traitant est réglé par le règlement.

Ce partage de responsabilités peut se résumer ainsi :

Requalification du sous-traitant en responsable de traitement
Il convient de préciser à toutes fins utiles que le sous-traitant qui viendrait à déterminer les finalités et moyens d'un traitement serait alors considéré comme responsable de traitement et devrait répondre de l'ensemble des obligations et responsabilités qu'implique cette qualification.

* *
*

Il résulte de ce qui précède qu'en cas de pluralité d'acteurs intervenant dans le cadre d'un traitement de données à caractère personnel, situation qui tend à devenir majoritaire, alors les relations entre ces acteurs doivent faire l'objet d'une attention particulière, et en tout état de cause être contractualisées.

Des process en vue de s'assurer du respect de ces contraintes doivent donc être formalisés.

En pratique
La gestion des relations entre les acteurs d'un traitement implique :
- d'élaborer, pour l'avenir, des modèles de clauses contractuelles ou des contrats types à conclure entre les différents acteurs (ou utiliser les conventions types qui pourront éventuellement à terme être rédigées par la Commission européenne ou les autorités nationales de contrôle s'agissant des relations avec les sous-traitants) ;
- de formaliser dans les processus de contractualisation l'obligation de vérifier la nécessité d'intégrer une telle clause ou de procéder au moyen d'un document contractuel dédié ;
- d'effectuer une revue des contrats existants pour vérifier si les stipulations obligatoires y figurent et, à défaut, les intégrer par voie d'avenant ou lors du renouvellement du contrat ;
- de formaliser des procédures d'échanges et de remontées d'information aux fins de respect des obligations respectives imposées aux acteurs dans le cadre des relations entre un responsable de traitement et un sous-traitant (ex : information sur le recours ou le changement de sous-traitant « ultérieur », demande d'aide pour la réalisation d'une étude d'impact ou la réponse à une demande d'une personne concernée, etc.) ou dans le cadre des relations entre deux responsables de traitement (ex : réponse aux demandes d'exercice de leurs droits par les personnes concernées).

Rendez-vous à la prochaine leçon pour approfondir les obligations de ces acteurs en termes de sécurité et de confidentialité des données…

Références textuelles
Considérants 79 à 81 et 146
Articles 26, 28, 29 et 82

Leçon 6 – Déployer les mesures de sécurité et de confidentialité adéquates

La sécurité est sans aucun doute une composante majeure du RGPD. En effet, si une section du règlement est spécifiquement dédiée à cette thématique, la sécurité des données se retrouve en filigrane dans l'ensemble des dispositions applicables et sous-tend l'ensemble des obligations applicables en matière de protection des données à caractère personnel.

La présentation des obligations en résultant nécessite de se pencher sur les obligations générales en matière de sécurité puis sur les éléments spécifiques liés à la gestion des failles de sécurité.

1/ L'obligation générale de sécurité

Le règlement prévoit que le responsable de traitement et le sous-traitant doivent, compte tenu de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du traitement, ainsi que du degré de probabilité et de gravité des risques associés pour les droits et libertés des personnes, mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un **niveau de sécurité adapté**.

Il résulte de cette disposition que des mesures doivent être prises, tant par le responsable de traitement que par le sous-traitant, pour assurer de manière effective la sécurité des données à caractère personnel traitées.

Le respect de cette obligation de sécurité doit se traduire, concrètement, par la mise en place des actions suivantes :

- une **méthode d'évaluation des risques** d'atteinte aux données (pour chaque traitement, en fonction de leur vraisemblance et de leur gravité) ainsi que de l'impact sur les droits et libertés des personnes concernées ;

En pratique
Lors de l'évaluation du niveau de sécurité approprié, il doit être tenu compte des risques pouvant notamment résulter de la destruction, de la perte, de l'altération, de la divulgation non autorisée des données à caractère personnel, ou encore de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

- une **politique de sécurité des données** adaptée au niveau de risque identifié, notamment en termes de confidentialité, d'intégrité, de disponibilité et de résilience des systèmes d'information et des services de traitement.

En pratique

Si une politique générale de sécurité des systèmes d'information existe habituellement au sein de toute entreprise, il est recommandé de formaliser également une politique de sécurité dédiée à la protection des données à caractère personnel dans la mesure où les éléments devant y être prévus présentent une certaine spécificité.

A titre d'exemple, les mesures suivantes doivent être prévues dans la politique de sécurité « données personnelles » et faire l'objet d'une attention particulière : méthode d'identification et d'authentification des utilisateurs, gestion des habilitations, sensibilisation et formation des utilisateurs (cf. risque d'ingénierie sociale), traçabilité et journalisation des accès et actions sur les données, sécurisation des postes de travail et de l'informatique mobile et nomade, plans de continuation / de reprise d'activité et/ou plan de secours informatique, gestion des incidents, sécurisation des locaux, du réseau interne, des serveurs et des applications, sécurisation des échanges avec les tiers, chiffrement, anonymisation ou pseudonymisation des données le cas échéant, archivage et sauvegarde sécurisés, lutte contre la vulnérabilité des canaux informatiques (surveillance de l'activité du réseau, interdiction de toute communication directe entre des postes internes et l'extérieur, cloisonnement des réseaux en sous-réseaux, interdiction de raccordement d'équipements informatiques non maîtrisés, etc.), mais également des canaux « papiers », mise à jour des logiciels et anti-virus, etc.

Par ailleurs, l'application d'un code de conduite ou d'un mécanisme de certification approuvé peut servir d'élément attestant du respect des exigences de sécurité.

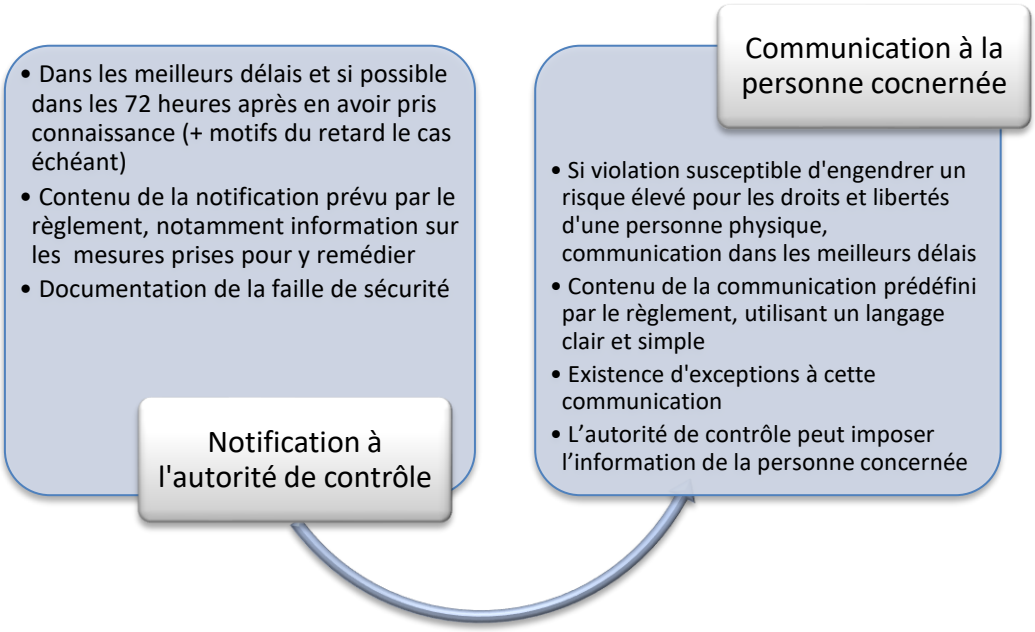
Enfin, une procédure visant à tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles prises pour la sécurité des traitements doit également être déployée. Elle doit être réalisée en concertation par des auditeurs techniques et juridiques. Une telle procédure d'audit de sécurité doit également être déployée auprès des sous-traitants par les responsables de traitement.

