BONDARD

Protect & Develop

DONNÉES À CARACTÈRE PERSONNEL @ Station F - 29/11/17

Maître Céline Bondard
Avocat aux Barreaux de Paris et New-York
Maître de conférences à IEP Paris, HEC, Ecole Polytechnique
Co-fondateur et Président de la French-American Bar Association

TABLE DES MATIÈRES

LE RÈGLEMENT EUROPÉEN, AUTREMENT INTITULÉ:

« LE RÈGLEMENT 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 »

Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

En mai 2016, l'Union européenne (UE) a publié le Règlement Général sur la Protection des Données («RGPD»).

Il sera applicable dans tous les Etats membres de l'UE à partir du 25 mai 2018.

A. DÉFINITION DES DONNÉES À CARACTÈRE PERSONNEL

On trouve la définition des données à caractère personnel à l'article 4, § 1 du nouveau règlement:

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

B. LA COLLECTE DE DONNÉES PERSONNELLES: OUI, SOUS CERTAINES CONDITIONS

Les données à caractère personnel doivent être (Art5, §1) :

- **Comment les traiter ?** → *de manière licite, loyale et transparente* au regard de la personne concernée
- **Pourquoi ?** →*collectées pour des finalités déterminées, explicites et légitimes,* et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; *adéquates, pertinentes et limitées* à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées
- **Quelles données ?** → *exactes et, si nécessaire, tenues à jour*
- **Comment les conserver ?** → *conservées sous une forme de manière intègre et confidentielle.*

C. LES DONNÉES « SENSIBLES » : NON, SAUF EXCEPTIONS (VASTES EXCEPTIONS…)

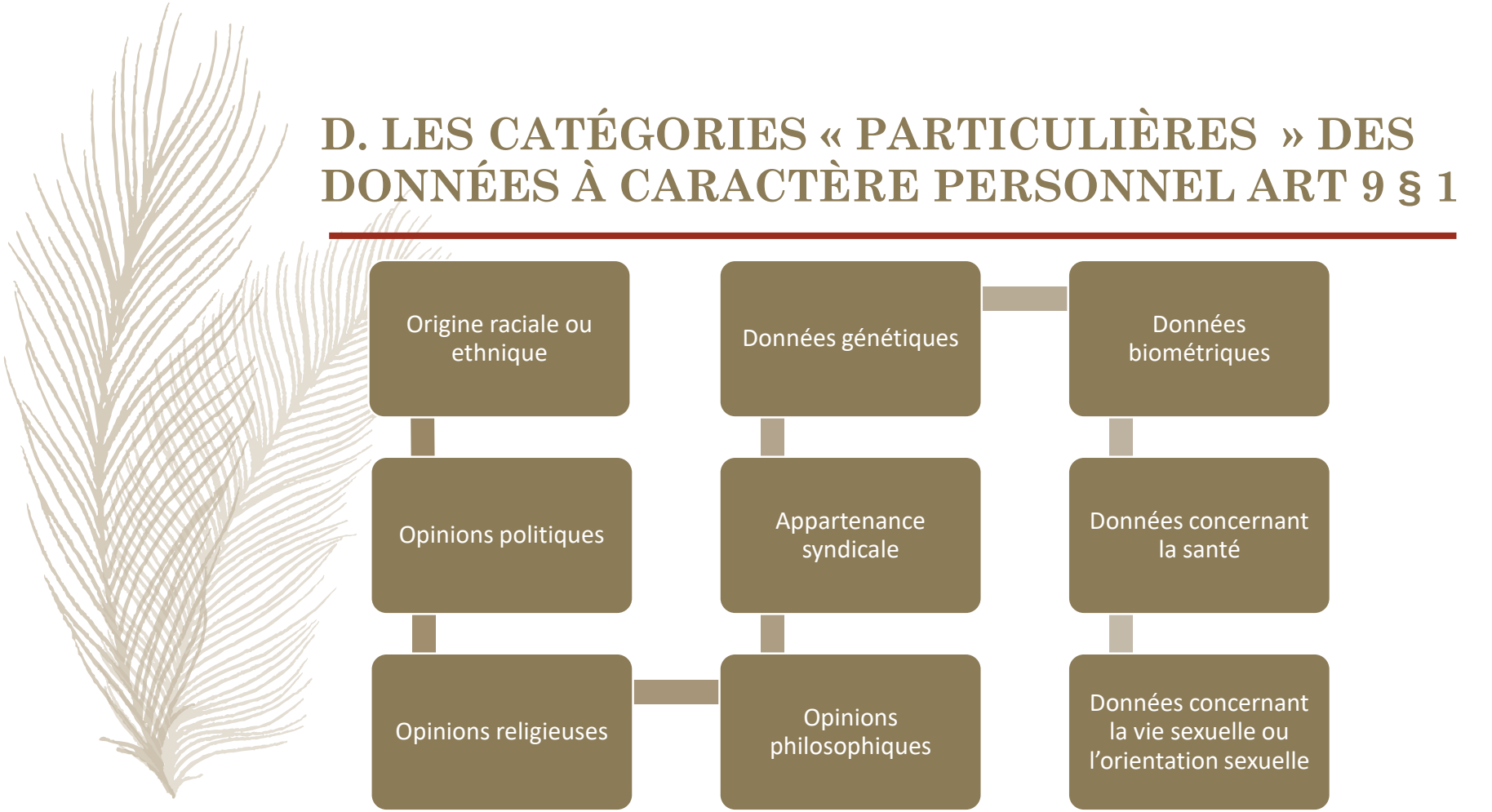
« Les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux ***méritent une protection spécifique****, car le contexte dans lequel elles sont traitées pourrait engendrer des risques importants pour ces libertés et droits ».*

