Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

Introduction to the GDPR, obligations of parties and data transfers

Debora Cohen

Martinique, 2 June 2023

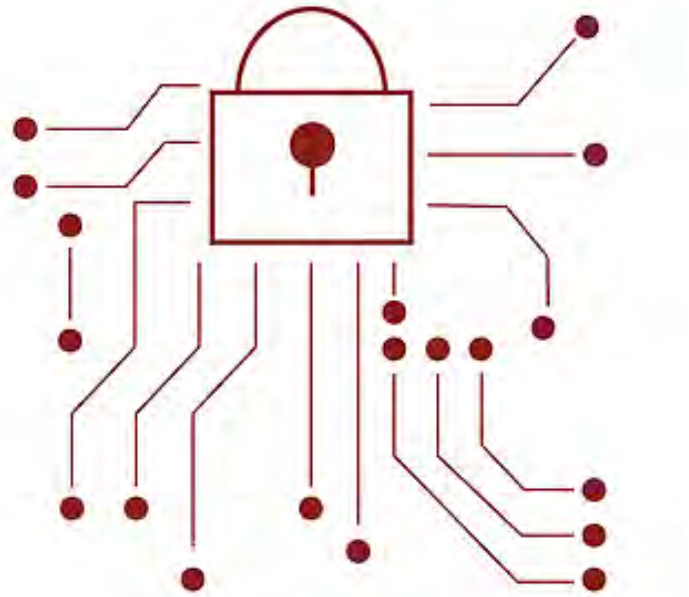
The project is co-financed with the support of the European Union's Justice programme

Le droit européen de la protection des données

AVOCAT

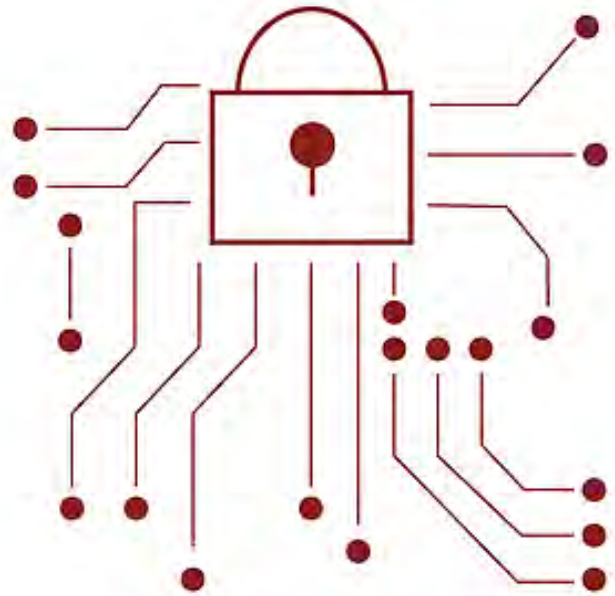
AVOCATS BARREAU • PARIS

Présentation générale du RGPD



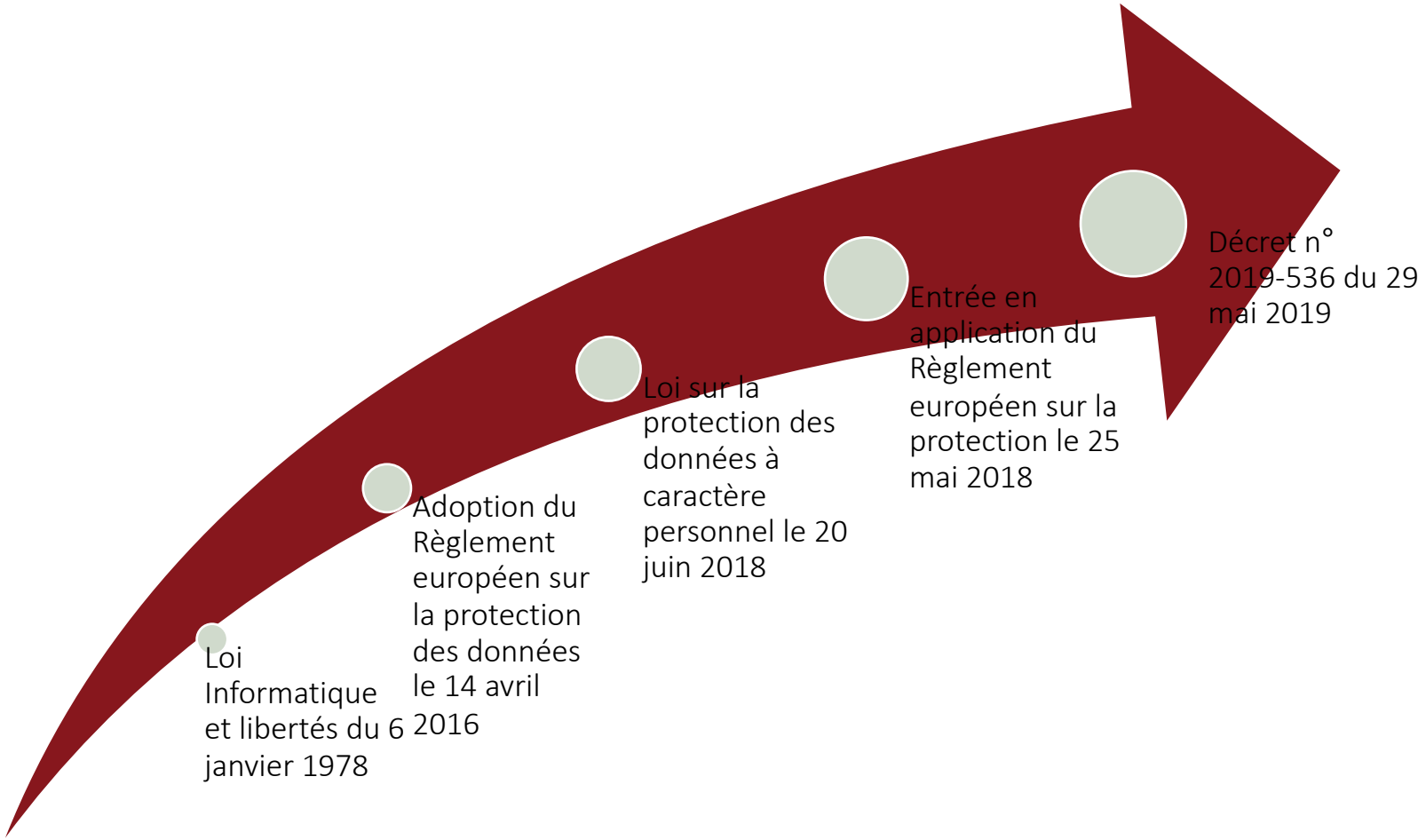
Présentation générale du RGPD

1. Historique de la réglementation en matière de protection des données personnelles
2. Qu'est-ce que le règlement général sur la protection des données ?
3. Quels sont les objectifs du RGPD ?
4. Les notions clés du RGPD
5. La notion de données personnelles
6. Les catégories des données personnelles
7. Le cas des données sensibles
8. Le traitement de données personnelles
9. Les acteurs
10. Un acteur incontournable : La Cnil l'autorité de contrôle
11. Mini QCM



Présentation générale du RGPD

1. Historique de la réglementation en matière de protection des données personnelles



2. Qu'est-ce que le règlement général sur la protection des données ?

Plus connu sous le nom de « RGPD », c'est le texte de référence pour les organismes afin d'assurer la mise en conformité de leur activité.

Ce texte européen s'inscrit dans la continuité de la loi Informatique et Libertés de 1978. Il a été adopté le 14 avril 2016 et est entré en application le 25 mai 2018.

Il a conduit à renforcer les droits des personnes physiques et à responsabiliser les acteurs traitant des données personnelles !

3. Quels sont les objectifs du RGPD ?

1. **Harmoniser la protection des données personnelles dans l'Union Européenne.**

Le RGPD est directement applicable dans l'ensemble des Etats membres de l'Union Européenne (UE), harmonisant ainsi la protection des données personnelles dans l'UE.

2. **Responsabiliser les acteurs qui traitent des données personnelles.**

L'organisme doit, à tout moment, être en mesure de prouver sa conformité au RGPD (à l'aide de politiques, procédures, contrôles, formations, …)

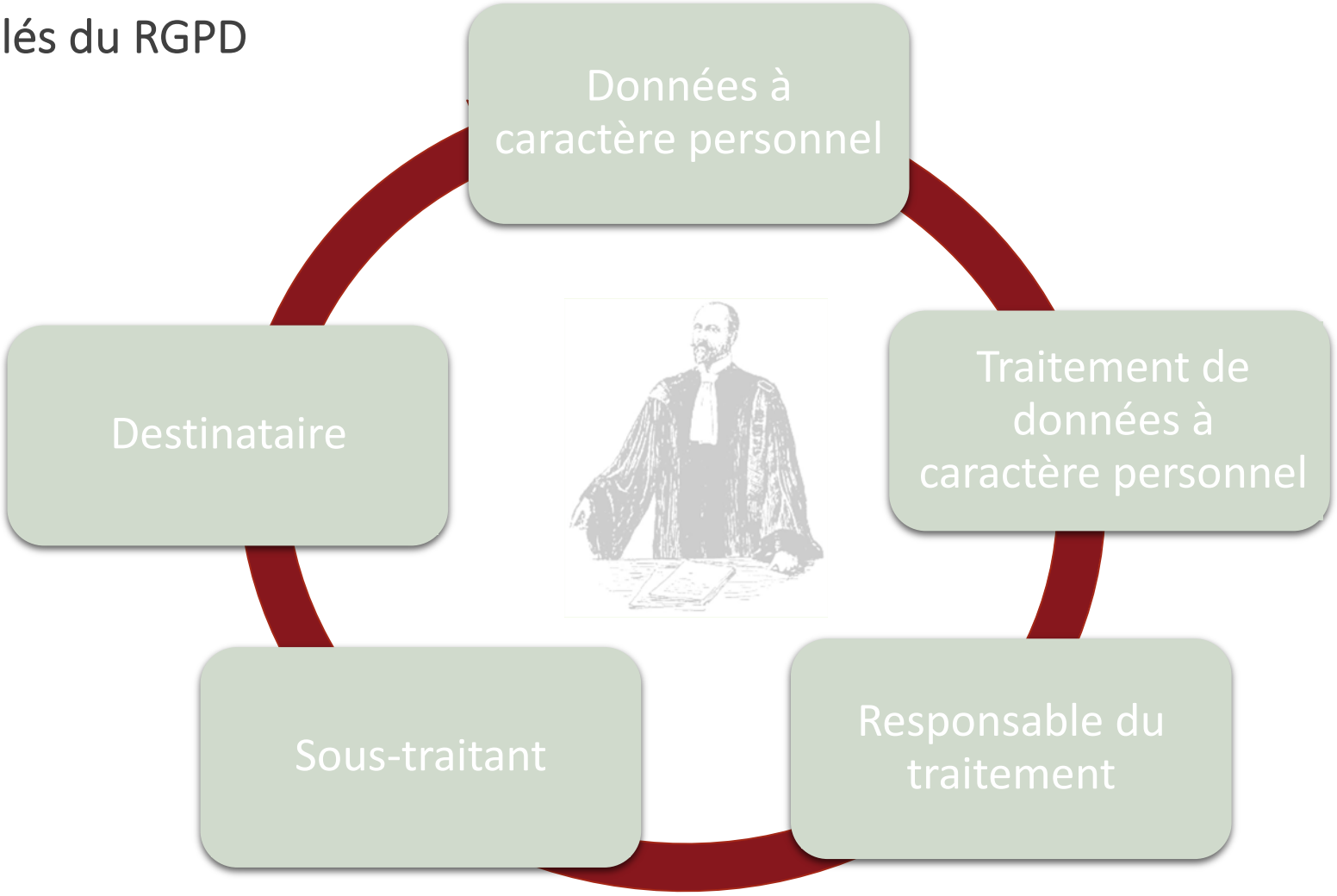
3. **Renforcer les droits des personnes concernées**

Le RGPD renforce les droits préexistants des personnes (droit d'accès, d'opposition, de rectification) et en crée de nouveaux (droit à la limitation, à la portabilité, …)

4. **Sanctionner la non conformité**

La Cnil est désormais en mesure de sanctionner un organisme à hauteur de 20 000 000 € en cas de non respect des dispositions du RGPD (ou de 4% du chiffre d'affaire annuel mondial consolidé, le montant le plus élevé étant retenu).

4. Les notions clés du RGPD



5. La notion de données personnelles

- Qu'est ce qu'une donnée personnelle ?

Une donnée à caractère personnel est toute information se rapportant à une personne physique (un client, un salarié, un prestataire, …) identifiée ou identifiable, directement ou indirectement

Identification Directe	Identification Indirecte	Croisement de données
• Nom • Prénom	• Numéro de téléphone • Numéro de sécurité sociale	• Adresse + Date de naissance + abonnement au magazine Y = Madame Dupont Dupond

6. Les catégories des données personnelles

Données relatives à l'identité	Données relatives à la vie personnelle	Données relatives à la vie professionnelle	Informations économiques	Données de localisation	Données sensibles
• Nom • Prénom • Date de naissance • Adresse • Lieu de naissance • Photo etc	• Situation familiale • Nombre d'enfants	• CV • Diplôme • Lieu de travail • Formation • Poste occupé	• Revenus • Fiche d'imposition • Donnée bancaires • Situation financières	• Coordonnées GPS • Géolocalisation du véhicule • Géolocalisation du téléphone	• Données de santé • Données raciales • Données politiques etc

7. Le cas des données sensibles

Certaines données personnelles sont qualifiées de **« particulières»** par le RGPD : le traitement de ce type de données est, par principe et sauf exception, **interdit**.

Origine raciales ou ethniques	• « d'origine turc » • « couple d'espagnol »
Opinions politiques	• « Maire LREM » • « Sympathisant les verts »
Convictions religieuses ou philosophiques	• « Franc-maçon » • « est en pèlerinage à Lourdes »
Appartenance syndicales	• « CFDT » • « syndiqué FO »
Données génétiques ou biométriques	• Analyse de l'ADN • Empreintes digitales comme mode d'identification
Données sur la vie ou l'orientation sexuelle	• « Couple homosexuelle » • « a deux femmes »
Données de santé	• « Bipolarité » • « a une tumeur »

8. Le traitement de données personnelles

- Qu'est ce qu'un traitement de données personnelles ?