2/ La gestion des failles de sécurité

Outre les obligations générales de sécurité applicables à tout responsable de traitement ou sous-traitant, le règlement impose que les violations de données à caractère personnel, à savoir les failles de sécurité en matière de données, fassent l'objet d'une gestion particulière.

En effet, en cas de faille de sécurité affectant des données à caractère personnel, le responsable de traitement doit mettre en œuvre un process spécifique.

Ce process est le suivant :



Cette procédure de gestion des failles de sécurité ne s'impose pas en tant que telle au sous-traitant mais ce dernier se voit tout de même contraint de notifier toute violation de données au responsable de traitement dans les meilleurs délais après en avoir pris connaissance.

En pratique

Afin de répondre aux exigences imposées en matière de gestion des failles de sécurité, il est recommandé de mettre en place les mesures suivantes :

1/ formaliser une procédure de gestion des failles de sécurité décrivant les grandes étapes de la gestion d'une faille de sécurité, à savoir : identification et correction « technique » de la faille, constitution d'un dossier de preuves techniques et juridiques, dépôt de plainte, déclaration de sinistre auprès de l'assurance, notification à l'autorité de contrôle et communication à la personne concernée le cas échéant, communication « publique » de type « communiqué de presse » éventuellement ;

2/ rédiger des modèles-types : notification à l'autorité de contrôle, communication à la personne concernée, communiqué de presse, etc. ;

2/ élaborer un registre documenté des failles de sécurité, assorti de retours d'expérience constructifs.

* *
*

Cette leçon vient donc démontrer l'importance de la sécurité en matière de protection des données à caractère personnel.

Toutefois, il convient de préciser que les éléments présentés dans cette leçon ne tiennent compte que des aspects « Informatique et libertés ».

Toutefois, d'autres obligations peuvent être applicables en matière de sécurité et de failles de sécurité, notamment celles issues de la directive « Network Security and Information », dite directive NIS[14], qui impose par exemple à certains acteurs la mise en place de mesures préventives d'ordre technique et opérationnel pour la détection des risques concernant la sécurité du réseau informatique, le déploiement de mesures de gestion de ces risques, mais également une obligation de déclaration de certaines failles de sécurité (piratage, intrusion, etc.) aux autorités compétentes (cf. en France, l'Agence nationale pour la sécurité des systèmes d'information, dite ANSSI).

En tout état de cause, rendez-vous à la prochaine leçon pour découvrir d'autres subtilités du règlement…

Références textuelles
Considérants 85 à 88
Articles 32 à 34

[14] Directive 2016/1148/UE du 6-7-2016 concernant les mesures destinées à assurer un niveau élevé de sécurité des réseaux et des systèmes d'information dans l'Union.

Leçon 7 – Désigner un délégué à la protection des données

Le RGPD donne une place primordiale à un nouvel acteur en matière de protection des données à caractère personnel : le Délégué à la protection des données (ou DPD), plus couramment désigné en anglais sous le terme de Data protection officer (ou DPO)[15].

La création de ce « remplaçant » du Correspondant Informatique et libertés est l'occasion de faire le point sur l'opportunité d'une telle désignation.

1/ La désignation d'un DPO est-elle obligatoire pour mon entité ?

Il convient de préciser que la désignation d'un DPO sera **obligatoire**, tant pour les responsables de traitements que pour les sous-traitants, dans un certain nombre d'hypothèses, à savoir :

- s'ils appartiennent au secteur public ;
- si leur activité principale les amène à réaliser un suivi régulier et systématique des personnes à grande échelle ;
- si leur activité principale les amène à traiter (toujours à grande échelle) des données dites « particulières » ou relatives à des condamnations pénales ou à des infractions.

Dans les autres cas, la désignation d'un DPO demeure facultative, sauf si le droit de l'Union européenne ou d'un Etat membre l'exige.

Bon à savoir : risque d'interprétation extensive des hypothèses de désignation obligatoire

Les hypothèses dans lesquelles la désignation d'un DPO est obligatoire sont rédigées en des termes assez larges et susceptibles d'interprétation : quid notamment de la notion de suivi « régulier et systématique » des personnes concernées, ou encore de la quantification de « à grande échelle » ? Aussi, chaque entité doit mener une analyse concrète, au regard des traitements qu'elle met en œuvre, des finalités poursuivies, des catégories de données traitées, du nombre de personnes concernées, etc. afin de déterminer si elle est contrainte de désigner un DPO.

[15] Sur le DPO ; voir également les guidelines et FAQ du G29 adoptées le 13-12-2016.

Or, il y a fort à parier que cette obligation risque d'être interprétée de manière extensive par les autorités de contrôle, et ce d'autant que l'objectif avoué du règlement est d'encourager la désignation d'un DPO, même lorsqu'une telle désignation n'est pas obligatoire… C'est d'ailleurs ce qui semble ressortir des premières recommandations du G29 en la matière.

En tout état de cause, la désignation d'un DPO est recommandée, tant au regard du principe de prudence qu'au regard du principe d'accountability[16], une telle désignation ayant notamment vocation à permettre un renforcement de la gouvernance « Informatique et libertés », à procurer un gage de conformité et de confiance, voire un avantage concurrentiel à l'entité concernée.

2/ Qui peut être désigné en qualité de DPO ?

La désignation du DPO se fait sur la base de ses **qualités professionnelles** : en pratique, ce dernier doit disposer de connaissances spécialisées du droit mais également des pratiques en matière de protection des données.

Le **profil idéal** : un profil juridique disposant de solides connaissances techniques (juriste ou avocat spécialisé en droit des nouvelles technologies et de la protection des données), ou inversement un profil technique pouvant justifier d'une formation juridique en matière de protection des données, étant précisé que le niveau de connaissances spécialisées requis doit être évalué au regard des spécificités, de la sensibilité et de la complexité des opérations de traitement (ex : sensibilité des typologies de données traitées, complexité des flux et échanges de données, etc.). En pratique, un profil de type « risk manager » peut également être une piste intéressante. Le DPO doit également avoir une bonne connaissance de l'entreprise et de son secteur d'activité.