Au titre des articles 9 et 10 du RGPD, ces données sont réparties en deux catégories :

- les données identifiées comme « particulières »

- les données relatives aux condamnations pénales et infractions, qui *« (…) ne devraient pas faire l'objet d'un traitement, à moins que celui-ci ne soit autorisé dans des cas spécifiques prévus par le présent règlement »* (considérant 51 du RGPD).

D. LES CATÉGORIES « PARTICULIÈRES » DES DONNÉES À CARACTÈRE PERSONNEL ART 9 § 1



D. LES EXCEPTIONS AU PRINCIPE D'INTERDICTION DES CATÉGORIES « PARTICULIÈRES » ART 9 § 1

Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie:

a) **En cas de consentement explicite**
b) Nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement
c) Nécessaire à la sauvegarde des intérêts vitaux de la personne concernée
d) Dans le cadre de leurs activités légitimes et moyennant des garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif
e) Le traitement des données personnelles rendues publiques
f) Nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice
g) Justifié pour des motifs d'intérêt public important
h) Nécessaire aux fins de la médecine préventive ou de la médecine du travail
i) (...) Dans le domaine de la santé publique
j) (...) À des fins archivistiques à des fins de recherche scientifique ou historique ou à des fins statistiques

❑ En résumé

- Les données à caractère personnel doivent respecter les principes généraux relatif aux données à caractère personnel figurant à l'article 5, §1 (licéité, loyauté, transparence, limitation des finalités, minimisation des données etc.).

- Il faut porter une attention encore plus grande pour les données sensibles:

  - ✓ Les catégories particulières des données à caractère personnel (Art 9 §1).

  - ✓ Les données relatives aux condamnations pénales et infractions (Art 10).

COMMENCER PAR LE COMMENCEMENT: AVOIR L'AUTORISATION DES CONCERNÉS

A. LE CONSENTEMENT DOIT ÊTRE TRÈS EXPLICITE

Le consentement étant nécessaire, il se doit d'être "**préalable**" à la collecte des données (Considérant 40 du RGPD).

*« Le consentement devrait être donné par un **acte positif clair** par lequel la personne concernée manifeste **de façon libre, spécifique, éclairée et univoque** son accord au traitement des données à caractère personnel la concernant (…)* » (Considérant 32 du RGPD).

Dans un formulaire en ligne, il peut se matérialiser, par exemple, par une case à cocher non cochée par défaut.

B. COMMENT PROUVER QUE VOUS AVEZ OBTENU LE CONSENTEMENT DES CONCERNÉS ? (Art 7 du RGPD)

– ***(…) le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement.*** *Cela implique donc de tracer et conserver la preuve que le consentement a été donné, ainsi que de la (ou des) finalité(s) pour lesquelles il a été donné ;*

– ***la demande de consentement doit être présentée sous une forme compréhensible****, aisément accessible, en des termes clairs et simples (…);*

– ***il doit apparaitre clairement*** *que l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement ;*

– ***la personne concernée doit être informée qu'elle a le droit de retirer son consentement*** *à tout moment, en précisant qu'il est aussi simple de retirer que de donner son consentement ».*