La notion de traitement de données personnelles est définie à l'article 4 du RGPD et fait référence à toutes les opérations qui visent à collecter, enregistrer, extraire, communiquer, organiser, conserver, adapter, modifier ou utiliser ces données

Traitement de données personnelles	Ø Traitement de données personnelles
• Collecter des données dans le cadre d'une demande d'abonnement téléphonique • Gérer la paie des salariés	• Compiler des données chiffrées

9. a) Les acteurs

Personne concernée

- Les personnes dont les données font l'objet d'un traitement

Responsable du traitement

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

9. b) Les acteurs

Sous-traitant

- Règlement européen
- « 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;»

Destinataire

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

10. Un acteur incontournable : La Cnil l'autorité de contrôle

Informer et Protéger	Accompagner et Conseiller	Anticiper et innover	Contrôler et sanctionner
La Cnil informe les particuliers et professionnels de leurs droits et répond à leur demande. La Cnil protège les citoyens en étudiant et en répondant à leur plainte	La Cnil accompagne les organismes dans leur mise en conformité au RGPD via des avis, guide, référenciel, communiqué publié sur son site	Pour anticiper et innover, la Cnil est a créée : - Le Laboratoire d'innovation numérique de la CNIL : un espace éditorial traitant de sujets d'actualité sous l'angle « protection des données » ; - Un Comité de Prospective chargé de soutenir et renforcer sa mission de veille, dans un espace d'échanges et de réflexion sur les libertés individuelles et la vie privée dans le monde numérique	La Cnil dispose de la possibilité de contrôler les organismes afin de vérifier leur mise en œuvre de la réglementation sur les données personnelles À ce titre elle peut prononcer différents types de sanctions (mise en demeure, amende etc.)

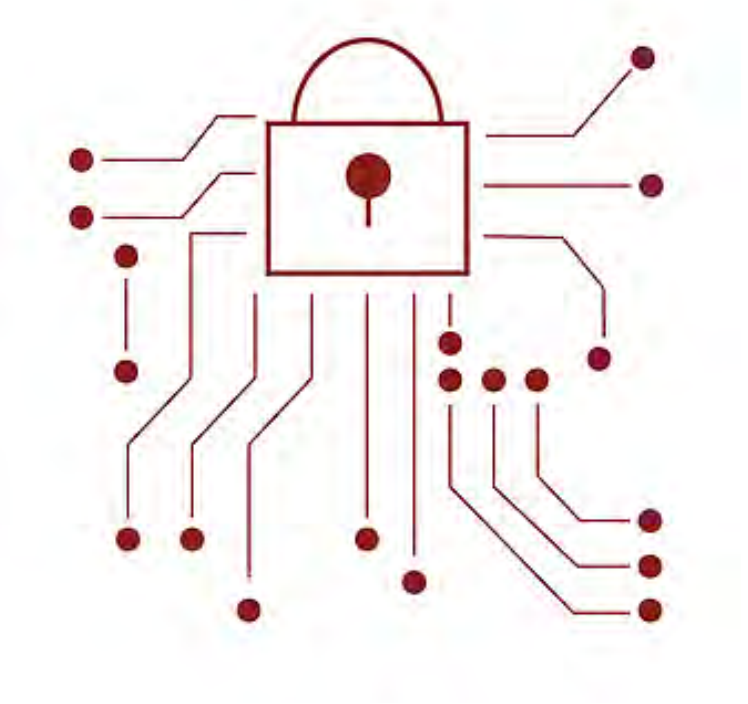
Présentation générale du RGPD

❖ **Mini QCM**

N°	QUESTIONS	Vrai	Faux
1	Le RGPD est le premier texte de référence en matière de protection des données en France.		
2	Le RGPD est entré en application le 25 mai 2020.		
3	Un lieu de travail est une donnée personnelle.		
4	L'appartenance syndicale est une donnée sensible.		
5	La Cnil peut prononcer une sanction allant jusqu'à 10% du chiffre annuel mondial d'une entreprise.		

Des questions ?

Le responsable du traitement et le sous-traitant



Les obligations du responsable du traitement et du sous-traitant

1. Responsable du traitement et sous-traitant : définitions
2. Le respect de principes fondamentaux
3. L'exactitude des données
4. D'autres principes essentiels
5. La sécurité et la gestion des violations de données
6. La notification d'une violation à la Cnil
7. Les obligations du responsable du traitement
8. Les obligations du sous-traitant
9. La sous-traitance, des garanties suffisantes
10. Registre des traitements du sous-traitant
11. Les responsabilités du responsable du traitement et du sous-traitant
12. Les sous-traitants secondaires
13. En bref : Garantir la conformité de mes sous-traitants au RGPD
14. La réalisation d'un accord sur la protection des données (DPA)

Mini cas pratique

Les obligations du responsable du traitement et du sous-traitant

1. Responsable du traitement et sous-traitant : définitions

Les responsables du traitement utilisent les données pour eux-mêmes !

Responsable du traitement

Chaque organisation est un responsable du traitement

= personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou des États membres, le responsable du traitement ou les critères spécifiques pour sa désignation peuvent être prévus par le droit de l'Union ou des États membres.

Le sous-traitant traite des données pour le compte de quelqu'un d'autre, généralement contre rémunération !

Sous-traitant

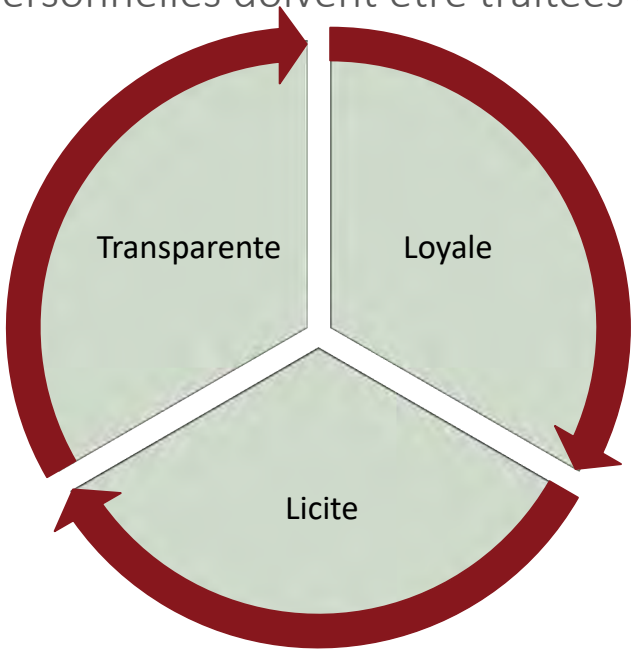
= personne physique ou morale, une autorité publique, une agence ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Les obligations du responsable du traitement et du sous-traitant

2. Le respect de principes fondamentaux

Du fait de sa qualité, un certain nombre d'obligations pèsent sur le responsable du traitement. Il est le garant de la mise en œuvre des « mesures techniques et organisationnelles appropriées » qui permettent d'assurer la conformité du traitement au règlement.

L'article 5 du RGPD énonce que les données personnelles doivent être traitées de manière licite, loyale et transparente !



Les obligations du responsable du traitement et du sous-traitant

Principe de licéité

Tout traitement de données à caractère personnel doit s'effectuer selon les 6 bases légales prévues par l'article 6 du RGPD.

Une attention particulière doit être donnée aux données sensibles.

Principe de proportionnalité

= Minimisation et exactitude des données

= Limitation de la durée de conservation

Principe de limitation des finalités du traitement

Un traitement de données à caractère personnel doit toujours être déterminé, explicite et légitime.

Les obligations du responsable du traitement et du sous-traitant

3. L'exactitude des données

L'exactitude des données → toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes soient effacées ou rectifiées sans tarder

Exemple : Une société de télécommunication a développé une application lui permettant de traiter de manière automatisée les demandes d'identification provenant de la Hadopi ou des services de police ou de gendarmerie. Or, l'application ne parvenant pas à détecter la personne associée à l'adresse IP, un client de la société de télécommunication fut identifié par défaut par l'application.

La société a donc porté plainte contre le client qui c'était vu attribuer à 1531 reprises en 2013 des adresses IP non identifiées par l'application informatique.

Dans ce cas d'espèce, la Cnil a constaté que la société n'avait pas respecté son obligation légale de transmettre des données exactes à la gendarmerie notamment.

Les obligations du responsable du traitement et du sous-traitant

4. D'autres principes essentiels

Principe de « Privacy by design »

Ce principe repose sur une prise en compte des aspects de protection des données dès la conception du produit ou service qui va être poursuivie tout le long de son cycle.

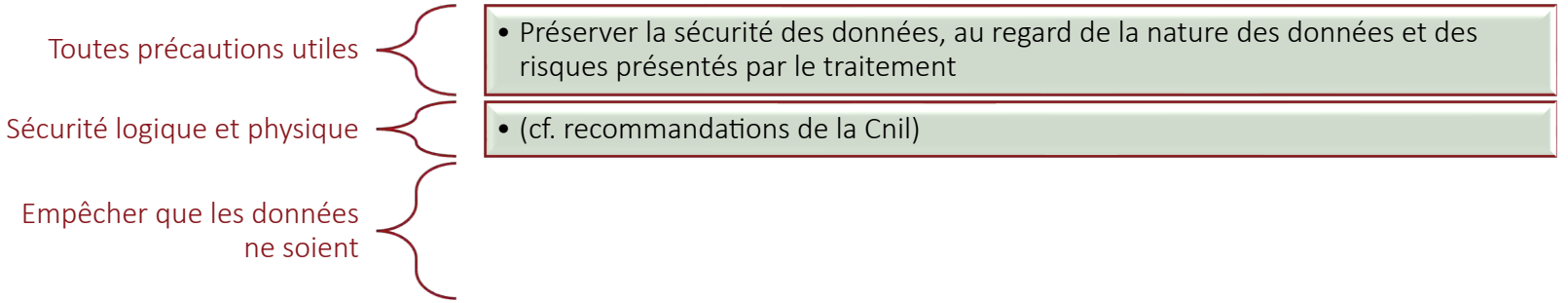
Principe de « Privacy by default »

Ce principe repose sur des mesures techniques et organisationnelles appropriées pour garantir que par défaut seules les données qui sont nécessaires au regard de la finalité du traitement sont traitées.

La « Privacy Impact Assessment »

Ce principe repose sur la réalisation d'une analyse d'impact lorsque certains traitements de données personnelles présentent un risque élevé pour les droits et libertés des personnes concernées

Les obligations du responsable du traitement et du sous-traitant



Les obligations du responsable du traitement et du sous-traitant

5. b) La sécurité et la gestion des violations de données

Gérez les habilitations et sensibilisez les utilisateurs

- définissez des profils d'habilitation
- supprimez les permissions d'accès obsolètes
- documentez les procédures d'exploitation

Authentifiez les utilisateurs

- définissez un identifiant (login) unique à chaque utilisateur
- adoptez une politique de mot de passe utilisateur rigoureuse
- obligez l'utilisateur à changer son mot de passe régulièrement

Sécurisez les postes de travail

- limitez le nombre de tentatives d'accès à un compte
- installez un « pare-feu » (firewall)
- utilisez des antivirus régulièrement mis à jour
- prévoyez une procédure de verrouillage automatique de session

Sauvegardez et prévoyez la continuité d'activité

- effectuez des sauvegardes régulières
- stockez les supports de sauvegarde dans un endroit sûr
- chiffrez les sauvegardes

Sécurisez l'informatique mobile

- prévoyez des moyens de chiffrement pour les ordinateurs portables et les unités de stockage amovibles (clés USB, CD, DVD…)

5. c) La sécurité et la gestion des violations de données

Art. 4 al. 12 du RGPD :

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

Les obligations du responsable du traitement et du sous-traitant

6. La notification d'une violation à la Cnil

Une violation de données personnelles se comprend comme une atteinte à (critères non cumulatifs) :

1. la CONFIDENTIALITÉ : un tiers non autorisé a accès à la donnée *(ex : un agent territorial communique par erreur un fichier contenant une base de données d'administrés à un tiers non autorisé.)*

2. l'INTÉGRITÉ : la donnée a été altérée *(ex. : un hacker s'introduit dans le système d'information RH et modifie les salaires de l'ensemble des agents territoriaux) ;*

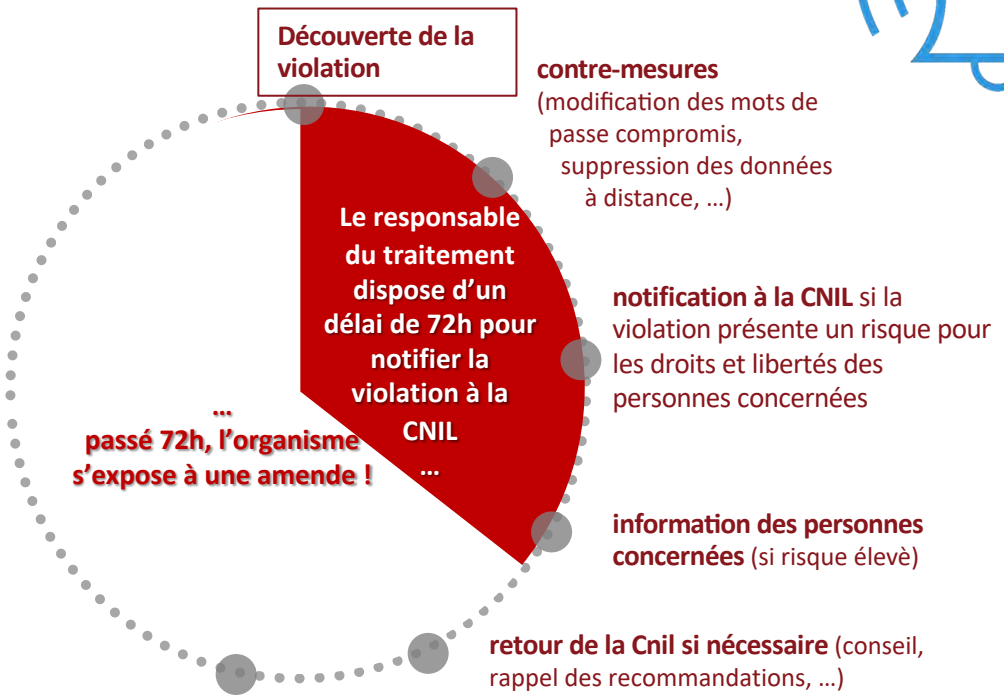
3. la DISPONIBILITÉ : la donnée n'est plus accessible *(ex.: un agent territorial supprime accidentellement une partie de la base de données d'un service public, non sauvegardée par ailleurs, ne permettant plus l'utilisation des applicatifs de gestion.) ;*

Afin de protéger les administrés, ses agents territoriaux et se conformer à la réglementation, la collectivité a mis en place des mesures visant à :

- PRÉVENIR d'éventuelles violations de données *(détections informatiques automatisées, sensibilisations des collaborateurs, …)* et,

- RÉAGIR de manière appropriée en cas de violation *(processus d'information CNIL en cas de violation, d'information des personnes dont les données ont fait l'objet d'une violation si nécessaire, documentation des violations dans un registre, …)*

Chaque violation de donnée à caractère personnel doit a minima faire l'objet d'une inscription au sein d'un registre prévu à cet effet au sein de la collectivité



Les obligations du responsable du traitement et du sous-traitant

7. Les obligations du responsable du traitement

Le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD.

Le responsable du traitement énonce au sous-traitant des instructions documentées pour réaliser un traitement de données à caractère personnel conforme au RGPD.

Le responsable du traitement est tenu à une obligation de collecte licite des données.