En tout état de cause, rien n'empêche le DPO de se faire assister dans sa mission par d'autres professionnels qualifiés venant compléter ses propres connaissances.

Bon à savoir : DPO interne ? Externe ? Mutualisé ?
Le DPO peut être un membre du personnel du responsable de traitement ou du sous-traitant. Toutefois, le règlement laisse la possibilité aux organismes de désigner un DPO externe, qui exerce alors ses missions non pas sur la base d'un contrat de travail mais sur la base d'un contrat de prestation de services. Par ailleurs, le règlement prévoit plusieurs hypothèses dans lesquels un DPO mutualisé peut être désigné, à savoir au sein d'un groupe d'entreprises, ou entre plusieurs autorités / organismes publics (au regard de leur structure organisationnelle et de leur taille).
Autant de possibilités qui visent à répondre au mieux aux besoins des organismes mettant en œuvre des traitements de données pour encourager la désignation d'un DPO.

3/ Une organisation spécifique est-elle nécessaire s'agissant de la fonction de DPO ?

Le DPO doit être **associé à toutes les questions relatives à la protection des données** à caractère personnel, d'une manière appropriée et en temps utile : le responsable du traitement ou le sous-traitant ayant procédé à une telle désignation doit y veiller !!

[16] Sur le principe d'accountability, voir leçon 4.

A cette fin, le DPO doit notamment :

- disposer des ressources nécessaires à l'exercice de sa mission ;
- avoir accès aux données et aux opérations de traitement ;
- disposer de la possibilité d'entretenir ses connaissances spécialisées en matière de protection des données.

En outre, il convient de préciser que la fonction de DPO est régie par les principes essentiels suivants :

- l'indépendance : il ne reçoit aucune instruction dans l'exercice de sa mission, il ne peut être pénalisé ou relevé de ses fonctions à ce titre, et il fait directement rapport au niveau le plus élevé de la direction de l'organisme ayant procédé à sa désignation ;

- l'absence de conflit d'intérêt, notamment lorsque le DPO exerce d'autres missions ou tâches au sein de l'entité, ou en raison de son rattachement hiérarchique ;

- la confidentialité : le DPO est soumis au secret professionnel ou à une obligation de confidentialité pour ce qui relève de l'exercice de sa mission.

Bon à savoir : organiser la fonction de DPO
La désignation d'un DPO n'est pas purement formelle. En effet, elle doit être accompagnée de la mise en œuvre d'une organisation spécifique lui permettant d'exercer de manière effective et efficace ses missions. Cela passe notamment par la mise à disposition de ce dernier de moyens techniques, financiers, humains et organisationnels pour mener à bien ses missions, la formalisation d'un processus de remontées d'informations en interne sur les opérations de traitement réalisées afin qu'il puisse y être associé dès l'origine (ex : relais du DPO, comité Informatique et libertés, etc.), la possibilité pour ce dernier de bénéficier d'heures de formation continue en matière de protection des données, la définition d'une position hiérarchique et fonctionnelle adaptée au sein de l'entité, etc.

4/ Et au quotidien, quelles sont les missions exactes du DPO ?

Le DPO est un élément-clé de la gouvernance « Informatique et libertés » au sein d'une entité. Du fait de ses connaissances spécialisées, il a vocation à **diffuser une « culture Informatique et libertés »** auprès des différents protagonistes et à **superviser la conformité** des traitements à la règlementation associée.

A cette fin, le règlement prévoit que les missions du DPO sont *a minima* les suivantes :

- il informe et conseille les membres de l'entité ayant procédé à sa désignation s'agissant des obligations leur incombant en matière de protection des données ;
- il contrôle le respect du règlement et des autres dispositions « Informatique et libertés » applicables ;
- il est impliqué dans le process d'analyse d'impact et en vérifie l'exécution ;
- il coopère avec l'autorité de contrôle ;

- il fait office de point de contact pour l'autorité de contrôle mais également pour les personnes concernées, ces dernières pouvant le saisir de toute question relative au traitement de leurs données et à l'exercice de leurs droits[17].

Toutefois, de nombreuses missions complémentaires en matière de protection des données peuvent lui être confiées. Pour des raisons de cohérence et pour une meilleure vision globale de cette thématique au sein de l'entreprise, il est d'ailleurs recommandé de centraliser l'ensemble des aspects « Informatique et libertés » auprès de cet unique acteur, du moins s'agissant de la supervision de ces aspects.

Bon à savoir : formaliser les missions du DPO

Le rôle du DPO doit être formalisé dans une lettre de mission ou a minima dans une fiche de poste détaillée dans la mesure où elle est fondamentalement transverse et peut, outre les missions expressément prévues par le règlement, recouvrir divers aspects complémentaires.

En pratique, le DPO devrait principalement être amené à intervenir :
- en amont de la mise en œuvre d'un nouveau traitement pour identifier l'ensemble des actions à déployer pour que ce traitement soit mis en œuvre conformément aux dispositions légales et réglementaires applicables (respect des principes de licéité, de limitation des finalités, de transparence et d'information des personnes concernées, de minimisation des données, de limitation de la conservation[18], vérification de l'adéquation des mesures de sécurité, etc.) ;
- dans le cycle de vie des traitements, notamment en procédant à la définition de mécanismes de vérification de la conformité ou encore à des audits pour contrôler le respect des obligations « Informatique et libertés » associées ;
- pour sensibiliser les acteurs pouvant être amenés à traiter des données à caractère personnel, notamment au moyen de l'élaboration d'une politique SIF (sensibilisation – information – formation) dédiée à la thématique « Informatique et libertés (ex : newsletter du DPO, page intranet dédiée, sessions de formation et e-learning, procédures internes, etc.) ;
- pour échanger avec l'autorité de contrôle, voire répondre aux demandes de cette dernière le cas échéant, notamment dans le cadre des consultations (obligatoires ou non) ;
- pour répondre aux questions, réclamations ou demandes d'exercice de leurs droits par les personnes concernées ;
- dans le cadre d'autres missions pouvant utilement être mises à sa charge telles que la tenue du registre des traitements, le maintien d'une documentation « Informatique et libertés » dédiée ou encore la réalisation de bilans ou de rapports réguliers s'agissant de son activité, etc.

* *
*

La nécessité ou l'opportunité de désigner un DPO ne doit donc pas être négligée, et ce d'autant que, même dans les hypothèses où une telle désignation n'est pas obligatoire, elle ne peut être que bénéfique pour l'entité concernée : en effet, désigner un DPO constitue un élément primordial en matière de **gouvernance** « Informatique et libertés » et d'***accountability.***

[17] Sur les droits des personnes concernées, voir leçon 3.
[18] Pour un développement plus précis concernant ces principes, voir leçon 2.

Le fait de ne pas disposer des compétences ou des ressources nécessaires en interne n'est en outre pas bloquant : un DPO externe pouvant être désigné, cette solution peut être une alternative intéressante en vue de la mise et du maintien en conformité « Informatique et libertés » tout en permettant une certaine souplesse.