(*Protection des données personnelles*, Gérer le consentement des personnes concernées, 1. Le consentement, une notion clé dans le RGPD, Edition Législatives, 2017)

❑ En résumé

- **Définition du consentement:** acte positif donné de façon libre, spécifique, éclairée et univoque (Art 7 §2).
- **Comment prouver que vous avez obtenu ce consentement:** le RGPD renforce la responsabilité du responsable de traitement (Art 7§1). Obligation de transparence, de clarté, de traçabilité et de conservation du consentement donnée par la personne concernée.
- **Question de preuve:** Il revient au responsable de traitement de prouver que les conditions applicables au consentement (Art 7) ont été respectées!

II

LES DROITS DES PERSONNES CONCERNÉES UNE FOIS LES DONNÉES COLLECTÉES.

(ILS SONT NOMBREUX!)

IV. LE RESPECT DES DROITS DE LA PERSONNE

1. Droit **d'information et d'accès** aux données personnelles
2. Droit de **rectification et d'effacement** (ou « droit à l'oubli ») des données personnelles
3. Droit à la **limitation du traitement** de données personnelles
4. Droit à la **portabilité des données personnelles**
5. Droit **d'opposition à un traitement de données personnelles**
6. Droit de ne pas faire l'objet d'une décision individuelle automatisée y compris en matière de **profilage**

1. LE DROIT D'INFORMATION ET D'ACCÈS AUX DONNÉES PERSONNELLES (*Art 13, 14 et 15*)

Lorsque les données ont été collectées auprès de la personne concernée, les informations à fournir doivent indiquer :

- L'identité du responsable du fichier ;
- La finalité du fichier ;
- Le caractère obligatoire ou facultatif des réponses et des conséquences d'un défaut de réponse ;
- Les destinataires des données ;
- Les éventuels transferts de données vers des pays hors UE.
- La durée de conservation des données à caractère personnel
- Leurs droits (droit d'accès, de rectification, et d'opposition) ;

2. LE DROIT D'ACCÈS ET DE RECTIFICATION (« DROIT À L'OUBLI », *Art 16 et 17*)

Toute personne peut:

- Accéder à l'ensemble des informations le concernant,
- Connaître l'origine des informations le concernant,
- Accéder aux informations sur lesquelles le responsable du fichier s'est fondé pour prendre une décision le concernant (par exemple, les éléments qui auraient servi pour ne pas vous accorder une promotion ou le score attribué par une banque et qui a conduit au rejet de votre demande de crédit),
- En obtenir la copie, (des frais n'excédant pas le coût de la reproduction peuvent être demandés)
- Exiger que ses données soient, selon les cas, rectifiées, complétées, mises à jour ou supprimées.

Et la Blockchain? Quid du droit à l'oubli?

3. LE DROIT À LA LIMITATION DU TRAITEMENT DES DONNÉES (*Art 18*)

La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'un des éléments suivants s'applique :

- l'exactitude des données à caractère personnel est contestée par la personne concernée
- le traitement est illicite et la personne concernée exige la limitation de leur utilisation
- le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice
- la personne concernée s'est opposée au traitement, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée (RGPD, art. 18, § 1).

4. LE DROIT À LA PORTABILITÉ DES DONNÉES (*Art 20*)

- Les personnes concernées **ont le droit de recevoir** leurs données à caractère personnel qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, **de les transmettre** à un autre responsable de traitement et **d'obtenir une transmission directe** d'un responsable du traitement à un autre, lorsque cela est techniquement possible, sans que le responsable du traitement originaire y fasse obstacle.
- Le droit à la **portabilité des données** n'est possible qu'à condition d'y exprimer expressément son consentement et que le traitement soit effectué l'aide des procédés automatisés.

5. LE DROIT D'OPPOSITION (*Art 21*)

- **Les personnes concernées doivent pouvoir s'opposer à la réutilisation** par le responsable du fichier de leurs coordonnées à des fins de sollicitations, notamment commerciales, lors d'une commande ou de la signature d'un contrat.
- **La simple mention de l'existence de ce droit dans les conditions générales n'est pas suffisante.**

6. LE DROIT DE NE PAS FAIRE L'OBJET D'UNE DÉCISION INDIVIDUELLE AUTOMATISÉE, Y COMPRIS EN MATIÈRE DE PROFILAGE (*Art 22*)

Définition du «profilage», Art 4 § 4 :

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

6. LE DROIT DE NE PAS FAIRE L'OBJET D'UNE DÉCISION INDIVIDUELLE AUTOMATISÉE, Y COMPRIS EN MATIÈRE DE PROFILAGE (*Art 22*)

- Art 22 § 1: « *La personne concernée a 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 de façon similaire.* »

- Une telle mesure existait déjà à l'article 15 de la directive 95/46/CE, lorsque le traitement automatisé était destiné à évaluer certains aspects de la personnalité de la personne concernée. Toutefois, les dispositions du RGPD sont plus larges dans la mesure où la finalité du profilage n'est pas précisée.