Le responsable du traitement est tenu de préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Les obligations du responsable du traitement et du sous-traitant

8. Les obligations du sous-traitant

Article 28 RGPD

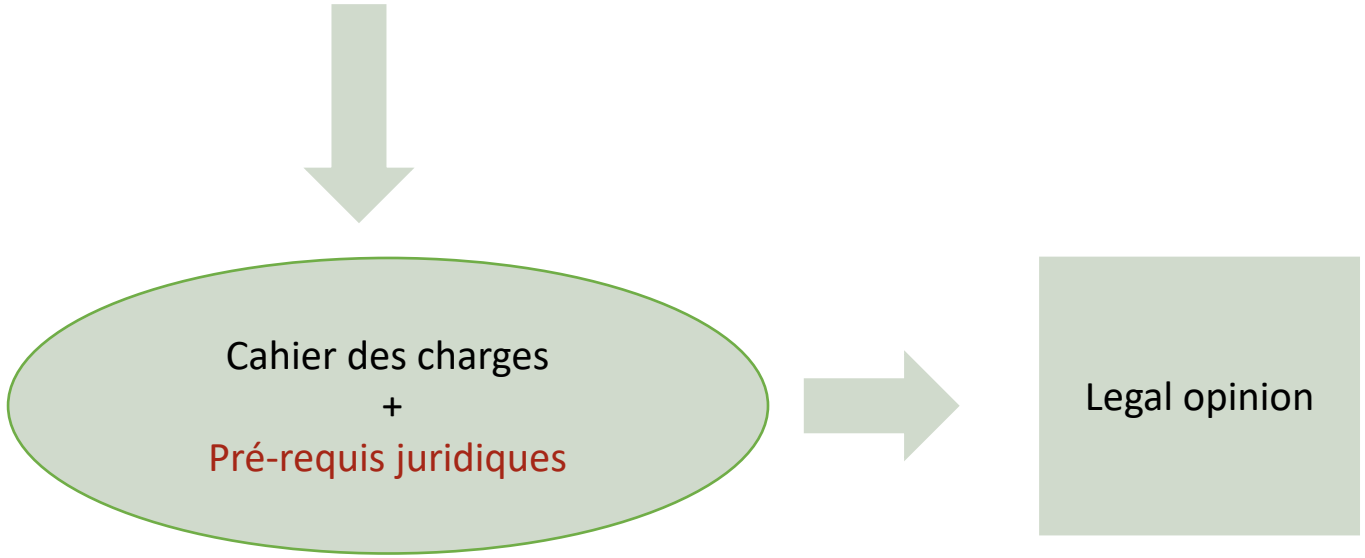
Garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles	Autorisation écrite préalable, spécifique ou générale du responsable de traitement pour le recrutement d'un autre sous-traitant par le sous-traitant	Obligation de confidentialité
Traitement des données sur instruction documentée du responsable de traitement	**Encadrement par un contrat ou autre acte juridique liant le sous-traitant au responsable de traitement**	Respecte les exigences de sécurité du règlement
Aide le responsable de traitement pour donner suite aux demandes d'exercice des droits des personnes concernées	Suppression ou renvoi des données au responsable de traitement au terme de la prestation (sauf si le droit de l'UE ou de l'Etat membre exige la conservation des données)	Mise à disposition du responsable de traitement des informations nécessaires pour apporter la preuve du respect de ses obligations et permettre la réalisation d'audits

9. La sous-traitance, des garanties suffisantes

Article 28

Article 28 du RGPD :

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 présent règlement et garantisse la protection des droits de la personne concernée.



10. Registre des traitements du sous-traitant

Article 30

Article 30 du RGPD : Registre des activités de traitement

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

a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données;
b) les catégories de traitements effectués pour le compte de chaque responsable du traitement;
c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;
d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

5. Les obligations visées aux paragraphes 1 et 2 ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

Les obligations du responsable du traitement et du sous-traitant

11. Les responsabilités du responsable du traitement et du sous-traitant

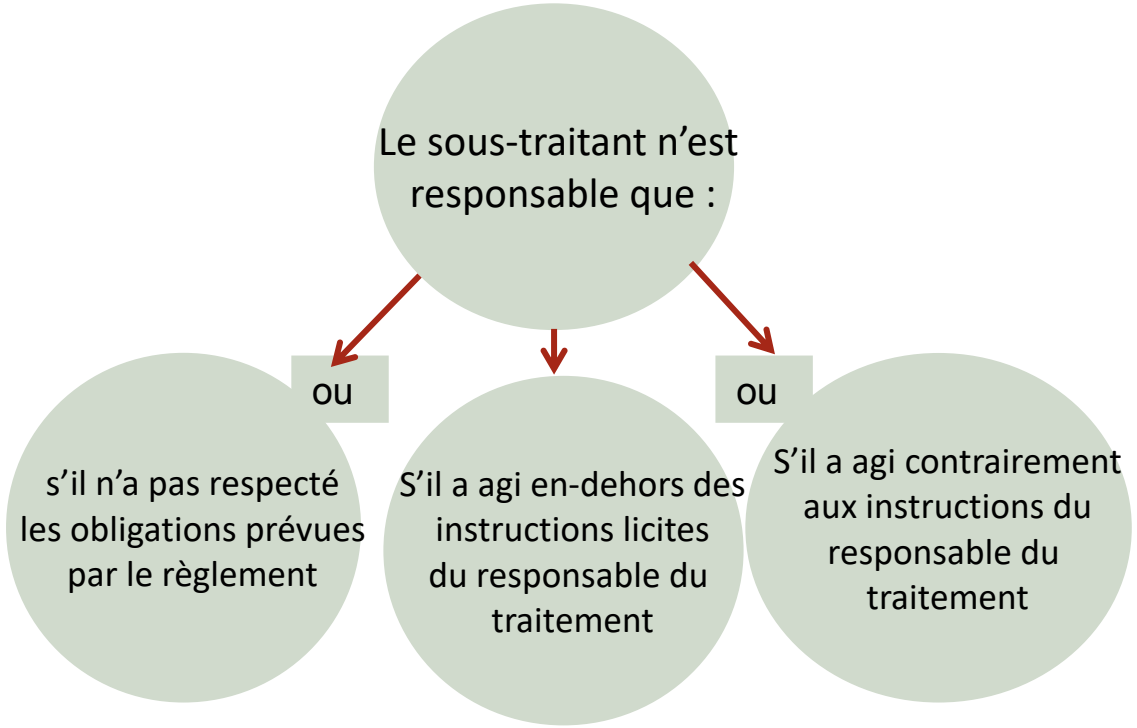
Article 82 RGPD

Le responsable du traitement est responsable en cas de manquement au RGPD survenu lors d'un traitement de données à caractère personnel

Responsabilité pour :

- Norme adéquate de protection des données (32 RGPD) ;
- Le sous-traitant est responsable devant l'autorité de contrôle ainsi que devant les personnes concernées dont il traite les données pour le compte du responsable du traitement ;
- Légalité des instructions du responsable du traitement ;
- Documentation des instructions du responsable du traitement;
- Appropriation des données = "marche" dans la sphère d'autorité du responsable du traitement

Le RGPD ne fait pas de différence entre un sous-traitant direct et un sous-traitant secondaire = responsabilité tout au long de la chaîne de traitement.



Les obligations du responsable du traitement et du sous-traitant

Article 28 RGPD

Attention

La responsabilité du sous-traitant

h) Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union relatives à la protection des données

=

Vérifier la légalité des instructions

Les obligations du responsable du traitement et du sous-traitant

12. Les sous-traitants secondaires

Article 28 RGPD

I – Autorisation écrite générale

c'est-à-dire pour une mission globale

II – Autorisation écrite spécifique

c'est-à-dire pour mener des activités de traitement spécifiques

Le sous-traitant informe le responsable de tout changement (ajout / remplacement d'autres sous-traitants)

Possibilité d'objections

Le sous-traitant secondaire a les mêmes obligations en matière de protection de données que celles fixées dans le contrat entre le responsable de traitement et le sous-traitant.

Le sous-traitant initiale « demeure pleinement responsable »

Les obligations du responsable du traitement et du sous-traitant

13. En bref : Garantir la conformité de mes sous-traitants au RGPD

Dans le cadre de ses activités, un responsable du traitement peut déléguer le traitement de données personnelles à un sous-traitant qui va traiter des données pour son compte

1 Déterminer si le sous-traitant traitera des données personnelles.

La première étape consiste à savoir si le responsable du traitement **envoie des données personnelles** au sous-traitant, si lui-même **accède à des données personnelles** détenues par le responsable du traitement ou s'il **collecte des données personnelles** pour le compte du responsable du traitement. Si la réponse est « oui », étape 2 !

2 Evaluer le sous-traitant et identifier les traitements sous-traités.

L'objectif est de déterminer si le **sous-traitant est respectueux des exigences du RGPD** (un DPO a-t-il été nommé, quelles sont les mesures de sécurité et de confidentialité en place, …) et d'identifier les traitements que celui-ci réalisera pour le compte du responsable du traitement.

Le RGPD instaure un principe de coresponsabilité : le responsable du traitement est responsable en cas de problèmes découlant du non-respect du RGPD par son sous-traitant !

3 Contractualiser la relation avec le sous-traitant

Un **contrat doit obligatoirement être signé** entre le responsable du traitement et le sous-traitant (comprenant des clauses spécifiques prévues par le RGPD) afin d'encadrer l'utilisation des données personnelles par le sous-traitant.

Sauf cas spéciaux, le responsable du traitement demeure pleinement responsable en cas de manquement au RGPD par son sous-traitant (20 millions d'€ d'amende)

14. La réalisation d'un accord sur la protection des données (DPA)

Quelques clauses à insérer dans le DPA

- Obligations du responsable du traitement
- Obligations du sous-traitant
- **Confidentialité de l'accord**
- Règles concernant les sous-traitants ultérieurs
- **Le transfert des données**
- Règles concernant les violations de données à caractère personnel et annexe sécurité
- Annexe sur le détail des traitements de données

❖ Mini cas pratique : le responsable du traitement et le sous-traitant

Le responsable du traitement est la personne qui détermine les finalités et les moyens du traitement. C'est celui qui décide du « pourquoi » et du « comment » les données sont traitées.

Exemple : Un restaurant compte trois salariés. Le propriétaire du restaurant décide de signer un contrat avec une entreprise X spécialisée dans le traitement de la paie pour le versement du salaire de ses employés. Le propriétaire du restaurant fournit toutes les informations nécessaires à l'établissement de la fiche de paie et au versement du salaire (date, montant, poste occupé etc).

Dans cette situation, qui est le responsable du traitement ?

Y a-t-il un sous-traitant ?

❖ Mini cas pratique : le responsable du traitement et le sous-traitant

Le responsable du traitement est la personne qui détermine les finalités et les moyens du traitement. C'est celui qui décide du « pourquoi » et du « comment » les données sont traitées.

Exemple : Un restaurant compte trois salariés. Le propriétaire du restaurant décide de signer un contrat avec une entreprise X spécialisée dans le traitement de la paie pour le versement du salaire de ses employés. Le propriétaire du restaurant fournit toutes les informations nécessaires à l'établissement de la fiche de paie et au versement du salaire (date, montant, poste occupé etc).

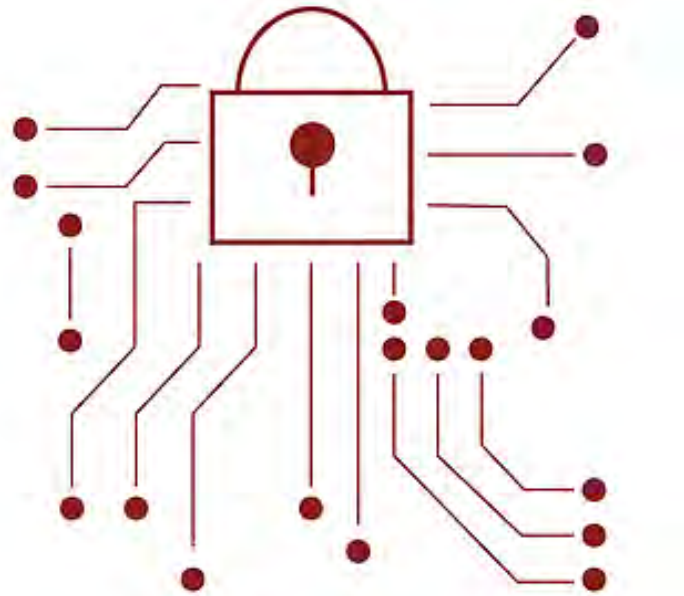
Dans cette situation, qui est le responsable du traitement ?

Y a-t-il un sous-traitant ?

Le propriétaire du restaurant est le responsable du traitement et l'entreprise X est le sous-traitant !

Des questions ?

Transferts de données à caractère personnel vers des pays tiers



Transferts de données à caractère personnel vers des pays tiers

1. Qu'est-ce qu'un transfert de données en dehors de l'UE ?
2. Principe de territorialité
3. Que faire si les données sortent en dehors de l'UE ?
4. Base des transferts vers des pays tiers avec l'article 45 du RGPD
5. Base des transferts vers des pays tiers avec l'article 46 du RGPD
6. Motifs supplémentaires de transfert vers des pays tiers avec l'article 49 du RGPD
7. Transmission réellement spécifique avec l'article 49, paragraphe 2, du RGPD
8. Le transfert des données vers le Royaume-Uni depuis le Brexit
9. L'arrêt Schrems II
10. Le rôle du CEPD
11. En résumé

Mini QCM

Transferts de données à caractère personnel vers des pays tiers

1. Qu'est-ce qu'un transfert de données en dehors de l'UE ?

= tout transfert de données à caractère personnel qui est activement mis à la disposition d'un nombre limité de parties ou de parties identifiées à la connaissance du cédant ou dans l'intention de permettre au destinataire d'accéder aux données à caractère personnel

Transfert de données vers des pays tiers

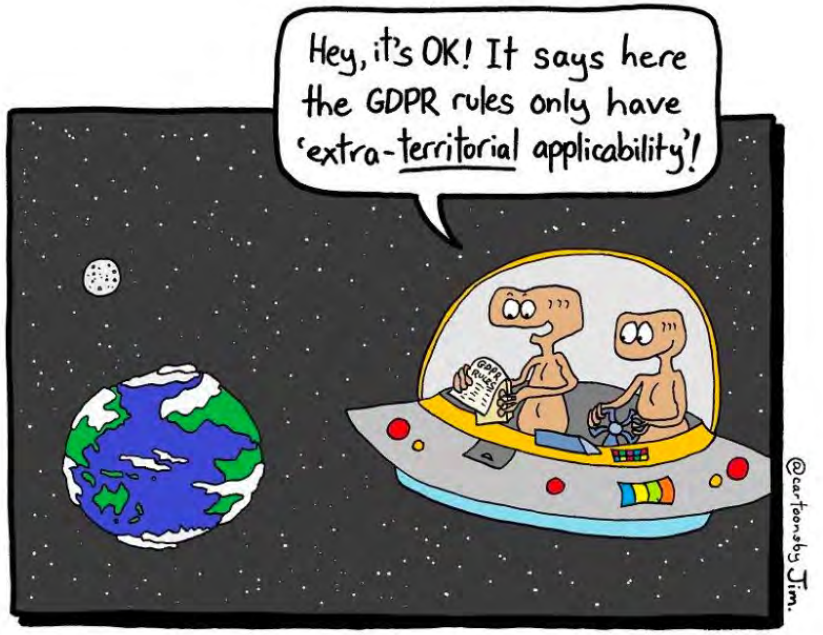
Transfert de données en dehors de la frontière sécurisée de l'Espace économique européen

Transferts de données à caractère personnel vers des pays tiers

2. Principe de territorialité

- Libre circulation des données au sein de l'Espace économique européen ;
- Pas de réglementation spécifique pour les transferts à l'intérieur de l'EEE ;
- Transfert de données = traitement des données
- Transferts de données en dehors de l'EEE = transfert de données vers des pays tiers et des organisations internationales.