La suite du décryptage du règlement aux prochaines leçons…

Références textuelles
Considérant 97
Articles 37 à 39

Leçon 8 – Encadrer les transferts de données hors Union européenne

Les flux de données à caractère personnel à destination et en provenance de pays en dehors de l'Union européenne ou d'organisations internationales sont nécessaires, notamment au développement du commerce international et de la coopération internationale.

Cependant, il importe que lorsque des données font l'objet de tels transferts, le niveau de protection des données des personnes physiques ne soit pas compromis.

C'est pourquoi, selon les termes du RGPD, les transferts de données vers des Etats non membres de l'Union européenne ou vers une organisation internationale ne peuvent être réalisés que s'ils répondent à des conditions particulières visant à s'assurer que des garanties appropriées sont mises en œuvre pour garantir les droits et libertés des personnes ainsi que la protection de leurs données à caractère personnel.

Avant de présenter les conditions de la licéité de tels flux de données, il est proposé de revenir sur la notion de transfert de données à caractère personnel.

1/ Notion de transferts de données hors Union européenne

Le règlement européen vise les transferts, vers un pays tiers à l'Union européenne ou une organisation internationale, de données qui font ou sont destinées à faire l'objet d'un traitement après ce transfert. Compte tenu de la notion particulièrement large que recouvre le terme « traitement », la simple consultation pouvant être constitutive d'un traitement, il semble possible de considérer que tout transfert de données hors Union européenne doit respecter les conditions posées par le règlement.

Mais ***que recouvre la notion de « transfert » ?***

Cette notion n'est pas définie par un texte mais a fait l'objet de diverses définitions par la CNIL qui peuvent être reprises à titre informatif :

- « *Constitue un transfert de données vers un pays tiers toute communication, copie ou déplacement de données par l'intermédiaire d'un réseau, ou toute communication, copie ou déplacement de ces données d'un support à un autre, quel que soit le type de ce support, dans la mesure où les données ont vocation à faire l'objet d'un traitement dans le pays destinataire*[19] »;

[19] CNIL, Guide « Transferts de données à caractère personnel vers des pays non membres de l'Union européenne », éd.2008.

- « *On parle de transfert de données personnelles lorsque les données personnelles sont transférées depuis le territoire européen vers un ou des pays situés hors de l'Union européenne. Le transfert peut s'effectuer, par copie, par déplacement de données, par l'intermédiaire d'un réseau ou d'un support à un autre (ex. d'un disque dur d'ordinateur à un serveur)*[20] » ;

- « *On parle de transfert de données à caractère personnel lorsque ces données sont transférées depuis le territoire européen vers un ou des pays qui n'appliquent pas les dispositions de la directive 95/46/CE (il s'agit des pays ni membres de l'Union européenne, ni membres de l'Espace économique européen). Le transfert peut s'effectuer par communication, copie ou déplacement de données, par l'intermédiaire d'un réseau (ex : accès à distance à une base de données) ou d'un support à un autre, quel que soit le type de support (ex. d'un disque dur d'ordinateur à un serveur)* [21] ».

En pratique
Des illustrations de transferts de données, ou flux transfrontières, ont également été données par la CNIL dans ses divers guides sur le sujet. Ainsi, il peut par exemple s'agir :
- de la centralisation intra-groupe, dans un pays hors Union européenne, de la base de données de gestion des commandes et de la comptabilité client ;
- de la centralisation intra-groupe, dans un pays hors Union européenne, de la base de données de gestion des ressources humaines d'un groupe multinational ;
- du transfert vers un prestataire situé dans un pays hors Union européenne, aux fins de saisies informatiques de dossiers manuels ;
- du recours à un centre d'appel hors Union européenne et d'un transfert du fichier correspondant pour le démarchage de clients ou des opérations de qualification ;
- de l'hébergement et de l'exploitation de plates-formes informatiques dans un pays hors Union européenne ;
- de systèmes internationaux de maintenance informatique faisant appel à des ressources hors Union européenne.

C'est donc dans ces situations que les dispositions du règlement relatives aux transferts hors Union européenne ont vocation à s'appliquer.

2/ Conditions de la licéité d'un transfert de données hors Union européenne

En premier lieu, un tel transfert de données à caractère personnel peut avoir lieu si le pays tiers ou l'organisation internationale a été reconnu par la Commission européenne comme assurant un **niveau adéquat de protection** des données. Dans cette hypothèse, aucune autorisation n'est nécessaire pour mettre en œuvre le transfert.

[20] CNIL, Guide « Transferts de données à caractère personnel vers des pays tiers à l'Union européenne », éd.2010.
[21] CNIL, Guide « Les transferts de données à caractère personnel hors Union européenne », éd.2012.

A ce jour, les pays reconnus par une décision d'adéquation comme offrant un niveau suffisant de protection des données à caractère personnel sont les suivants :

- la Suisse[22];
- le Canada[23] ;
- l'Argentine[24] ;
- Guernesey[25] ;
- l'Ile de Man[26] ;
- Jersey[27];
- Andorre[28] ;
- les Iles Féroé[29] ;
- Israël[30] ;
- l'Uruguay[31]
- la Nouvelle-Zélande[32].

Les Etats de l'Espace économique européen (la Norvège, l'Islande et le Lichtenstein) sont également considérés comme disposant d'un niveau de protection adéquate.

Par ailleurs, depuis une décision de la Commission européenne du 26 juillet 2000[33], les entreprises américaines ayant adhéré au Safe Harbor[34] étaient considérées comme assurant une protection adéquate des données. Néanmoins, le 6 octobre 2015, la Cour de justice de l'Union européenne (CJUE) a invalidé la décision de la Commission européenne du 26 juillet 2000[35]. Aussi, depuis cette décision, les transferts de données à caractère personnel qui s'opèrent encore sur la base du « Safe Harbor» sont illégaux.

Un nouvel accord a alors été trouvé entre la Commission européenne et les Etats-Unis imposant des obligations plus fortes aux sociétés américaines qui se voient communiquer des données à caractère personnel depuis l'Europe. Cet accord se nomme EU-US Privacy Shield. Le 12 juillet 2016, la Commission européenne a adopté une décision[36] visant à reconnaître aux principes du EU-US Privacy Shield un niveau de protection adéquat. Cet accord fait à ce jour l'objet de controverses. Toutefois, les entreprises américaines qui ont adhéré à ce mécanisme sont par principe considérées comme assurant un niveau de protection adéquat.

[22] Décision 2000/518/CE du 26-07-2000.
[23] Décision 2002/2/CE du 20-12-2001.
[24] Décision 2003/490/CE du 30-06-2003.
[25] Décision 2003/821/CE du 21-11-2003.
[26] Décision 2004/411/CE du 28-04-2004.
[27] Décision 2008/393/CE du 08-05-2008.
[28] Décision 2010/625/UE du 19-10-2010.
[29] Décision 2010/146/UE du 5-3-2010.
[30] Décision 2011/61/UE du 31-1-2011.
[31] Décision 2012/484/UE du 21-8-2012.
[32] Décision 2013/65/UE du 19-12-12.
[33] Décision 2000/520/CE du 26-7-2000.
[34] Ensemble de principes de protection des données personnelles publié par le Département du Commerce américain, auquel des entreprises établies aux Etats-Unis adhèrent volontairement afin de pouvoir recevoir des données à caractère personnel en provenance de l'Union européenne.
[35] CJUE, 06 10 2015, n° C-362/14 (affaire Schrems).
[36] Décision 2016/1250/UE du 12-7-2016.