6. LE DROIT DE NE PAS FAIRE L'OBJET D'UNE DÉCISION INDIVIDUELLE AUTOMATISÉE, Y COMPRIS LE PROFILAGE (*Art 22*)

Exceptions à ce principe (RGPD, art. 22, § 2):

- Lorsque la décision individuelle automatisée est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement
- Lorsqu'elle est autorisée par le droit de l'Union ou le droit de l'Etat membre auquel le responsable du traitement est soumis
- Lorsqu'elle est fondée sur le consentement explicite de la personne concernée. *Disposition nouvelle.*

6. LE DROIT DE NE PAS FAIRE L'OBJET D'UNE DÉCISION INDIVIDUELLE AUTOMATISÉE, Y COMPRIS LE PROFILAGE (*Art 22*)

Problème: de nombreux services numériques fonctionnent sur la base d'un traitement algorithmique automatisé et les utilisateurs donnent aisément leur consentement à l'usage de tels outils sans pour autant avoir conscience de leur mode de fonctionnement.

- Les exceptions ne sont-elles pas en mesure de vider le principe de son sens?

(Protection des données personnelles, Edition Législatives, 2017, page 106)

❑ En résumé

1. Droit d'information et d'accès aux données personnelles (Art 13,14, et 15).
2. Droit de rectification et d'effacement (ou « droit à l'oubli ») des données personnelles (Art 16 et 17).
3. Droit à la limitation du traitement de données personnelles (Art18).
4. Droit à la portabilité des données personnelles (Art 20).
5. Droit d'opposition à un traitement de données personnelles (Art 21).
6. Droit de ne pas faire l'objet d'une décision individuelle automatisée y compris le profilage (Art 22).

IV

GESTION PRATIQUE DU TRAITEMENT DES DONNÉES PERSONNELLES

A. DÉFINITION DU TRAITEMENT (Art 5, RGPD)

- **La définition du « traitement » se trouve à l'article 4 § 2 :**

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

B. DÉLÉGUÉ À LA PROTECTION DES DONNÉES

- Les responsables du traitement et les sous-traitants doivent chacun désigner un **délégué à la protection des données** («DPD») si leurs (i) **activités de base** requièrent une surveillance ou un traitement à (ii) **grande échelle** (iii) **régulière et systématique** des personnes concernées.

- Les responsables du traitement doivent **conserver un registre** de leurs activités de traitement comportant un certain nombre d'informations.

Exemple: *la finalité du traitement, une description des catégories de personnes concernées, les mesures techniques et organisationnelles mises en œuvre ou encore tout transfert de ces données vers des pays tiers.*

C. UNE DURÉE DE CONSERVATION LIMITÉE DANS LE TEMPS

- **Une durée de conservation des données** doit être définie pour un temps limitée. Cette durée correspond au temps nécessaire à l'accomplissement de l'objectif qui était poursuivi lors de leur collecte. (Art 5. 1 c))

- **Par exemple, des données archivées pour faire valoir un droit en justice doivent être supprimées lorsque cette action est prescrite.**

D. UN TRAITEMENT SÉCURISÉ

- **Les responsables du traitement** doivent mettre *« en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ».* (RGPD, Art 32) Lesquelles peuvent inclure :
  - La mise en place de politiques de protection des données
  - L'adhésion à des codes de conduite approuvés
  - L'adhésion à des mécanismes de certification approuvés.

- **Lorsque l'archivage est confié à un sous-traitant,** le responsable du fichier doit s'assurer que son prestataire présente des garanties suffisantes en matière de sécurité et la confidentialité des données qui lui sont confiées.