Transferts de données en dehors de l'EEE : une approche en deux étapes : Obligations générales + obligations supplémentaires prévues au chapitre V du RGPD



Transferts de données à caractère personnel vers des pays tiers

3. Que faire si les données sortent en dehors de l'UE ?

Identifier et encadrer les transferts de données hors Union européenne

Transferts assortis d'une décision relative au caractère adéquat du niveau de protection

⇩

Transfert libre

(absence d'autorisation particulière)

Transferts moyennant des garanties appropriées

⇩

Transfert libre (absence d'autorisation particulière) dans le cadre de mise en œuvre de garanties appropriées

⇩

Fondement :

- Instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics
- Règles d'entreprises contraignantes (BCR)
- Clauses types de protection des données
- Code de conduite ou mécanisme de certification approuvé ;
- Clauses contractuelles (subordonnées à l'autorisation préalable d'une autorité de contrôle)

Transferts de données à caractère personnel vers des pays tiers

4. Base des transferts vers des pays tiers avec l'article 45 du RGPD

Décisions de la CE :

1. Suisse (2000/518/CE)
2. Canada (2002/2/CE)
3. Argentine (2003/490/CE)
4. Guernesey (2003/821/CE)
5. île de Man (2004/411/CE)
6. Jersey (2008/393/CE)
7. Îles Féroé (2010/146/UE)
8. Andorre (2010/625/UE)
9. Israël (2011/61/UE)
10. Uruguay (2012/484/UE)
11. Nouvelle-Zélande (2013/65/UE)
12. Japon - C(2019) 304
13. République de Corée - C(2021) 9316
14. Royaume-Uni – 28.6.2021

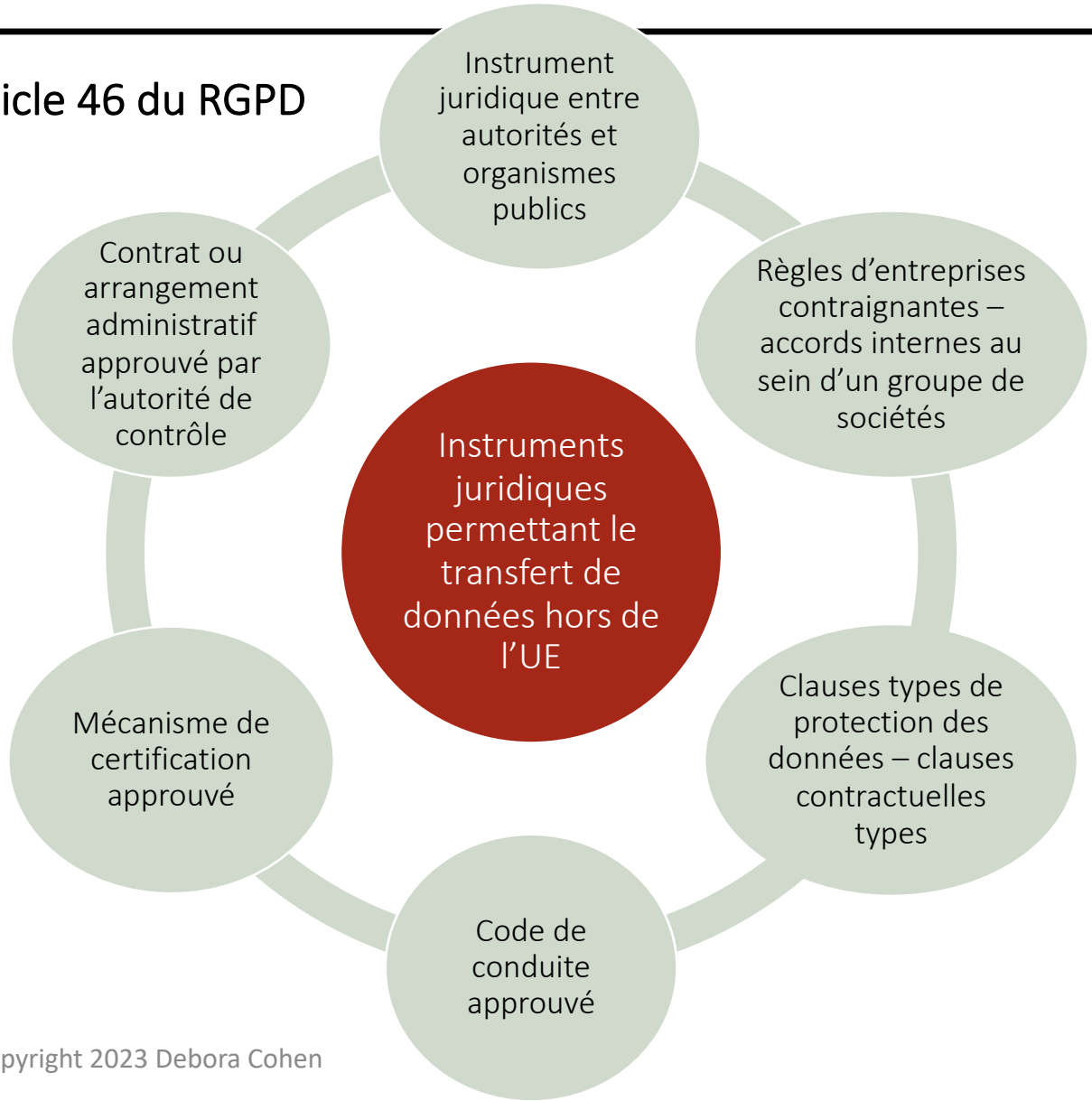
La Commission européenne peut décider que certains pays assurent une protection adéquate des données à caractère personnel.

Transferts de données à caractère personnel vers des pays tiers

5. Base des transferts vers des pays tiers avec l'article 46 du RGPD

Il est possible de transférer des données vers des pays tiers "sous réserve de garanties appropriées", ce qui signifie :

<u>Sur la base des instruments juridiques spécifiques</u>



Transferts de données à caractère personnel vers des pays tiers

6. Motifs supplémentaires de transfert vers des pays tiers avec l'article 49 du RGPD

Motifs spécifiques de transfert de données

- Consentement fondé sur le risque
- Exécution d'un contrat ou pour la conclusion d'un contrat à la demande d'une personne
- Conclusion ou exécution d'un contrat, lorsque cela est dans l'intérêt de la personne concernée, qui n'est pas partie au contrat
- Intérêt public
- Réparation
- Protection des intérêts vitaux d'une personne concernée lorsqu'elle n'est pas en mesure de donner son consentement physiquement ou juridiquement
- Transfert à partir du registre public dans des conditions normales d'accès

Transferts de données à caractère personnel vers des pays tiers

7. Transmission réellement spécifique avec l'article 49, paragraphe 2, du RGPD

Pour bénéficier de l'exportation de données en vertu de l'article 49, paragraphe 2, il faut que :

Le transfert de données peut avoir lieu sur la base de motifs spécifiques qui sont les intérêts légitimes impérieux du responsable du traitement :

1. Le transfert ne soit pas répétitif
2. Le transfert concerne un nombre limité de personne
3. Le transfert soit nécessaire aux fins des intérêts légitimes du responsable du traitement
4. les intérêts, droits et libertés de la personne concernée ne sont pas outrepassés
5. le responsable du traitement a procédé à une évaluation complète de la situation
6. assurer des garanties suffisantes pour la protection des données à caractère personnel
6. Informer l'autorité de contrôle
6. Informer la personne concernée

8. Le transfert des données vers le Royaume-Uni depuis le Brexit

- La Commission européenne a adopté le **28 juin 2021 deux décisions d'adéquation** vis-à-vis du Royaume-Uni - l'une au titre du RGPD et l'autre au titre de la directive en matière de protection des données dans le domaine répressif.

- **Les transferts de données personnelles depuis l'Union européenne vers le Royaume-Uni peuvent donc s'effectuer sans encadrement spécifique,** dans la mesure où la Commission européenne constate par ses décisions que ces données bénéficient d'un niveau de protection substantiellement équivalent à celui garanti en vertu de la législation de l'Union.

- En pratique, les flux de données personnelles depuis l'UE vers le Royaume-Uni sont bien considérés comme des transferts vers un pays tiers, mais les responsables du traitement et sous-traitants peuvent librement mettre en œuvre ces traitements, sans garanties ou conditions supplémentaires.

Transferts de données à caractère personnel vers des pays tiers

9. L'arrêt Schrems II

Maximilian Schrems, initiateur de l'arrêt annulant les décisions des programmes Safe Harbour (2015) et Privacy Shield (2020)

Arrêt de la CJUE C-311/18 du 16.07.2020 dit Schrems II

La CJUE invalide le Privacy Shield (absence de garanties procédurales pour les personnes non américaines soumises à une surveillance électronique de masse).

La CJUE laisse en place les clauses contractuelles types .... mais il n'est pas nécessairement légal de transférer des données sur la base des clauses contractuelles types - plus de signature mécanique des clauses contractuelles types en raison du risque d'écoute par la NSA.

Depuis le 27 décembre 2022, les anciennes clauses contractuelles types ne peuvent plus être utilisées = seules les CCT mises à jour en 2021, ou l'utilisation d'un autre outil de transfert sont valables.

Transferts de données à caractère personnel vers des pays tiers

10. Le rôle du CEPD

Le CEPD doit fournir des recommandations pour les garanties fondamentales : Évaluer si la législation du pays de destination nuit à l'efficacité de l'outil de transfert

- Les règles d'accès aux données sont-elles claires ?
- La nécessité et la pertinence de l'accès à des fins légitimes sont-elles assurées ?
- Existe-t-il un mécanisme de contrôle d'accès indépendant ?
- Les personnes disposent-elles d'outils juridiques efficaces ?

Transferts de données à caractère personnel vers des pays tiers

11. En résumé

Identifier les situations dans lesquelles il y a un transfert de données en dehors de l'EEE ; vérifier les contacts avec les contreparties en dehors de l'EEE.

La base la plus pratique pour transférer des données en dehors de l'Union est constituée par les clauses types de protection des données.

Le consentement est une base peu pratique pour l'exportation de données car il peut être révoqué à tout moment.

Le devoir d'information des personnes concernées dont les données sont transférées en dehors de l'EEE existe et lorsque le transfert se fait sur la base de :

- des clauses types de protection des données
- des décisions sur l'adéquation de la protection des données

Transferts de données à caractère personnel vers des pays tiers

❖ **Mini QCM**

N°	QUESTIONS	Vrai	Faux
1	Un transfert de données vers un pays tiers suppose nécessairement un transfert vers un pays hors de l'Espace économique européen.		
2	Le transfert de données au sein de l'Union européenne repose sur des exigences spécifiques.		
3	Un code de conduite peut servir d'instrument juridique permettant le transfert de données en dehors de l'Union européenne.		
4	Un transfert de données hors de l'Union européenne peut être motivé par l'intérêt public.		
5	Le transfert de données vers les Etats-Unis repose sur des garanties suffisantes.		

Des questions ?

Merci pour votre participation

- Site internet : www.dcavocat.com
- P. : +33 (0) 6.50.08.23.47
- Mail : debora.cohen@dcavocat.com

AVOCATS BARREAU • PARIS

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

Principle of consent

Florence Ivanier

Martinique, 2 June 2023

The project is co-financed with the support of the European Union's Justice programme

Sommaire

- Introduction: principe du consentement ou mythe du consentement?

1. La consécration du consentement, corollaire de l'autodétermination informationnelle
2. Le consentement au nombre des 6 bases légales de traitement
3. Caractéristiques et conditions de validité du consentement
4. Caractère libre du consentement: déséquilibre des rapports de force & conditionnalité
5. Protection particulière des mineurs
6. Consentement e-privacy et consentement RGPD

- Conclusion

Content

- *Introduction: principle of consent or myth of consentement?*

1. *The consecration of consent, a corollary of informational self-determination*
2. *Consent is one of the 6 legal bases for processing*
3. *Characteristics and conditions of validity of consent*
4. *Focus on a consent freely given: power imbalance & conditionality*
5. *E-privacy consent and GDPR consent*

- *Conclusion*

Introduction

Principe du consentement ou mythe du consentement?

- un recours souvent excessif à l'utilisation du consentement
- il peut se révéler contre-productif de s'appuyer sur le consentement

⇒ Le responsable de traitement doit vérifier si le recours à cette base légale est pertinent

Art. 4 du RGPD : « *Toute manifestation de validité, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.* »

- le consentement doit être éclairé, spécifique, libre, et univoque
- il doit pouvoir être démontré par le responsable de traitement
- il donne lieu à un traitement éminemment précaire

=> malgré sa place croissante, le consentement n'est pas le fondement prioritaire d'un traitement et n'est pas nécessairement le plus adapté

Key takeaways

It can be counterproductive to rely on consent

⇒ *The controller must check whether the use of consent is relevant to ensure the lawfulness of the processing*

⇒ *consent is not the primary basis for processing and is not necessarily the most appropriate*

1. La consécration du consentement, corollaire de l'autodétermination informationnelle

Un peu d'histoire

- 1978 - LIL 1: pour lever l'interdiction de traiter des données sensibles
- LIL 2 (2004): singularisation du consentement comme base légale de référence
- 2016: consécration du concept d'autodétermination informationnelle : *« toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant »*
- 2018: le RGPD élargit le champ du consentement
- 2009 révision Directive eprivacy
- Art. L34-5 Code des postes et communications: prospection commerciale directe par sms - mail

Key takeaways

2016: Principle of informational autodetermination :

Each individual has a right to decide and control the uses made of their personal data

2. Le consentement au nombre des 6 bases légales de traitement

Art. 6 RGPD: un traitement n'est licite que si au moins l'une des conditions suivantes est remplie:

a) Consentement

b) Exécution d'un contrat ou de mesures pré-contractuelles

c) Respect d'une obligation légale

d) Sauvegarde des intérêts vitaux

e) Mission d'intérêt public

f) Intérêt légitime

Key takeaways

Lawfulness of processing:

a) Consent

b) Performance of a contract or pre-contractual steps

c) Compliance with a legal obligation

d) Protection of vital interest

e) Public interest

f) Legitimate interest

3. Caractéristiques et conditions de validité du consentement

Art 4.11 RGPD: « Toute manifestation de volonté libre, spécifique, éclairée et univoque, par laquelle la personne concernée accepte par une déclaration ou un acte clair le traitement »

- ❖ Spécifique: un consentement distinct pour chaque finalité
- ❖ Éclairé: identité du RT, finalité granulaire, types de données collectées, existence du droit de retirer son consentement, prise de décision automatisée, risques en cas de transmission de données hors UE
- ❖ Univoque: explicite, pas de cases par défaut, l'acceptation globale donnée à des Conditions Générales ne vaut pas consentement
- ❖ Susceptible de retrait: au travers de la même action que celle par laquelle il a été donné, sans entraîner de préjudice
  - ⇒ les opérations fondées sur le consentement ayant eu lieu avant le retrait restent valables
  - ⇒ Le RT ne peut passer silencieusement à une autre base légale
- ❖ Démontrable

Cas des mineurs (art. 8 RGPD) licite à compter de 16 ans, avec nécessité d'un consentement donné par l'autorité parentale avant

Key takeaways

Valid consent:

- *Specific*
- *Informed*
- *Explicit*
- *Subject to withdrawal*
- *demonstrated*

3. Caractéristiques et conditions de validité du consentement

Checklist

Solliciter le consentement

✓ Est-ce la base légale la plus appropriée?