Nécessité d'une vérification périodique
Le règlement prévoit qu'un mécanisme d'examen périodique des décisions d'adéquation par la Commission européenne, au moins une fois tous les quatre ans, devra être déployé : la Commission devra alors réévaluer le niveau de protection offert par chaque pays (ou organisation internationale) concerné(e) ayant fait l'objet d'une décision d'adéquation afin de s'assurer que ce niveau de protection est toujours suffisant. A défaut, elle pourra modifier, abroger ou suspendre la décision d'adéquation. A cet égard, il est par ailleurs précisé que les décisions adoptées à ce jour demeurent en vigueur jusqu'à leur modification, remplacement ou abrogation par la Commission européenne.

Or, il résulterait de l'abrogation par exemple d'une décision d'adéquation que les transferts fondés sur cette décision deviendraient illicites et devraient alors faire l'objet d'un autre encadrement…

Il convient donc pour chaque organisme procédant à des transferts de données hors Union européenne sur le fondement de décisions d'adéquation de mettre en œuvre un process interne de vérification régulière de la validité desdites décisions d'adéquation, par exemple au moyen d'un suivi régulier de la doctrine de la Commission européenne sur ce point.

En deuxième lieu, le transfert peut être fondé sur un **mécanisme assurant des garanties appropriées**. En fonction du mécanisme retenu, une autorisation de l'autorité de contrôle peut devoir être obtenue.

Ces mécanismes sont listés dans le tableau infra, selon qu'une autorisation de l'autorité de contrôle est nécessaire ou non :

Absence de nécessité d'une autorisation particulière	Nécessité d'une autorisation de l'autorité de contrôle
Instrument juridique contraignant et exécutoire entre les autorités ou organismes publics concernés.	Dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits effectifs et opposables pour les personnes concernées.
Règles d'entreprise contraignantes (couramment désignées sous le terme anglais « binding corporate rules » ou « BCR »). *Précision : les BCR concernent un groupe d'entreprises, leur contenu est régi par le règlement et ce document doit être validé par l'autorité de contrôle avant de pouvoir constituer un fondement valable pour les transferts de données.*	Clauses contractuelles ad hoc entre d'une part le responsable de traitement ou le sous-traitant, et d'autre part l'organisme situé dans un pays tiers ou l'organisation internationale.
Clause contractuelles types adoptées par la Commission européenne ou par l'autorité de contrôle et approuvée par la Commission européenne. *Précision : les autorisations accordées à ce jour par les autorités de contrôle s'agissant des*	

transferts de données fondés sur des mécanismes contractuels ainsi que les clauses contractuelles types adoptées par la Commission européenne demeurent valables jusqu'à leur modification, remplacement ou abrogation éventuelle.	
Code de conduite / mécanisme de certification approuvé, dans les conditions du RGPD, assorti de l'engagement contraignant et exécutoire pris par le destinataire des données dans le pays tiers d'appliquer les garanties appropriées, y compris pour ce qui concerne les droits des personnes concernées.	

En troisième lieu, des **dérogations pour des situations particulières** sont également prévues par le règlement en l'absence de décision d'adéquation ou de garanties appropriées.

Ainsi, des transferts de données vers des Etats hors Union européenne ou une organisation internationale peuvent être mis en œuvre à condition de répondre à **une des conditions** suivantes :

- la personne concernée a consenti explicitement au transfert ;
- le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable de traitement, ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ;
- le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable de traitement et un tiers ;
- le transfert est nécessaire pour des motifs importants d'intérêt public reconnus par le droit de l'Union européenne ou le droit de l'Etat membre auquel le responsable de traitement est soumis ;
- le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ;
- le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité de donner son consentement ;
- le transfert a lieu au départ d'un registre qui est destiné à fournir des informations au public et est ouvert à la consultation du public en général, ou de toute personne justifiant d'un intérêt légitime (uniquement conformément aux conditions prévues dans le droit de l'Union européenne ou de l'Etat membre concerné).

Enfin, **si aucune de ces dérogations n'est applicable**, le règlement prévoit qu'un transfert de données vers un Etat hors Union européenne ou une organisation internationale ne peut être mis en œuvre que si les conditions suivantes sont ***cumulativement*** remplies, de tels transferts ne devant être mis en œuvre que dans des hypothèses résiduelles :

- absence de caractère répétitif ;
- nombre limité de personnes concernées ;

- transfert nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable de traitement sur lesquels ne prévalent pas les intérêts ou droits et libertés des personnes concernées ;
- évaluation par le responsable de traitement de toutes les circonstances entourant le transfert (notamment au regard de la nature des données transférées, à la finalité et à la durée des opérations, ainsi qu'à la situation du pays d'origine et du pays destinataire) et garanties appropriées prises sur la base de cette évaluation ;
- information de l'autorité de contrôle ;
- information de la personne concernée notamment sur le transfert et les intérêts légitimes impérieux poursuivis.

Attention
Ces dérogations ou exceptions risquent de faire l'objet d'une interprétation restrictive par les autorités de contrôle et ne doivent donc être utilisées pour fonder un transfert de données qu'avec prudence, après une analyse approfondie préalable du respect des conditions posées par le règlement. Par ailleurs, en l'absence de décision d'adéquation, le droit de l'Union européenne ou d'un Etat membre peut venir fixer des limites au transfert de certaines catégories spécifiques vers des Etats non membres ou des organisations internationales, ce dont il résulte qu'une vérification de ces hypothèses au cas par cas s'impose, en sus des dérogations précitées stricto sensu.

* *
*

En conclusion, si diverses possibilités s'offrent aux responsables de traitements et aux sous-traitants pour leur permettre de procéder à la mise en œuvre de transferts de données à caractère personnel vers des Etats non membres de l'Union européenne ou vers des organisations internationales, de telles opérations doivent être anticipées et faire l'objet d'une analyse préalable afin de déterminer le fondement pouvant légitimer de tels transferts ainsi que les mesures à déployer pour encadrer ces flux de données (clauses contractuelles, règles d'entreprise contraignantes, obtention d'une autorisation ou de l'approbation de l'autorité de contrôle, information de cette dernière, etc.).