Quel que soit le type d'archive, la consultation des données archivées doit être tracée

E. UN MODE DE TRAITEMENT LIBRE

Le choix du mode de traitement est laissé à l'appréciation du responsable du fichier. Des données peuvent ainsi être archivées :

- **Dans une base d'archive spécifique**, distincte de la base active, avec des accès restreints aux seules personnes ayant un intérêt à en connaitre en raison de leurs fonctions
- **Ou dans la base active**, à condition de procéder à un **isolement** des données archivées au moyen d'une séparation logique pour les rendre inaccessibles aux personnes n'ayant plus d'intérêt à les traiter.

Recommandations de la CNIL, « Durée de conservation et archivages des données ».

❑ En résumé

La gestion du traitement des données personnelles par le responsable du traitement, le ou les sous-traitant(s) ainsi que le délégué à la protection des données (« DPO ») implique :

- La conservation d'un registre (Art 30).
- Un tri qui doit permettre de ne conserver que les données indispensables et utiles (*Article 5. 1 (b)*).
- Une durée limitée dans le temps (Art 5. 1 c)).
- Un traitement sécurisé (« *mesures techniques et organisationnelles appropriées* », Art 32).
  - *Mais le mode de traitement est libre (Recommandations de la CNIL, « Durée de conservation et archivages des données »).*

V LA RESPONSABILITÉ DE LA COLLECTE: « RESPONSABLE » ET/OU « SOUS-TRAITANT »?

A. LOGIQUE DE CONTRÔLE A POSTERIORI

- **Sous la directive 95/49/CE,** la principale obligation à la charge du responsable du traitement consistait en l'accomplissement de formalités préalables.

- **Cette obligation est supprimée au profit d'une logique de contrôle *a posteriori* et non plus *a priori*.** Désormais, le responsable du traitement doit rendre compte et respecter un certain nombre d'obligations dont il doit apporter la preuve. (Art 5 paragraphe 2 du RGPD)

B. LE RESPONSABLE DE TRAITEMENT ET LE SOUS-TRAITANT: QUI EST QUI ?

- **Le RGPD, tout comme la directive 95/46/CE avant lui, impose au responsable du traitement des obligations, mais encore faut-il savoir de qui il s'agit.** L'article 26, § 1 du RGPD reconnait la possibilité d'une responsabilité conjointe du traitement, lorsque tout les responsables du traitement ont déterminés conjointement les finalités et les moyens du traitement.

- **Les parties définissent de manière transparente leurs obligations respectives,** aux fins d'assurer le respect des exigences du RGPD, notamment en ce qui concerne l'exercice des droits de la personne concernée et leurs obligations respectives, par voie d'accord entre eux. (*Protection des données personnelles*, Obligations au sein de l'Union, Responsabilité du sous-traitant et précision de la relation contractuelle, Editions Législatives, 2017)

C. LE SOUS-TRAITANT: DÉFINITION

- **Le sous-traitant est la personne physique ou morale,** l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (RGPD, art. 4, § 8).

- **Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes** quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée (art. 28, § 1).

- **Le sous-traitant n'est tenu responsable que s'il n'a pas respecté les obligations prévues par le RGPD** qui incombent spécifiquement au sous-traitant ou qu'il **a agi en dehors des instructions licites du traitement** ou contraire à celle-ci (art. 28, § 3).

D. LE SOUS TRAITANT : OBLIGATIONS

Le contrat ou l'acte juridique qui lie le responsable de traitement et le sous-traitant doit en outre prévoir que le sous-traitant :

- Ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis (Art 28 §3, a)).
- Veille à ce que les personnes autorisées à traiter les données à caractère personnel respectent la confidentialité (Art 28 §3, b)).
- Prend toutes les mesures requises en matière de sécurité des traitements (Art 28 §3, c)).
- Aide le responsable du traitement au respect du RGPD (Art 28 §3, d) à h))

Exemple: Respect du droit des personnes concernées

(*Protection des données personnelles*, Obligations au sein de l'Union, Obligations générales, Editions Législatives, 2017)

E. ACTIONS EN JUSTICE

- **Responsabilité *in solidum*** du responsable de traitement et du sous-traitant lorsqu'ils participent au même traitement en cas de dommage causé. (Art 26)

- Une **action récursoire** est possible pour le responsable ayant réparé totalement le dommage causé par tous les responsables de celui-ci (Art 26).

❑ En résumé

La responsabilité de la collecte inclut :

➢ Le responsable de traitement (Art 24).