✓ Le consentement est sollicité séparément des conditions générales

✓ Le consentement résulte d'un acte positif

✓ Granularité

Démontrer le consentement: conserver la preuve, quand et comment?

Gérer le consentement

✓ Le revoir à intervalles réguliers

✓ Rendre simple la modalité de retrait

✓ Tirer les conséquences du retrait

Consent's checklist:

Asking for consent:

- ✓ *most appropriate lawful basis*
- ✓ *request for consent separate from T&Cs*
- ✓ *ask a positive opt-in*
- ✓ *give granular options to consent to different purposes*

Recording consent: *keep a record of when and how we got consent*

Managing consent

- ✓ *Regularly review*
- ✓ *Make withdrawal easy*
- ✓ *Act on withdrawal of consent*

aurele IT avocats

4. Caractère libre du consentement: déséquilibre des rapports de force & conditionnalité

Déséquilibre des rapports de force:

Base légale à priori inappropriée pour les autorités publiques ou dans les relations de travail:

⇒sauf si l'employeur démontre que le consentement est donné librement , en démontrant l'absence de tout élément de contrainte et de conséquences négatives en cas de refus

Conditionnalité:

Le consentement est présumé ne pas avoir été donné librement en cas de couplage avec l'acceptation d'un contrat ou de subordination de la fourniture d'un service au consentement.

Key takeaways

Power imbalance:

Public authority or employer may not use consent as a legal basis unless the absence of detriment is demonstrated

Conditionality

***Consent is presumed to be not freely given when it is bundled** with acceptance of T&Cs or tied to the provision of a service*

5. La protection particulière des mineurs apportée par le RGPD

Niveau de protection supplémentaire concernant le consentement des enfants pour une une offre directe des services de la société de l'information (art.8 RGPD)

- ❖ Offre directe : si un prestataire indique clairement qu'il ne propose ses services qu'à des majeurs (non contredit par le contenu du site web) => ces services ne seront pas considérés comme étant proposés directement à un enfant
- ❖ Enfant âgé de moins de 16 ans / 15 ans en France

  => âge pouvant être abaissé jusqu'à 13 ans par les Etats Membres. En France, fixé à 15 ans (art 45 LIL)

  ⇒ consentement donné par le titulaire de la responsabilité parentale à l'égard de l'enfant: un seul des 2 titulaires, le consentement de l'autre étant présumé, sauf opposition
- ❖ Le RT s'efforce raisonnablement de vérifier que l'utilisateur a dépassé l'âge minimum de consentement numérique

  ⇒ ces efforts doivent être proportionnels à la nature des activités de traitement et aux risques qui y sont liés

  (Lignes Directrices Consentement 10 avril 2018)

  ⇒ le RT doit éviter des solutions de vérification qui impliquent une collecte excessive; il doit cependant procéder à une évaluation constante de ses procédures et de la technologie disponible
- ❖ Une fois l'âge minimum de consentement numérique atteint: l'enfant peut retirer son consentement par lui-même (art. 7 &3 RGPD).

  => le RT doit informer l'enfant de cette possibilité

6. Consentement *eprivacy* et consentement RGPD

Directive eprivacy : condition de licéité au stockage et à l'accès de l'information présente sur le terminal

2 exceptions (art. 5.3 de la Directive):

- ➢ le stockage visant exclusivement à effectuer la transmission d'une communication électronique
- ➢ les opérations strictement nécessaires à la fourniture d'un service de la société de l'information, expressément demandé par l'utilisateur

- Les 2 corps de règles s'appliquent conjointement. La Directive s'applique quel que soit le type d'information, pas nécessairement des données personnelles
- Le consentement requis par la Directive est soumis aux mêmes conditions de validité que celles posées par le RGPD

2 questions:

- ✓ Ai-je obtenu le consentement préalable pour le stockage ou l'accès aux informations sur le terminal?
- ✓ Mon traitement est-il fondé sur l'une des 6 bases légales?

=> si j'ai choisi le consentement, je pourrai collecter par un seul opt-in mes 2 consentements e-privacy et RGPD

Key takeaways

Eprivacy: consent is a condition to storage and access to information existing on a user's device

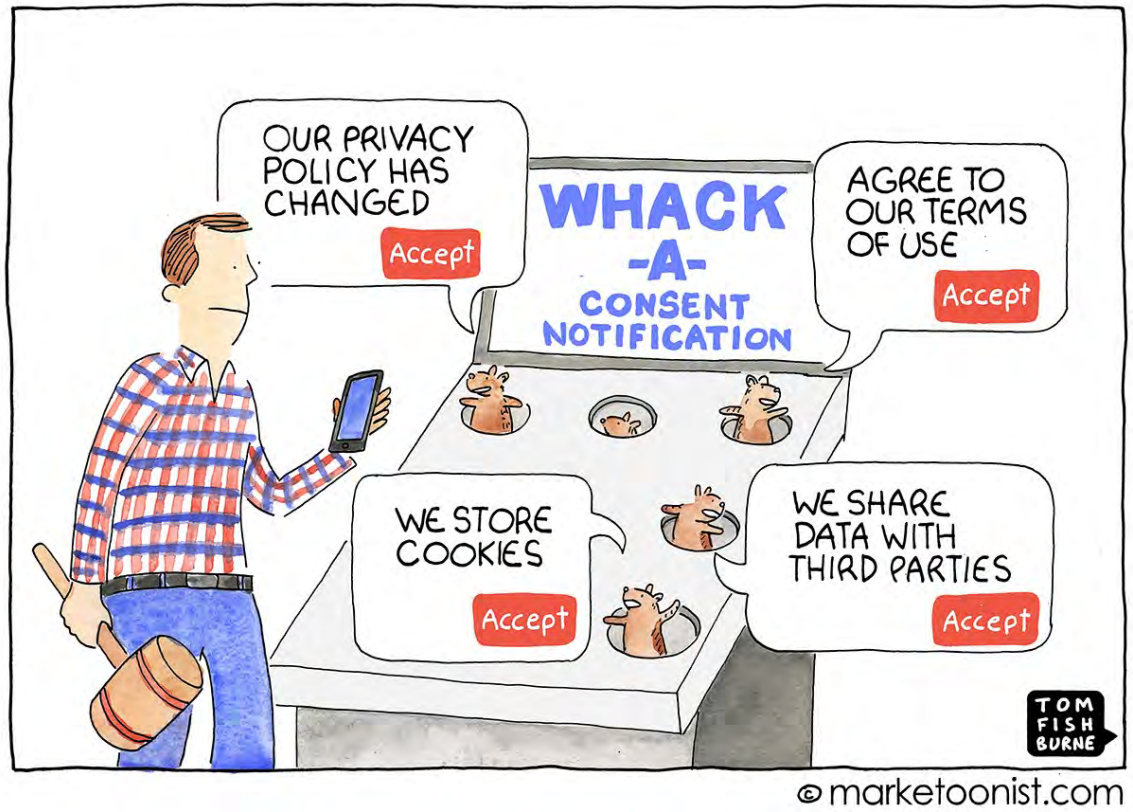
2 exceptions:

- storage or access for the sole purpose of carrying out the transmission of a communication

-as strictly necessary in order to provide an information society service explicitly requested by the user

Conclusion

- Fatigue du consentement: projet de reglement e-privacy



Key takeaways

- Eprivacy regulation:
- Consent fatigue : end-users will be able to give consent to the use of certain types of cookies by whitelisting providers in their browser settings.

Merci pour votre attention

Questions

Florence Ivanier

Avocat à la Cour – DPO

fivanier@aurele-it.fr, www.aurele-it.fr

6, rue Jean de Lafontaine 75016 Paris

+ 33 1 89 16 81 12

aurele IT avocats

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

Data subject rights

Florence Ivanier

Martinique, 2 June 2023

The project is co-financed with the support of the European Union's Justice programme

Séminaire TRADATA 2 Martinique

Les droits des sujets de traitement , y compris les droits dans le cadre des enquêtes et de la procédure pénale

Florence Ivanier, Avocat au barreau de Paris

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

2 juin 2023

aurele IT avocats

FLORENCE IVANIER

- Avocate au barreau de Paris depuis 1995
- Fondatrice du cabinet Aurele IT , créé en 2014, spécialisé en droit du numérique et en data
- Déléguée à la Protection des Données (Data Protection Officer) certifiée - Université Paris Dauphine
- DPO externe désignée auprès de la CNIL
- Co-Responsable de la Commission Ouverte du barreau de Paris Innovation Numérique et Audiovisuel (COMINA)

Mail: fivanier@aurele-it.fr

Tel. 01 89 16 81 12
6, rue Jean de Lafontaine 75016 Paris
Site www.aurele-it.fr

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

aurele IT avocats

Sommaire : Droits des sujets de traitement y compris dans le cadre des enquêtes et de la procédure pénale

1) Sources de droit applicables
   - ✓ Paquet européen de protection des données
   - ✓ Champs d'application respectifs du RGPD, de la Directive Police Justice et de la LIL titre IV
2) Quels droits et quel contenu lorsque le RGPD s'applique?

   Focus:
   - ✓ Le droit d'accès et la montée en puissance de son instrumentalisation
   - ✓ Le droit à la limitation
3) Limites aux droits des sujets de traitement entrant dans le cadre de la Directive Police Justice

1) Sources de droit applicables: le paquet européen de protection des données

RGPD

Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

=> directement applicable dans les pays membres depuis le 25 mai 2018

- Section 1 – art. 12 - Transparence des informations et des communications et modalités de l'exercice des droits
- Section 2 – Information et accès aux données personnelles (art. 13 à 15)
- Section 3 – Rectification et effacement (art. 16 à 20)
- Section 4 – Droit d' opposition et décision individuelle automatisée (art. 21-22)
- Section 5 – Limitations – art. 23

1) Sources de droit applicables: le paquet européen de protection des données

Directive Police Justice

DIRECTIVE (UE) 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (…) 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 (…)

=> transposée en France au sein du chapitre XIII de la loi Informatique et Libertés.

- Chapitre 3: Droits de la personne concernée : art. 12 à 18 Directive

1) Sources de droit applicables

LIL– Titre IV - Traitements relevant de la sûreté de l'État et la défense nationale

=> Dispositions entrées en vigueur en 2019

- s'applique aux traitements d'activités qui ne relèvent pas du champ d'application du droit de l'Union européenne
- traitements mis en œuvre pour le compte de l'État et qui intéressent la sûreté de l'État ou la défense nationale
- Chapitre Ier (art. 116 à 120 LIL): droits de la personne concernée

1) Sources de droit applicables

Directive Passenger Name Record (PNR)

Directive 2016/681/EU relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière

⇒***transposée en France par la loi n° 2017-1510 du 30 octobre 2017*** qui renforce la sécurité intérieure et la lutte contre le terrorisme, pérennise le dispositif API-PNR et transpose la Directive PNR.

- le fichier API PNR repose sur la collecte des données de réservation (données PNR), ainsi que des données d'enregistrement et d'embarquement (données API) des passagers aériens
- ces données sont communiquées par les transporteurs aériens au service à compétence nationale dénommé « Unité Information Passagers » (UIP)
- l'UIP procède à l'exploitation de ces données sur demande des services compétents: police, gendarmerie et renseignement et transmet les réponses

1) Champs d'application respectifs

❖ Directive Police Justice - 2 conditions cumulatives:

a) finalité de « prévention et de détection des infractions pénales ou d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces
   i. en matière pénale: prévention et constatation d'infractions à l'occasion des déplacements des passagers (traitement API-PNR) ou gestion des mesures d'application des peines judiciaires
   ii. activités ne relevant pas de la sphère pénale mais se rapportant à des activités de police effectuées en amont de l'infraction => ex. protection contre les menaces pour la sécurité publique, maintien de l'ordre public

b) traitement mis en œuvre par une autorité compétente:
   i. toute autorité publique compétente pour la prévention et la détection des infractions pénales, les poursuites ou l'exécution de sanctions pénales: autorités judiciaires, police, autorités répressives
   ii. tout autre organisme à qui est confié l'exercice de l'autorité publique et des prérogatives de puissance publique aux fins de mettre en œuvre un traitement relevant de la Directive => ex. services internes de sécurité de la RATP et de la SNCF, fédérations sportives agréées aux fins de sécurisation des manifestations sportives etc.

❖ Titre IV LIL: activités ne relevant pas du champ d'application du droit de l'UE, mis en œuvre pour le compte de l'État et intéressant la sûreté de l'État ou la défense nationale

❖ RGPD: résiduel : traitements de données relevant du champ d'application du droit de l'UE, secteurs public & privé

2) Quels droits des sujets de traitement lorsque le RGPD s'applique?

- Droit d'être informé
- Droit d'accès (15)
- Droit de rectification (16)
- Droit à l'effacement - droit à l'oubli (17)
- Droit à la limitation (18)
- Droit d'être informé des destinataires (19)
- Droit à la portabilité (20)
- Droit d'opposition (21)
- Droit à ne pas faire l'objet d'une décision individuelle automatisée, y compris le profilage (22)
- Droit à retrait du consentement (7.3)
- Droit d'être informé d'une violation de données (34.1)
- Droit d'introduire une réclamation auprès d'une autorité de contrôle (77.1) et droit à un recours juridictionnel effectif contre une autorité de contrôle (78)
- Droit d'obtenir réparation de son préjudice (82.1)

Focus: droit d'accès

Le droit d'accès (art 15 RGPD) comprend:

- le droit d'obtenir confirmation du responsable du traitement que des données personnelles sont ou ne sont pas traitées
- l'accès à ces données, par la fourniture d'une copie des données
- des informations sur les finalités du traitement
  - les catégories de données
  - les destinataires / catégories de destinataires auxquels les données ont été ou seront communiquées.
  - en cas de destinataires établis dans des pays tiers, les garanties appropriées pour le transfert
  - la durée de conservation envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée
  - lorsque les données ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source
  - l'existence d'une prise de décision automatisée, y compris un profilage et en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues du traitement pour la personne concernée.

Focus: droit d'accès

Quelles données?