La suite aux prochaines leçons…

Références textuelles
Considérants 101) à 116)
Articles 44 à 50

Leçon 9 – Gérer le sort des données présentant une certaine sensibilité

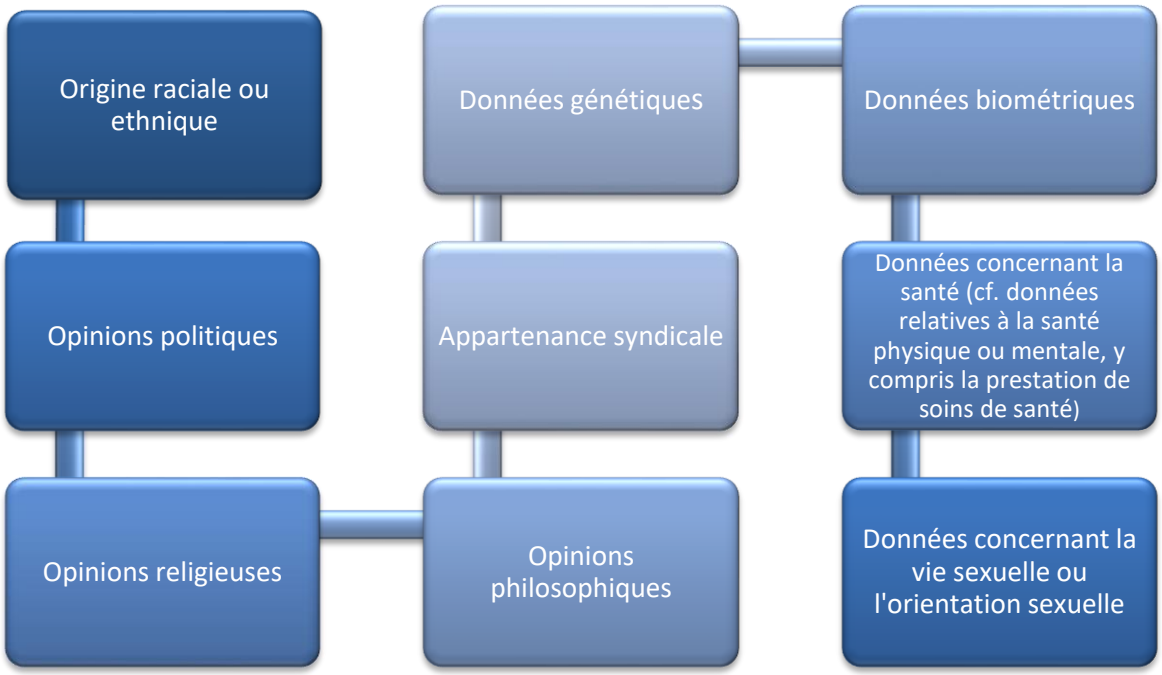
Le traitement de certaines données spécifiques doit faire l'objet d'une attention renforcée. Ces données peuvent être réparties en deux catégories : d'une part les données identifiées par le RGPD comme « particulières », et d'autre part les données relatives aux condamnations pénales et infractions.

En ce qu'elles présentent une certaine sensibilité, ces données ne peuvent faire l'objet d'un traitement que sous certaines conditions.

1/ Les données dites « particulières »

Certaines catégories de données identifiées comme « particulières » sont visées par le règlement comme des données dont le traitement est par principe **interdit**.

Il s'agit des données suivantes :



Toutefois, des **exceptions** à cette interdiction existent. Aussi, en cas de nécessité de procéder au traitement de telles données, alors il convient de vérifier si une de ces exceptions est applicable.

Le tableau ci-après donne un aperçu des situations dans lesquelles ces données dites « sensibles » peuvent être traitées. Des commentaires, pour chaque exception, sont destinés à en faciliter la compréhension.

Exception	Commentaires
Consentement explicite de la personne concernée	Ce consentement doit viser un ou plusieurs finalités déterminées. Par ailleurs, cette exception n'est pas valable dans les hypothèses dans lesquelles le droit de l'Union européenne ou d'un Etat membre prévoit que l'interdiction ne peut pas être levée par la personne concernée.
Traitement nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale	Exemples : traitement de gestion des retraites, traitement à des fins de sécurité, de surveillance et d'alerte sanitaire, de prévention ou de contrôle de maladies transmissibles et d'autres menaces graves pour la santé, traitement poursuivant un objectif de santé publique et de gestion des services de soins de santé, en particulier pour assurer la qualité et l'efficience des procédures de règlement des demandes de prestations et de services dans le régime d'assurance-maladie. Cette exception ne peut être valablement utilisée que si le droit de l'Union européenne, le droit d'un Etat membre ou une convention collective prévoit un tel traitement ainsi que des garanties appropriées pour les droits et libertés des personnes concernées.
Traitement nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne	Cette exception ne peut être valablement utilisée que si la personne concernée se trouve dans l'incapacité de donner son consentement, et à condition qu'une décision immédiate doive être prise pour la sauvegarde de la vie de la personne concernée.
Traitement effectué dans le cadre de leurs activités légitimes et moyennant les garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale	Conditions cumulatives pour l'application de cette exception : - le traitement ne peut se rapporter qu'aux membres et anciens membres dudit organisme ou aux personnes entretenant avec lui des contacts réguliers en liaison avec ses finalités ; - les données ne sont pas communiquées en dehors de cet organisme sans le consentement de la personne concernée. Cette exception ne peut être valablement utilisée que pour les typologies de données en lien avec la finalité poursuivie par l'organisme. A titre d'illustration, elle ne semble pas pouvoir justifier qu'une association politique dispose des données de santé de ses membres, ou encore d'informations relatives à leurs opinions religieuses.
Données manifestement rendues publiques par la personne concernée	Cette exception doit être interprétée restrictivement. A titre d'illustration, le G29 a ainsi pu considérer, dans le cas des réseaux sociaux par exemple, qu'il ne suffit pas qu'une

	personne communique ses données « sensibles » pour qu'il puisse en être déduit qu'elle les a rendues publiques. Ainsi, selon le G29, un réseau social qui souhaite collecter des données sensibles sur ses membres doit obtenir leur consentement explicite, libre, informé et spécifique. Si ces données figurent parmi les champs à compléter pour s'inscrire, il doit y être indiqué très clairement que ces champs sont purement facultatifs[37] et que l'internaute accepte en les complétant que ces informations soient publiées sur internet au sein du réseau social en question.
Traitement nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou lorsque les juridictions agissent dans le cadre de leurs fonction juridictionnelle	S'agissant de la constatation, l'exercice ou la défense d'un droit en justice, cette exception est valable que ce soit dans le cadre d'une procédure judiciaire, administrative ou extra-judiciaire.
Traitement nécessaire pour des motifs d'intérêt public important	Cette exception ne peut être valablement utilisée que sur la base du droit de l'Union européenne ou d'un Etat membre, qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et intérêts de la personne concernée.
Traitement nécessaire aux fins de la médecine préventive, de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services sanitaires et sociaux	Cette exception ne peut être valablement utilisée que sur la base du droit de l'Union européenne, du droit d'un Etat membre ou en vertu d'un contrat conclu avec un professionnel de santé. Dans cette hypothèse, les données ne peuvent être traitées que par un professionnel de santé soumis à une obligation légale, règlementaire ou ordinale de secret professionnel ou, sous sa responsabilité, par une autre personne également soumise à un tel secret. Cette exception peut également viser le traitement, par les autorités de gestion et les autorités centrales de santé nationales, des données en vue du contrôle de la qualité, de l'information des gestionnaires et de la supervision générale du système de soins de santé ou de la protection sociale, et en vue d'en assurer la continuité, ou à des fins de sécurité, de surveillance et d'alerte sanitaire, ainsi que pour des études menées dans l'intérêt public dans le domaine de la santé publique.
Traitement nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique	Exemple : finalité de protection contre les menaces transfrontalières graves pesant sur la santé, finalité visant à garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux. Cette exception ne peut être valablement utilisée que sur la base du droit de l'Union européenne ou d'un Etat membre qui prévoit des mesures appropriées et spécifiques pour la