➢ Le ou les sous-traitant(s), à travers ses obligations (Art 28):

- Traitement des données personnelles uniquement sur instruction (Art 28 §3, a)).
- Respect de la confidentialité (Art 28 §3, b)).
- Mesures en matière de sécurité des traitements (Art 28 §3, c)).
- Aide le responsable du traitement au respect du RGPD ((Art 28 §3, d) à h))

➢ Responsabilité *in solidum et action récursoire (Art 26).*

VI

LES AMENDES ADMINISTRATIVES ET SANCTIONS

A. LES AMENDES ADMINISTRATIVES, Art 82 § 2

- **Pour imposer une amende administrative et décider de son montant en cas de non respect du règlement** ayant causé un dommage matériel ou moral, l'autorité de contrôle doit notamment tenir compte de :

  - la nature, la gravité et la durée de la violation, compte tenu de
  - la nature, de la portée ou de la finalité du traitement concerné, ainsi que
  - du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi.

A. LES AMENDES ADMINISTRATIVES, Art 82 § 2

- En fonction des articles du règlement en infraction, des amendes administratives pourront s'appliquer pour un montant allant de **10 à 20.000.000 euros** ou, dans le cas d'une entreprise, de **2 à 4 % du chiffre d'affaires annuel mondial** total de l'exercice précédent, le montant le plus élevé étant retenu (RGPD, art 83).

B. LES SANCTIONS ÉTAT PAR ÉTAT, Art 83

- **Pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83,** il incombe aux Etats membres de déterminer le régime des autres sanctions applicables.

- **Chaque Etat membre doit notifier à la Commission** les dispositions légales qu'il va adopter au plus tard le 25 mai 2018 et toute modification ultérieure les concernant.

- **Toutes amendes ou sanctions doivent être effectives, proportionnées et dissuasives.**

❑ En résumé

- Les conséquences du non respect au RGPD:
  - ✓ Les amendes administratives (Art 82 §2).
  - ✓ Les sanctions étatiques (Art 83).
- Toutes amendes ou sanctions doivent être effectives, proportionnées et dissuasives (Art 83 §1).

VII

LES RECOMMANDATIONS

VII. LES RECOMMANDATIONS

Points d'attention, quels que soient les traitements de données:

- Assurez-vous que seules les données strictement nécessaires à la poursuite de vos objectifs sont collectées et traitées.
- Identifiez la base juridique sur laquelle se fonde votre traitement (consentement, contrat, obligation légale).
- Révisez vos mentions d'information.
- Vérifiez que vos sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités.
- Prévoyez les modalités d'exercice des droits des personnes concernées.
- Vérifiez les mesures de sécurité mises en place.

QUI?

Inscrivez dans le registre les coordonnées des responsables du traitement + DPO + sous traitant.

QUOI?

Identifiez les données personnelles + particulières.

JUSQU'À QU'AND ?

Indiquez, pour chaque catégorie de données, combien de temps vous les conservez.

POURQUOI?

Indiquez la ou les finalité(s) de la collecte du traitement.

COMMENT?

Précisez les mesures de sécurité mises en œuvre.

Où?

Déterminez le lieu où les données sont hébergées.
+ les pays où elles sont transférées.

VIII

PRIVACY BY DESIGN + LEGAL DESIGN

VIII. PRIVACY BY DESIGN + LEGAL DESIGN

PRIVACY BY DESIGN + LEGAL DESIGN:

- Confiance
- Transparence
- Politique vertueuse (pas de vente des data)
- Conformité

→ Contrainte devenu un avantage en mettant en valeur les données personnelles du client et lui donner la possibilité d'être pro actif.

A. PRIVACY BY DESIGN

La tenue d'un registre des traitements permet de faire le point. Il faut, au préalable, recenser précisément:

- Les différents traitements de données personnelles.
- Les catégories des données personnelles traitées.
- Les objectives poursuivis par les opérations de traitement des données.
- Les acteurs (internes ou externes) qui traitent ces données et identifier les prestataires sous-traitants.
- Les flux en indiquant l'origine et la destination des données afin d'identifier les éventuels transferts de données hors UE.

Recommendations de la Cnil

B. LEGAL DESIGN

- CGV / CGU
- POLITIQUE DE CONFIDENTIALITÉ ET DE COOKIES
- MENTIONS LÉGALES, ETC

BONDARD

Protect & Develop

Maître Céline Bondard

Cabinet Bondard

Avocat aux Barreaux de Paris et New York

P.: +33 (0)6 19 41 31 52

cb@bondard.fr

www.bondard.fr