Toutes les données personnelles concernant la personne concernée

- quel que soit le support utilisé: papier, enregistrement audio, vidéo
- stockées en base courante ou en archives intermédiaires
- y compris les données déduites ou résultat de traitement (ex. achats enregistrés sur une carte de fidélité)

Quel délai de réponse et quelle périodicité?

- Réponse dans le mois, porté à 3 mois sous certaines conditions (8 jours pour les données de santé)
- Périodicité à intervalles réguliers (Considérant 63)

Sous quelle forme?

- d'une façon concise, transparente, compréhensible et aisément accessible, termes clairs et simples

Gratuité: sous les limites précisées ci-après

Focus: droit d'accès

Quelles limites?

- Respect des droits et libertés d'autrui: ne pas porter atteinte aux droits des tiers

⇒en pratique doivent être supprimés les éléments susceptibles d'identifier un tiers, de porter atteinte au secret des correspondances, à la vie privée, ou au secret des affaires

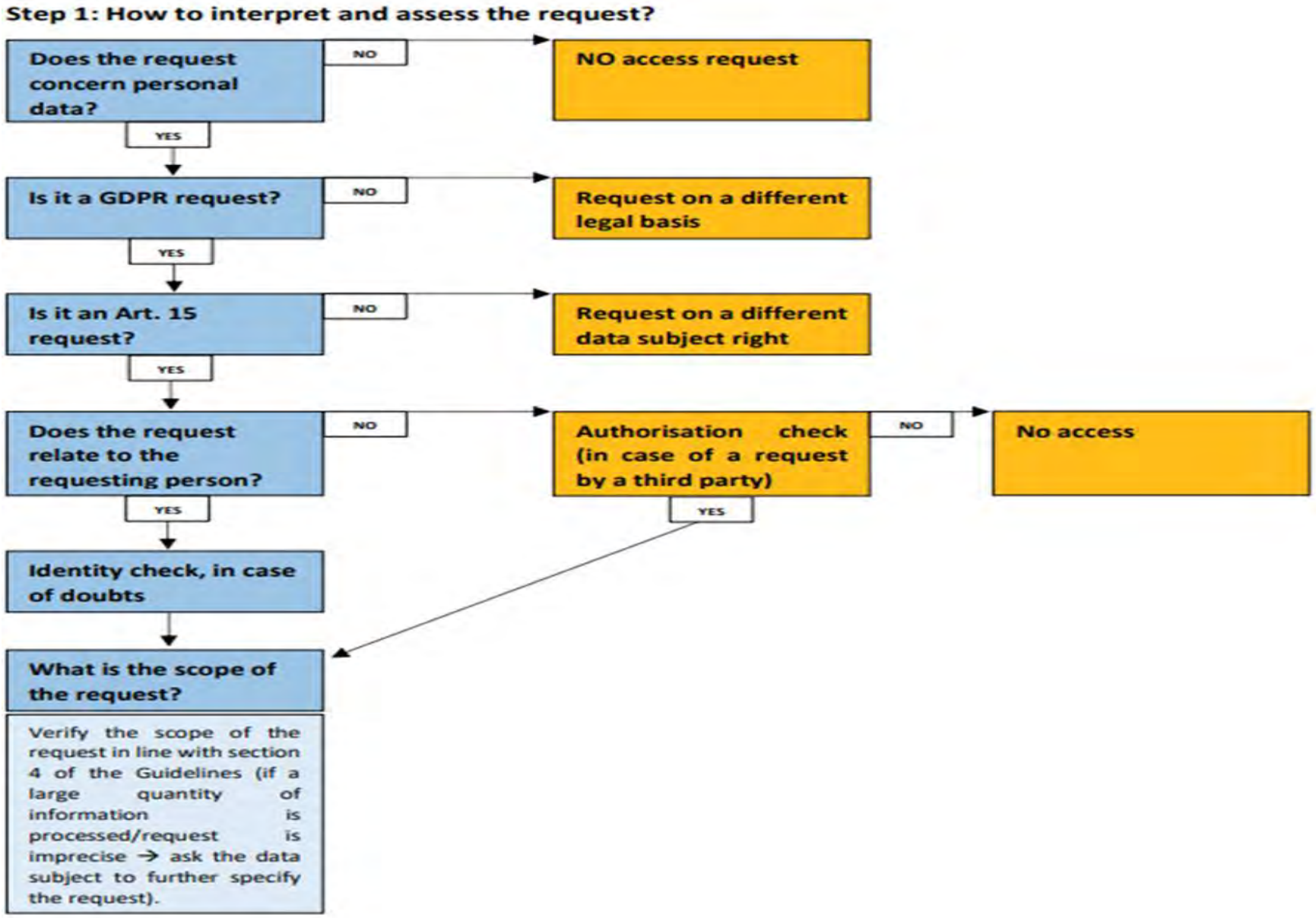
- Demandes sont manifestement infondées ou excessives (notamment caractère répétitif) le responsable du traitement peut:

a) exiger le paiement de frais raisonnables tenant compte des coûts administratifs supportés

ou

b) refuser de donner suite à ces demandes

Focus: droit d'accès



Répondre à une demande de droit d'accès

Toute personne peut obtenir

Des informations la concernant, de manière claire :
- Quelles données collectées ?
- Quelles durées de conservation ?
- Quels destinataires ?
- etc.

Une copie de ses données, quel que soit leur support de conservation

1 Si nécessaire, vérifiez qui est le demandeur

En cas de doute :

2 Si nécessaire, demandez si la demande concerne

Des données spécifiques

Toutes les données de la personne

3 Vérifiez que la demande ne concerne pas un tiers

Conjoint

Collègue

Secret des affaires

Propriété intellectuelle

4 Répondez à la demande

1 mois max.
Demande simple

8 jours max.
Données de santé

3 mois max.
Demande complexe
(par ex. beaucoup de données)

Vous pouvez refuser si
- la demande est infondée ou excessive
- les données ont été effacées

Dans tous les cas, informez la personne sous un mois maximum

Droit d'accès - Montée en puissance de son instrumentalisation

Un droit emblématique et quasi-illimité qui répond à l'objectif du RGPD d'accroître le contrôle des individus sur leurs données

❖ cependant désormais largement détourné de sa finalité originelle par son instrumentalisation à des fins contentieuses:

⇒ litiges prud'homaux / commerciaux/ consommateurs

⇒ afin d'obtenir un accès large à des données dans un but autre que la vérification du traitement ou non de données personnelles

⇒ à des fins probatoires, ce qui permet de contourner l'art. 15 CPC

⇒ à des fins de rétorsion

❖ Droit inconditionnel, sans nécessité de justifier d'un motif légitime

Cf Guidelines CEPD 28/03/2023: "*data subjects are not obliged to give reasons or to justify their request. As long as the requirements of Art. 15 GDPR are met, the purposes behind the request should be regarded as irrelevant*"

Focus: droit à la limitation

Quelle portée?

Mesure conservatoire*: « marquage de données personnelles conservées, en vue de limiter leur traitement futur »* (art. 4.3 RGPD)

Quelle finalité ?

- finalité conservatoire, visant à assurer la préservation contre tout risque, notamment de disparition
- s'apparente à une mesure précontentieuse, en ce qu'il permet de demander au responsable de traitement de conserver des preuves

  => vient compléter d'autres droits (ex. accompagne une demande de rectification ou d'opposition et permet de geler les données pendant la période d'instruction de la demande)

  ou

  ⇒ constitue une alternative, notamment à une demande d'effacement

Focus: droit à la limitation

Quel champ d'application?

Exclu dans le cadre des traitements à des fins de défense et sûreté de l'Etat et aménagé dans le cadre de la Directive Police Justice

4 hypothèses de limitation au titre du RGPD (art.18 RGPD):

- Exactitude des données contestée pendant une durée permettant au responsable de traitement de vérifier l'exactitude
- Traitement illicite et la personne concernée s'oppose à l'effacement, exigeant à la place la limitation
- Le responsable n'a plus besoin des données mais elles sont nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice
- La personne concernée a exercé son droit d'opposition et la limitation a lieu pendant la vérification que les motifs légitimes poursuivis par le responsable de traitement prévalent sur ceux de la personne concernée

3) Directive Police Justice - Point sur les obligations de l'organisme

Conditions d'application (art. 88 LIL)

Le traitement licite uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne

- ❖soit s'il est autorisé par une disposition législative ou réglementaire
- ❖soit s'il vise à protéger les intérêts vitaux d'une personne
- ❖ soit s'il porte sur des données manifestement rendues publiques

3) Directive Police Justice - Point sur les obligations de l'organisme

Obligations similaires à celles imposées par le RGPD:

- MTO appropriées et mesures afin de garantir un niveau de sécurité adapté au risque (art. 19 & 29 Directive)
- Privacy by design & by default (art.20 Directive)
- Les sous-traitants présentent des garanties suffisantes (art. 22 Directive)
- Registre des activités de traitement (art. 24 Directive)
- AIPD lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes (art. 27 Directive)
- notifier à l'autorité les violations dans les 72h en cas de risques pour les droits et libertés d'une personne (art. 30 Directive)
- communiquer à la personne concernée la violation en cas de risque élevé pour ses droits et libertés (art. 31 Directive)
- désigner un DPO (art. 32 Directive)
- respecter les conditions définies pour le transfert de données vers des pays tiers (art 35 et s. Directive)

3) Directive Police Justice - Point sur les obligations de l'organisme

Obligations spécifiques imposées par la Directive Police Justice

- Consulter l'autorité de contrôle si l'AIPD présente des risques résiduels élevés ou si le traitement, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques initiaux élevés
- établir une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées (art 6 Directive)

  => ex: personnes reconnues coupables d'une infraction pénale, personnes victimes, tiers
- distinguer entre les données personnelles fondées sur des faits et celles fondées sur des appréciations personnelles (art. 7 Directive)
- traitement licite: nécessaire à l'exécution d'une mission effectuée par une autorité compétente, pour les finalités prévues par la Directive et fondé sur le droit de l'Union ou le droit d'un Etat membre (art. 8 Directive)
- traitement portant sur des données sensibles uniquement en cas de nécessité absolue (art. 10 Directive)

3) Limites aux droits dans le cadre de la Directive Police Justice

Droits présents dans le RGPD ne se retrouvant pas dans la Directive:

- droit à la portabilité

Droits présents dans le RGPD assortis de limitations dans le cadre de la Directive

❖**information de la personne concernée**, sous réserve de possibles limitations (art. 13)

❖**droit d'accès** (14) sous réserve des limitations, entières ou partielles, qui peuvent lui être apportées notamment pour ne pas gêner les enquêtes, éviter de nuire à la prévention et à la détection des infractions pénales (art. 15).

=> en pratique, la limitation du droit d'accès pourra conduire à la mise en œuvre d'un « droit d'accès indirect », c'est-à-dire exercé par l'intermédiaire de l'autorité de contrôle compétente

❖**droit de rectification ou d'effacement** (art. 16)

❖**droit à la limitation** - 2 hypothèses:

(i) données conservées à des fins probatoires ou

(ii) exactitude des données contestées et il ne peut être déterminé si elles sont exactes ou non

3) Limites aux droits dans le cadre de la Directive Police Justice

Limitations prévues en France par la LIL

- Les droits de la personne concernée peuvent faire l'objet de restrictions aussi longtemps qu'une telle restriction constitue une « *mesure nécessaire et proportionnée dans une société démocratique en tenant compte des droits fondamentaux et des intérêts légitimes de la personne* », pour
  - éviter de gêner des enquêtes, des recherches ou des procédures
  - éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites ou à l'exécution de sanctions pénales ;
  - protéger la sécurité publique, la sécurité nationale , les droits et libertés d'autrui (art. 107 LIL)
- Lorsque les conditions ci-dessus sont remplies, le responsable de traitement peut :
  - retarder ou limiter la communication des informations ou ne pas les communiquer
  - refuser ou limiter le droit d'accès
  - ne pas informer la personne du refus de rectifier ou d'effacer des données ou de limiter le traitement, ni des motifs de cette décision
- L'information de la personne concernée sur ce refus peut ne pas être fournie lorsque la communication risque de compromettre l'un des objectifs ci-dessus.

  => le responsable de traitement consigne les motifs sur lesquels se fonde la décision et met ces informations à la disposition de la CNIL

3) Limites aux droits dans le cadre de la Directive Police Justice

Limitations prévues en France par la LIL (art.111 LIL)

❖ Ce régime ne s'applique pas lorsque les données figurent:

- dans une décision judiciaire
- dans un dossier judiciaire faisant l'objet d'un traitement lors d'une procédure pénale

=> l'accès à ces données et les conditions de rectification ou d'effacement sont régis par le code de procédure pénale

Merci pour votre attention

Florence Ivanier
Avocat à la Cour – DPO
fivanier@aurele-it.fr
www.aurele-it.fr
6, rue Jean de Lafontaine 75016 Paris
01 89 16 81 12

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

GDPR in practice

Valérie Hayek

Martinique, 2 June 2023

The project is co-financed with the support of the European Union's Justice programme

Tout savoir sur le RGPD en pratique

Présenté par Maître Valérie Hayek

Tradata 2

SOMMAIRE

PARTIE 1 : INTRODUCTION

Audit « Informatique et libertés » (tel que dénommé par la CNIL)*

- Il s'agit d'une procédure de vérification de la conformité des process de l'entreprise au regard du RGPD.
- Pour le DPO auditeur : respecter les principes de déontologie, de présentation impartiale des résultats, de conscience professionnelle, d'indépendance et d'approche systématique.

I. Préparation de l'audit

1. Sélection des échantillons
2. Plan d'audit
3. Organisation d'entretiens
4. Questionnaires d'audit

II. Mise en œuvre de l'audit

1. Recensement des traitements
2. Analyse des traitements
3. Rapport d'audit

*https://www.cnil.fr/sites/default/files/atoms/files/labelscnil-audit-demande_0.doc Consulter Annexes 4 et 5.

PARTIE 1 : INTRODUCTION
Responsable de traitement

Chapitre IV du RGPD

- Le responsable de traitement est la personne morale ou physique qui détermine les **finalités et les moyens** d'un traitement, c'est-à-dire l'objectif et la façon de le réaliser* ;
- Plus précisément, il détermine le « *pourquoi* » et le « *comment* » du traitement de données, c'est-à-dire sa finalité (objectifs poursuivis) et ses moyens (conditions de mise en œuvre notamment sur le plan technique, matériel et organisationnel) ;
- Exemples dans le secteur privé : président, directeur général, PDG, etc. ;
- Exemples dans le secteur public : ministre, maire, président de l'EPCI, conseil départemental, etc.