[37] G29, Avis 5/2009 du 12-6-2009 sur les réseaux sociaux en ligne.

	sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel. La notion de « santé publique » doit s'interpréter selon la définition prévue dans le règlement 2008/1338/CE[38] : tous les éléments relatifs à la santé, à savoir l'état de santé, morbidité et handicaps inclus, les déterminants ayant un effet sur cet état de santé, les besoins en matière de soins de santé, les ressources consacrées aux soins de santé, la fourniture des soins de santé, l'accès universel à ces soins, les dépenses de santé et leur financement, ainsi que les causes de mortalité. Le règlement précise que de tels traitements ne doivent pas aboutir à ce que des données à caractère personnel soient traitées à d'autres fins par des tiers, tels que les employeurs, les compagnies d'assurance ou les banques.
Traitement nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques	Cette exception ne peut être valablement utilisée que sur la base du droit de l'Union européenne ou d'un Etat membre, qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et intérêts de la personne concernée.

Cas particulier des données génétiques, biométriques et de santé
Les Etats membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données de santé, des données génétiques et des données biométriques. Par conséquent, seule une vérification des textes de droit national en sus des dispositions du règlement peut permettre de s'assurer des conditions de licéité d'un traitement.

2/ Les données relatives aux infractions et condamnations

Des dispositions spécifiques sont également applicables aux données relatives aux infractions, aux condamnations pénales et aux mesures de sûreté connexes. En effet, le traitement de telles données ne peut être effectué qu'à l'une des conditions suivantes :

- le traitement est effectué sous le **contrôle de l'autorité publique** (tout registre complet des condamnations pénales ne peut d'ailleurs être tenu que sous le contrôle de l'autorité publique) ;

- le traitement est **autorisé par le droit** de l'Union européenne ou par le droit d'un Etat membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées.

[38] Règlement 2008/1338/CE du 16-12-2008 relatif aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail.

Aussi, hormis le cas des autorités publiques, il convient, avant de mettre en œuvre un tel traitement, de vérifier s'il est autorisé par un texte du droit de l'Union européenne ou du droit national qui serait applicable à l'organisme concerné. A défaut, le traitement de telles données est interdit.

Illustration
A titre d'exemple, il est courant que les entreprises mettent en œuvre un traitement de gestion des contentieux, a minima en vue de provisionner les sommes nécessaires à une éventuelle condamnation financière. Or, de tels traitements peuvent éventuellement mener à traiter des données relatives à des infractions ou condamnations pénales (et ce même si le contentieux en cause n'intervient pas en matière pénale). Il résulte du règlement que seul un texte du droit de l'Union européenne ou du droit national pourra autoriser un tel traitement.

* *
*

La mise en œuvre de traitements portant sur de telles données doit donc s'accompagner de précautions particulières afin de vérifier si les conditions nécessaires à leur licéité sont remplies.

Par ailleurs, outre les conditions nécessaires à la licéité du traitement, il convient également de rappeler que des conséquences résultent du traitement de telles données pour les entités à l'origine de leur mise en œuvre, notamment : la mise en œuvre d'analyses d'impact obligatoires[39], la nécessité de désigner un délégué à la protection des données[40], l'obligation d'insérer le traitement dans un registre dans tous les cas, etc.

Rendez-vous à la prochaine leçon pour clore cette série en faisant le point sur les voies de recours et sanctions encourues en cas de non-respect des dispositions du règlement, et les moyens de s'y préparer.

Références textuelles
Considérants 51) à 56)
Articles 9 et 10

[39] Sur l'analyse d'impact, voir leçon 4.
[40] Sur le délégué à la protection des données, voir leçon 7.

Leçon 10 – Anticiper les poursuites et les sanctions

Les leçons précédentes avaient vocation à appréhender les grandes lignes du règlement et les contraintes et conséquences générales en résultant. Cette dernière leçon est l'occasion de faire le point sur les poursuites et sanctions éventuellement encourues en cas de non-respect des dispositions applicables en matière de protection des données à caractère personnel.

1/ Les pouvoirs de l'autorité de contrôle

L'autorité de contrôle a notamment pour mission de contrôler l'application du règlement et de veiller au respect de celui-ci. Elle peut donc effectuer des **enquêtes** à cette fin, notamment (mais non exclusivement) sur la base d'informations reçues d'une autre autorité de contrôle, ou encore d'une autre autorité publique par exemple. Elle peut également effectuer des enquêtes sur sa propre initiative ou encore suite à une réclamation d'une personne concernée.

Dans le cadre de son pouvoir d'enquête, l'autorité de contrôle peut notamment :

- ordonner la communication de toute information dont elle a besoin pour l'accomplissement de ses missions ;
- procéder à des audits de protection des données ;
- procéder à un examen des certifications délivrées ;
- notifier une violation alléguée du règlement ;
- obtenir l'accès à toutes les données à caractère personnel et informations nécessaires à l'accomplissement de ses missions ;
- obtenir l'accès à tous les locaux, notamment à toute installation et à tout moyen de traitement.

Par ailleurs, toute personne concernée a le droit d'introduire une **réclamation** auprès d'une autorité de contrôle si elle considère qu'un traitement de données à caractère personnel la concernant constitue une violation du règlement. Une telle réclamation peut être introduite tant à l'égard d'un responsable de traitement que d'un sous-traitant, elle est gratuite pour la personne concernée et l'autorité de contrôle doit même veiller à ce que l'introduction de telles réclamations soit facilitée (ex : formulaire en ligne notamment).

Suite à une enquête ou à une réclamation introduite par une personne concernée, l'autorité de contrôle dispose du pouvoir d'adopter diverses **mesures correctrices**, à savoir :

Thème	Détail de la mesure
Avertissement	Prononcer un avertissement sur le fait que les opérations de traitement envisagées sont susceptibles d'une violation du règlement.
Rappel à l'ordre	Prononcer un rappel à l'ordre en cas de violation du règlement.