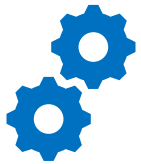
*https://www.cnil.fr/fr/definition/responsable-de-traitement

PARTIE 1 : INTRODUCTION
Responsable de traitement
Article 24 du RGPD

Le responsable de traitement est notamment tenu de :

Mettre en œuvre des mesures techniques et organisationnelles appropriées

Démontrer que le traitement est conforme



Mettre en œuvre des politiques appropriées

Appliquer un code de conduite

Être certifié

PARTIE 1 : INTRODUCTION
Délégué(e) à la protection des données (DPO)

Articles 37 à 39 du RGPD : missions et obligations du DPO

- **Compétences :**
  - Expérience juridique et technique en matière de protection des données personnelles ;
  - Bonne connaissance du secteur d'activité, de l'organisation interne, des systèmes d'information, des besoins en matière de protection et de sécurité des données.
- **Moyens suffisants :**
  - Temps, moyens humains et adéquats, accéder à des informations utiles, être associé en amont sur des projets impliquant des données personnelles, être facilement joignable par les personnes concernées.
- **Indépendance :**
  - Pas de situation de conflit d'intérêt, possibilité de rendre compte de son action au plus haut niveau de la direction de l'organisme, ne pas être sanctionné pour l'exercice de ses missions de DPO, ne pas recevoir d'instruction dans le cadre de l'exercice de ses fonctions*.

*https://www.cnil.fr/fr/designation-dpo

PARTIE 2 : ENTRETIEN CLIENT

Voici un argumentaire à présenter au client :

Confiance

Le RGPD a pour but d'assurer une plus grande confiance entre vos clients et vous. En respectant ce règlement, vous leur montrez votre allégeance aux valeurs de respects des droits de la vie privée, et votre capacité à être une entreprise responsable

Efficacité commerciale

Le respect du RGPD demande à ce que vos données soient exactes et mises à jour régulièrement, ce qui garantit une information fiable pour le développement de votre à activité

Avantage concurrentiel

Les utilisateurs font confiance aux entreprises « labelisées RGPD » et soucieuses de la protection de leurs données personnelles. Être conforme au RGPD permet donc d'améliorer l'image de l'entreprise et sa réputation*.

* *https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf*

PARTIE 3: AUDIT INTERNE
Arrivée dans l'entreprise le Cluedo commence

Licéité du traitement
Article 6-1 du RGPD

Lorsqu'un organisme souhaite collecter des données personnelles, il doit **identifier le fondement** de cette démarche.
Un traitement ne peut être mis en œuvre que s'il est fondé sur une des 6 conditions de licéité suivantes*:

Consentement

Intérêt légitime

Respect d'une obligation légale

Nécessaire à l'exécution du contrat

Nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique

Nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou tout autre personne

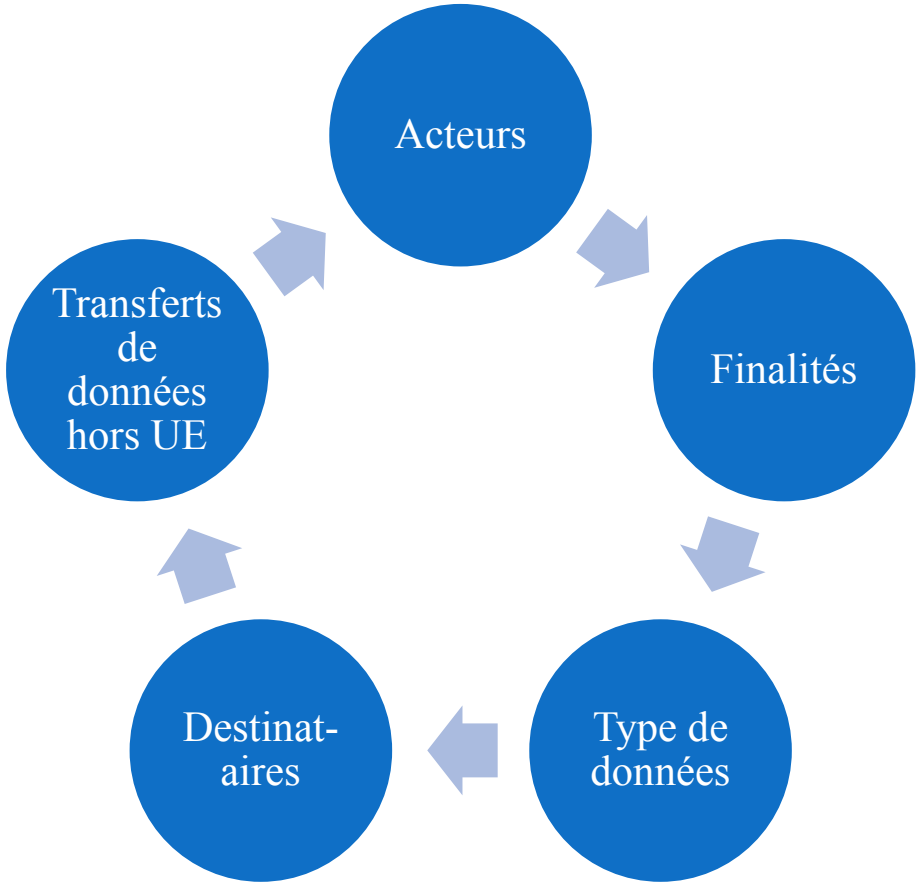
*https://www.cnil.fr/fr/la-liceite-du-traitement-lessentiel-sur-les-bases-legales-prevues-par-le-rgpd

PARTIE 3: AUDIT INTERNE
Processus de mise en conformité en 6 étapes

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf

PARTIE 3: AUDIT INTERNE
But de l'audit : cartographier les traitements



PARTIE 3: AUDIT INTERNE

Composition

Les 2 phases de l'audit interne sont :

- L'audit du site internet (le *Front Office* et le *Back Office*) ;
- L'audit des différents services de l'entreprise.

L'audit des services consiste à savoir comment travaillent les membres de l'entreprise afin d'identifier le chemin des données.

PARTIE 3: AUDIT INTERNE
Audit du site internet

Comment se déroule un contrôle à distance de la CNIL* ?

Le contrôle en ligne vise prioritairement à obtenir des **copie d'informations (éléments techniques et juridiques) permettant d'évaluer les conditions dans lesquelles sont mis en œuvre les traitements**. Dans le cas d'un contrôle en ligne réalisé à la suite d'un signalement d'une violation de données, celui-ci a également pour objet de constater l'existence et l'étendue de la violation de données.

- Toute donnée librement accessible depuis le nom de domaine ou le site web visé par la décision de contrôle peut être recueillie (p. ex. **copie d'écran**, extraits de base de données, code source de la page, etc.)
- les données librement accessibles ou rendues accessibles.

Les agents du contrôle se comportent comme tout internaute.

En pratique : formulaires en ligne, tester des liens de désinscription, **procédures permettant l'exercice des droits.**

Les agents de contrôle peuvent faire usage d'une identité d'emprunt pour les opérations de contrôle en ligne.

**https://www.cnil.fr/sites/default/files/atoms/files/cnil-charte_des_controles.pdf*

PARTIE 3: AUDIT INTERNE
Audit du site internet

1er résultat du contrôle de la CNIL : un PV*

Enfin, au cours des opérations de contrôle en ligne, un procès-verbal est dressé faisant mention de :

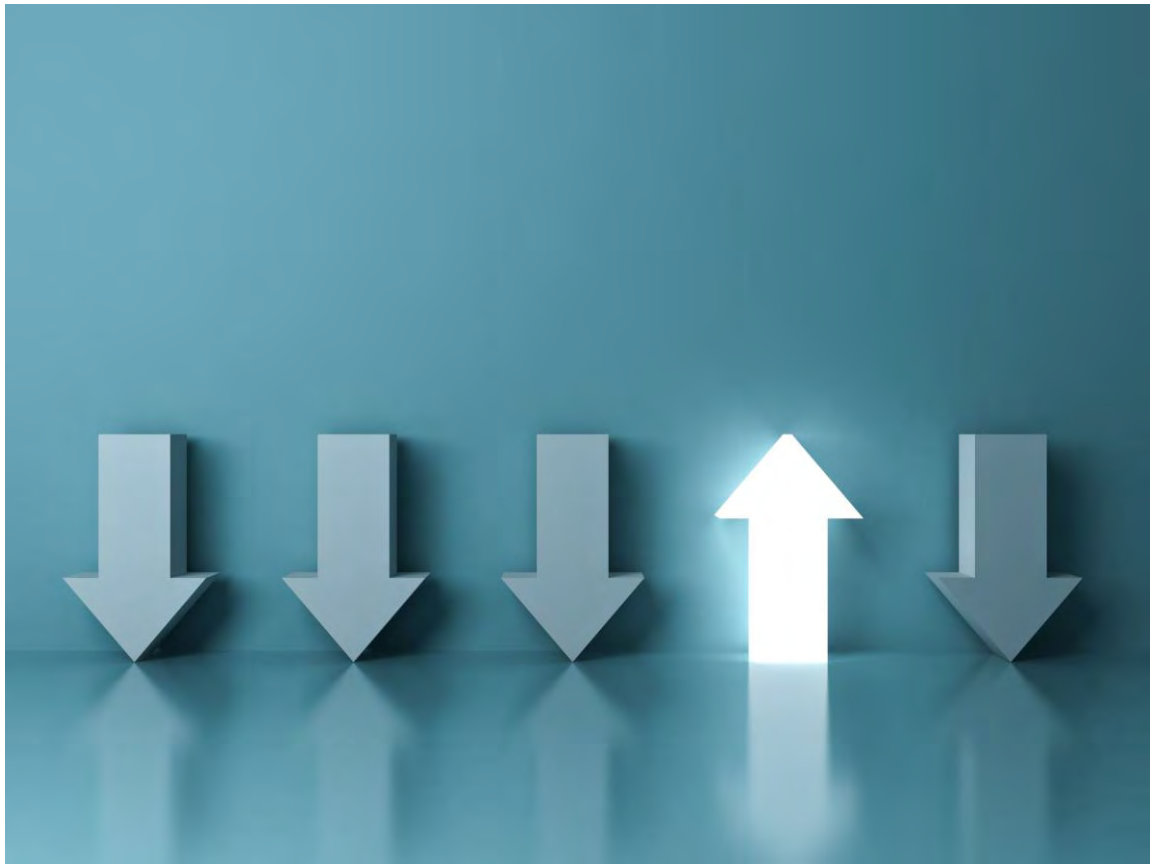
- L'ensemble des **constatations** des agents de contrôle ;
- La liste les pièces placées en annexe ;
- **L'identité** et la qualité des personnes avec lesquelles la délégation de la CNIL s'est entretenue ;
- Les demandes de communication de **pièces complémentaires** (contrats, extractions de bases de données, etc.) dans un **délai imparti** ;
- Les **pièces complémentaires** doivent être adressées à la CNIL de manière à en assurer la sécurité et la confidentialité.
- Il est signé par les agents de contrôle de la CNIL.

**https://www.cnil.fr/sites/default/files/atoms/files/cnil-charte_des_controles.pdf*

PARTIE 3:
AUDIT INTERNE

Audit du site internet

- Bandeau Cookies
- Mentions légales / Politique de confidentialité
- Adresses mail DPO
- CNIL comme autorité compétente
- Sécurité informatique (norme ISO 27021)
- Sous-traitants
- Réseaux sociaux
- Exercice des droits
- Notification



PARTIE 3: AUDIT INTERNE
Audit du site internet

Déléguée à la protection des données

Il est nécessaire de vérifier si DPO est déclaré et si la déclaration est conforme*.

1	Date de la dÃ(	SIREN organis	Nom organisn	Secteur activi	Code NAF org	Adresse posta	Code postal o	Ville organism	Pays organism	Moyen conta(	Moyen conta(	Moyen conta(	Moyen conta(	Moyen conta(	Moyen conta(	Moyen conta(
2	25/05/2018										https://www.	153732222	Commission n	75007	PARIS	France
3	25/05/2018									donneespersc	https://www.monuments-n		Centre des m	75004	PARIS	France
4	25/05/2018									'pd@grandes	https://www.grandest.fr/donnees-personnelles					
5	25/05/2018									DiRECTION.HUET@AELYS95		139593280	26 RUE DU D(	95600	EAUBONNE	France
6	25/05/2018									dpo@seinem	https://www.	235035347	Monsieur le D	76101	ROUEN CEDE	France
7	25/05/2018									donneespersonnelles@meduane-habitat.f			15 quai GAME	53000	LAVAL	France
8	25/05/2018									dpd@charente-maritime.fr		546317055	85 boulevard	17076	LA ROCHELLE	France
9	25/05/2018									rgpd@unicaen.fr		231565660	UniversitÃ© d	14032	CAEN	France
10	25/05/2018	837528561	C83 BRUNO F	N	8299Z	280 CHE DE L/	83500	LA SEYNE-SUF	France	c83.bfouquet@gmail.com		771728496	AVEFETH 100	83000	TOULON	France
11	25/05/2018									cil@megalis.bretagne.bzh			15 rue Claude	35510	CESSON-SEVI(	France
12	25/05/2018									privacy@cgi.com			CGI - immeub	92097	COURBEVOIE	France
13	25/05/2018									dpo@mediapart.fr			Mediapart DÁ	75012	PARIS	France
14	25/05/2018									cm@toucantoco.com		179739666	2-4 rue Paul C	75008	PARIS	France
15	25/05/2018									p.denorme@mairie-petit-ca		235048626	3 RUE DU VAL	76370	PETIT-CAUX	France
16	25/05/2018									data-protection@3Xconsultants.com			3X Consultant	31400	TOULOUSE	France
17	25/05/2018									dpo@adlpartner.fr			ADLPARTNER	60500	CHANTILLY	France
18	25/05/2018									ssandoval@groupeais.fr		251807939	2, rue MichaÃ	44800	SAINT-HERBL	France
19	25/05/2018									dpd@neo-soft.fr		299839802	318 rue de Fo	35700	RENNES	France
20	25/05/2018									cil-insa@ingroupe.com		140583000	104, avenue d	75016	PARIS	France
21	25/05/2018									gandre@notaires.fr		386544026	6 rue Saint Ni(	89700	TONNERRE	France
22	25/05/2018									donneespersc	http://www.c	784467899	165 avenue d(	59000	LILLE	France
23	25/05/2018									dpd@eptb-vil	https://www.	299908844	Boulevard de	56130	LA ROCHE BE	France

*https://www.data.gouv.fr/fr/datasets/organismes-ayant-designe-un-e-delegue-e-a-la-protection-des-donnees-dpd-dpo/

PARTIE 3 : AUDIT INTERNE
Audit des services de l'entreprise

Les salariés de l'entreprise sont des acteurs clés de l'audit RGPD

Le RGPD impose
le consentement des salariés
pour l'usage et la communication de
leurs données personnelles.
Vérifier la conservation qui en est faite

Les dispositions du Code du travail
sont très protectrices des salariés
et de leurs données personnelles