Mise en conformité	Ordonner de mettre les opérations de traitement en conformité avec le règlement, le cas échéant de manière spécifique et dans un délai déterminé.
Respect des droits des personnes	Ordonner de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits.
	Ordonner de communiquer à la personne concernée une violation de données à caractère personnel.
	Ordonner la rectification ou l'effacement des données, ou la limitation du traitement conformément au règlement, et la notification de ces mesures aux destinataires auxquels les données ont été divulguées.
Limitation	Imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement.
Retrait / refus de certification	Retirer une certification, demander à l'organisme de certification de retirer une certification ou de ne pas délivrer une telle certification si les conditions requises ne sont pas ou plus satisfaites.
Suspension des flux	Ordonner la suspension des flux de données adressées à un destinataire situé dans un pays tiers à l'UE ou à une organisation internationale.

Par ailleurs, des **amendes administratives** peuvent être prononcées par l'autorité de contrôle. Ces amendes peuvent être prononcées en complément ou à la place des mesures susvisées.

En pratique, s'agissant des amendes administratives encourues, le RGPD distingue les violations en deux catégories :

Les violations pouvant faire l'objet d'amendes administratives pouvant s'élever jusqu'à ***10 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total*** de l'exercice précédent (le montant le plus élevé étant retenu).

Quelques exemples

- non-respect des principes de privacy « by design » et « by default » ;
- absence de tenue du registre des activités de traitement lorsqu'il est obligatoire ;
-absence de notification à l'autorité de contrôle ou à la personne concernée d'une violation de données à caractère personnel ;
- mesures de sécurité des données inexistantes, insuffisantes ou inappropriées ;
- absence de réalisation de l'analyse d'impact lorsqu'elle est nécessaire ;
- défaut d'encadrement contractuel des relations entre les responsables conjoints de traitement ou avec les sous-traitants ;
- absence de désignation d'un délégué à la protection des données dans les hypothèses où une telle désignation est obligatoire ;
- etc.

Les violations pouvant faire l'objet d'amendes administratives pouvant s'élever jusqu'à ***20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total*** de l'exercice précédent (le montant le plus élevé étant retenu).

Quelques exemples

- non-respect des principes de base applicables aux traitements de données à caractère personnel (loyauté, transparence, limitation des finalités, minimisation des données, durée de conservation, etc.) ;
- non-respect des conditions de licéité du traitement ;
- non-respect des droits des personnes concernées (information, accès, rectification, effacement, etc.) ;
- non-respect des conditions devant présider à la mise en œuvre de traitements de données « particulières » ;
- mise en œuvre de transferts de données vers des pays tiers ou une organisation internationale sans que les conditions requises soient respectées ;
- non-respect d'une injonction prononcée par l'autorité de contrôle ;
- etc.

Enfin, l'autorité de contrôle peut saisir les autorités judiciaires, voire **agir en justice**, en vue de faire appliquer les dispositions du règlement.

La règle d'or : anticiper, coopérer et réagir
Dans le cadre de l'évaluation des mesures et sanctions qu'elle peut être amenée à prononcer, l'autorité de contrôle tiendra compte de circonstances « aggravantes » (par exemple, mesures ou sanctions antérieurement prononcées) ou « atténuantes » (par exemple, coopération avec l'autorité de contrôle ou mesures correctives prises en vue de remédier à la violation et d'en atténuer les effets négatifs) pouvant être mises à la charge du responsable de traitement ou du sous-traitant concerné.

Aussi, il est indispensable :
- d'anticiper : en déployant dès à présent les actions nécessaires à la mise et au maintien de son entité en conformité avec le règlement, notamment en ce qui concerne les mesures techniques et organisationnelles nécessaires au respect des principes d'accountability et de sécurité ;
- de coopérer : en collaborant avec l'autorité de contrôle en cas d'enquête ou de réclamation, des guidelines à cette fin (sensibilisation du personnel, formalisation d'un guide des relations avec l'autorité de contrôle, etc.) pouvant utilement être déployées pour anticiper une telle situation ;
- de réagir : en déployant, en cas d'enquête de l'autorité de contrôle ou de réclamation, un plan d'actions à effet immédiat en vue de remédier aux éventuelles non-conformités.

2/ Le recours juridictionnel

Les personnes concernées ont le droit à un recours juridictionnel effectif si elles considèrent que les droits que leur confère le règlement ont été violés du fait d'un traitement de données à caractère personnel.

Une telle action peut être intentée tant à l'égard d'un responsable de traitement que d'un sous-traitant, notamment en vue d'obtenir la cessation du dommage ou de l'atteinte subi, et la réparation du préjudice moral ou matériel subi.

Par ailleurs, il est précisé que les Etats membres ont toute latitude pour déterminer le régime d'autres sanctions qui pourraient être applicables en cas de violation du règlement. Notamment, le règlement mentionne expressément dans ses considérants que les Etats membres devraient pouvoir déterminer le régime des sanctions pénales applicables en cas de violation du règlement, y compris de violation des dispositions nationales adoptées en application et dans les limites dudit règlement.

Possibilité de recours cumulatifs
Sous réserve de l'application du principe de « non bis in idem » en matière pénale (c'est-à-dire le principe selon lequel une même infraction résultant des mêmes faits ne peut pas faire l'objet de plusieurs poursuites) interprété à la lumière de la jurisprudence de la Cour de justice de l'Union européenne (CJUE), il résulte de ce qui précède qu'un recours juridictionnel n'est pas exclusif d'une réclamation auprès d'une autorité de contrôle, et inversement.

* *
*

Le non-respect des dispositions du règlement ainsi que des dispositions nationales prises en vertu de ce règlement peut donc faire l'objet de sanctions particulièrement sévères.

Actions des organismes, organisations et association à but non lucratif
Il est à noter que le règlement prévoit que les organismes, organisations et associations à but non lucratif constitués conformément au droit d'un Etat membre, dont les objectifs statutaires sont d'ordre public et qui sont actifs dans le domaine de la protection des données à caractère personnel peuvent intervenir dans le cadre des différents recours reconnus à la personne concernée :
- soit sur mandat de la personne concernée pour agir en son nom et exercer le droit de cette dernière à obtenir réparation ;
- soit, indépendamment de tout mandat, en vue de la cessation de l'atteinte (dans cette hypothèse, la réparation du préjudice ne peut toutefois pas être poursuivie).

La multiplicité des voies de recours ouvertes ainsi que des mesures et sanctions pouvant être prononcées doit convaincre chaque organisme, chaque entité de déployer un plan d'actions efficace, effectif et approprié en vue de se mettre et de se maintenir en conformité avec les dispositions du règlement.

Ainsi s'achèvent les « 10 leçons » principales nécessaires à une vision globale et à une approche générale du règlement.

Mais de nombreux focus thématiques pourront être proposés, afin d'approfondir et d'analyser de manière pragmatique certains sujets précis.

N'hésitez pas à nous faire part des thématiques que vous souhaiteriez voir abordées….

Références textuelles
Considérants 129) et 141) à 152)
Articles 57, 58 et 77 à 84

Pour nous contacter :

Agil'IT
40 rue du Colisée
75008 PARIS

Tel : 01 81 70 99 24
Mail : laure.landes-gronowski@agilit.law

www.agilit.law