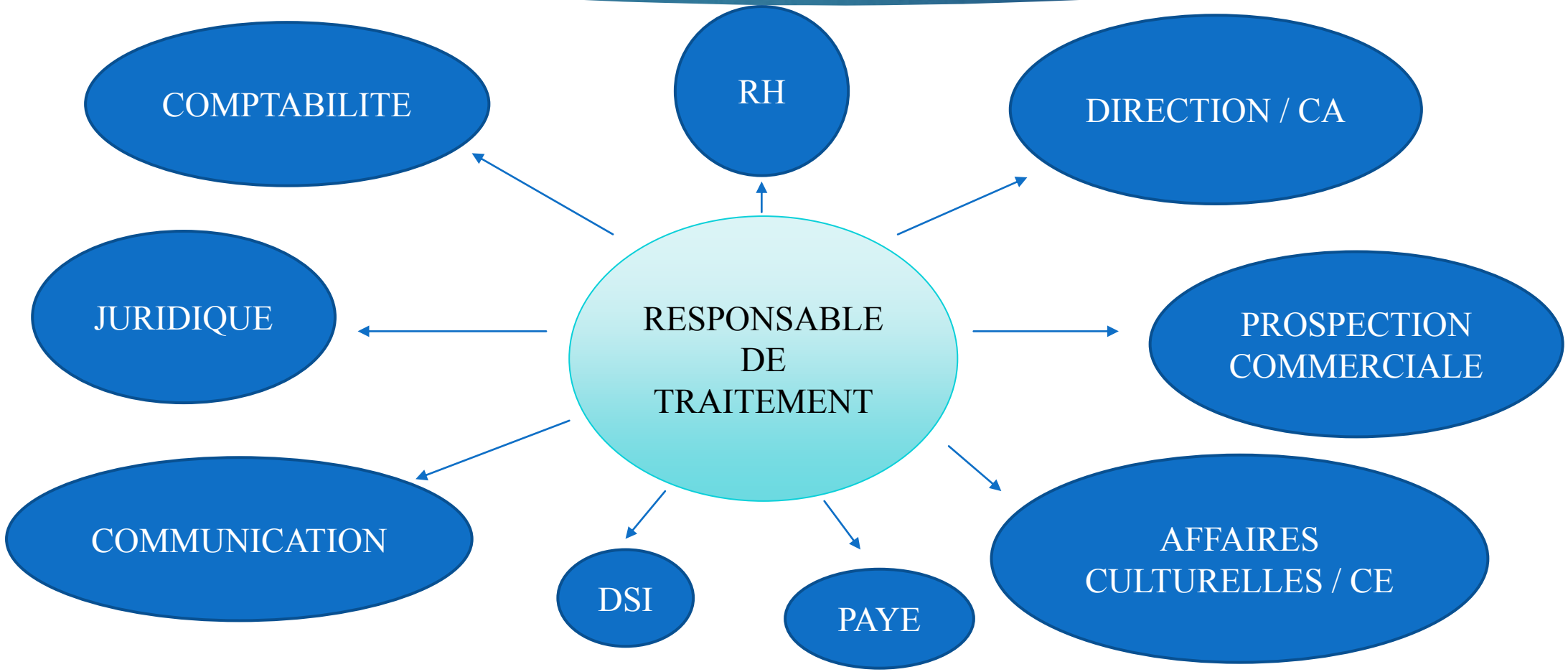
Préciser aux salariés leurs droits d'accès, de modification, d'opposition et d'effacement*.
Indiquer que ces droits peuvent s'exercer à tout moment

*https://www.cnil.fr/fr/definition/traitement-de-donnees-personnelles

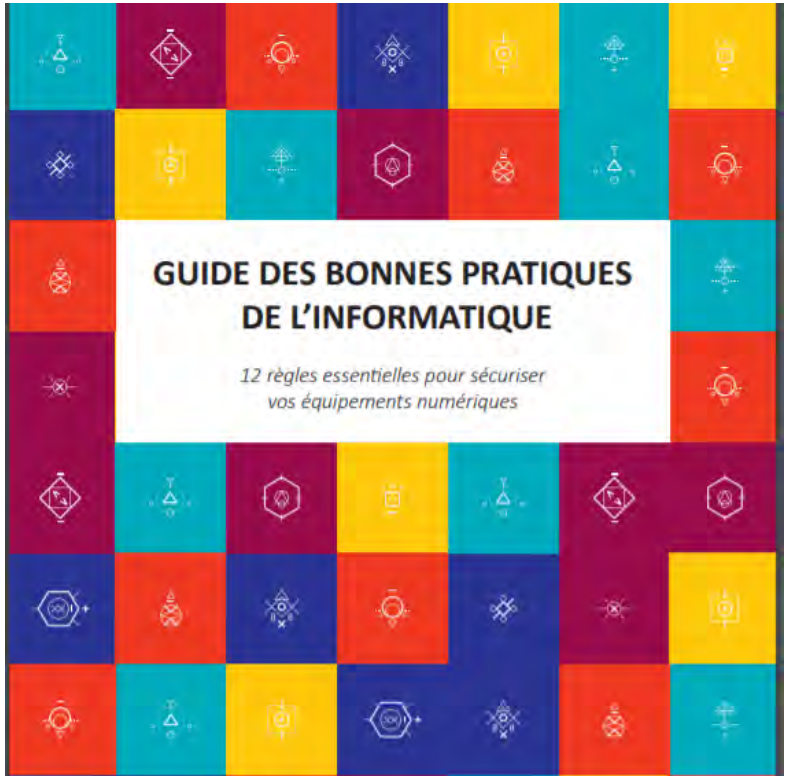
PARTIE 3 : AUDIT INTERNE

Audit des services de l'entreprise

Tous les services sont concernés !



PARTIE 3 : AUDIT INTERNE
Audit des services de l'entreprise

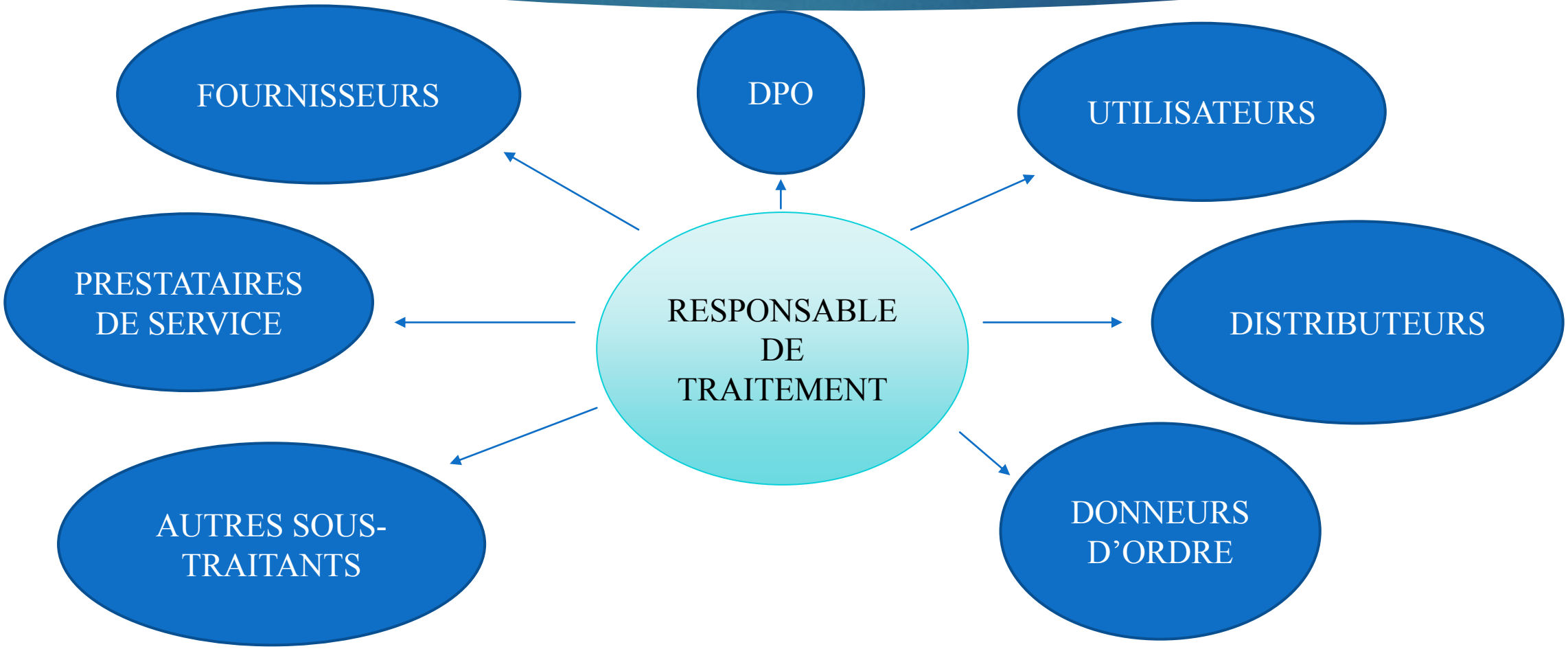


Les 12 règles d'or de la sécurité informatique*

1. Choisir avec soin ses mots de passe ;
2. Mettre à jour régulièrement vos logiciels ;
3. Bien connaître ses utilisateurs et ses prestataires ;
4. Effectuer des sauvegardes régulières ;
5. Sécuriser l'accès Wi-Fi de votre entreprise ;
6. Être aussi prudent avec son ordiphone (smartphone) ou sa tablette qu'avec son ordinateur ;
7. Protéger ses données lors de ses déplacements ;
8. Être prudent lors de l'utilisation de sa messagerie ;
9. Télécharger ses programmes sur les sites officiels des éditeurs ;
10. Être vigilant lors d'un paiement sur Internet ;
11. Séparer les usages personnels des usages professionnels ;
12. Prendre soin de ses informations personnelles, professionnelles et de son identité numérique.

*https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

PARTIE 4 : AUDIT EXTERNE
Les sous-traitants - Article 28 du RGPD



PARTIE 4 : AUDIT EXTERNE
Une question de responsabilité

Il est important de procéder à un audit de l'activité du sous-traitant. En effet, deux régimes de responsabilités peuvent être engagés en cas de contrôle par la CNIL :

- La **co-responsabilité** avec le responsable de traitement* ;
- La **responsabilité en cascade** qui permet de remonter au responsable de traitement.

L'audit permet également de déceler une potentielle faille de sécurité qui peut porter atteinte à l'image de la société auditée.

** Guidelines 07/2020 on the concepts of controller and processor in the GDPR : https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en*

PARTIE 4 : AUDIT EXTERNE
Que se passe-t-il après un audit ?

La mise en conformité au RGPD s'effectue dans chaque service.

Coopérer avec votre DPO interne pour arriver à être conforme.

Mettre en place un processus de mise en conformité.

Cela fait partie des objectifs de la société concernée et des KPIs.

Le RGPD est un avantage concurrentiel pour la société concernée

La réussite de la mise en conformité au RGPD dépend de chacun de vous !

MERCI POUR VOTRE ATTENTION

Crédits photos : Site de la CNIL et MOOC « l'atelier RGPD » de la CNIL, site de l'ANSSI

Crédits vidéo : YouTube

Maître Valérie Hayek

Cabinet Hasperak Avocats

hayek.valerie@hasperakavocats.com

07 61 82 21 53

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

Directive 2016/680

Valérie Hayek

Martinique, 2 June 2023

The project is co-financed with the support of the European Union's Justice programme

La directive 2016/680 Données personnelles, infractions et sanctions pénales

Présenté par
Valérie Hayek
Avocate

Sommaire

I – Le domaine de la directive

A – Au début, il était difficile d'appliquer la directive

La nécessité d'avoir un processus harmonisé en matière de protection de la vie privée :

- RGPD : **s'applique à tout traitement de données**

- Règlement n°2018/1725 du 23 Octobre 2018 relative à la **protection de la personne physique** au sujet du **traitement des données à caractère personnel par les institutions, organes, bureaux et agences** et sur la libre circulation de telles données*.

Des changements ?

- **La catégorie des personnes** : séparer les personnes convaincues, les victims et les témoins

- Pas de transparence

- **Droit d'accès restreint** : sécurité nationale, enquête

- Coopération policière

*Protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union : des règles actualisées et renforcées, PEYROU Sylvie : file:///C:/Users/Val%C3%A9rieHayek/Downloads/2382-Texte%20de%20l'article-13870-1-10-20190201.pdf

I – Le domaine de la directive

A – Au début, il était difficile d'appliquer la directive

Besoin de lignes directrices : Conseil de l'Europe : Manuel sur la loi européenne de protection des données*

2021 : La **CJUE condamne l'Espagne** pour **non-transposition de la directive** : amende de 15 millions en raison d'infractions futures**

Harmonisation avec la **directive de l'UE sur les données du passenger name record (PNR) ou dossier passager : validité :** CJUE, 21 juin, 2022 C-817/19*** :

- But du traitement des données
- Principe de légalité
- Traitement automatique des données personnelles
- Publication d'informations

*https://www.echr.coe.int/LibraryDocs/UE-FRA-2018-Handbook_data_protection_FRE.pdf **https://www.editions-legislatives.fr/actualite/lespagne-condamnee-a-payer-15-millions-deuros-pour-navoir-pas-transpose-la-directive-police-justice/ *** https://www.dalloz.fr/documentation/Document?id=CJUE_LIEUVIDE_2022-06-21_C81719#_

I – Le domaine de la directive

B – Révision de la directive en 2022

Nouveau besoin d'harmonisation :

- Modernisation de la Convention 108 et des protocoles du Conseil de l'Europe*
- Schengen
- Coopération policière et judiciaire en matière pénale qui prend 3 formes**:
  - coopération entre les forces de police nationales;
  - coopération entre les administrations nationales (en particulier sur les services douaniers);
  - coopération entre les autorités judiciaires nationales.

Révision de la directive : 27 Janvier 2022***: infraction pénale, enquête, poursuites pénales

Mais aussi : exécution de sanctions pénales, menace pour la sécurité publique, mesures de prévention

*https://www.coe.int/en/web/data-protection/convention108-and-protocol **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Apolice_judicial_cooperation ***https://www.lexisveille.fr/revision-de-la-directive-police-justice-la-commission-europeenne-consulte-sur-la-protection-des

I – Le domaine de la directive

B – Révision de la directive en 2022

Décision préliminaire de la CJUE le 8 décembre 2022* :

- Protection des personnes physiques concernant le traitement des données à caractère personnel
- Concept d'un **"intérêt légitime"**
- Concept de "tâche réalisée **dans l'intérêt public** ou dans l'exercice de l'autorité officielle"
- **Légalité** du traitement des données à caractère personnel dans le cadre d'une **enquête criminelle**
- **Traitement ultérieur** de données relatives à une **victime** présumée d'une infraction pénale **dans le but de porter une accusation formelle** à son égard
- Concept de **finalité "autre** que celle pour laquelle les données à caractère personnel sont collectées"
- Données utilisées par le **Ministère public** d'un Etat membre pour **sa défense** dans une action en dommages et intérêts contre l'Etat

*https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62021CA0180&from=FR

I – Le domaine de la directive

C – Evaluation de la directive et de la biométrie

2022 : Evaluation de la directive : La directive sur l'application de la loi sur la protection des données (LED)

- Gouvernance et **pouvoirs des autorités de surveillance de la protection des données**
- Recours et **droits des personnes concernées**
- 1ères leçons de l'application et du **fonctionnement de LED**

Résultats : un **niveau plus élevé de sensibilisation** et d'attention sur la protection des données par les **autorités nationales** compétentes, en particulier concernant la **sécurité du traitement**

Besoin d'en faire plus sur les trasnferts de données internationaux :

- Pomouvoir activement d'éventuelles **nouvelles décisions d'adéquation** avec les principaux partenaires internationaux;
- **Négocier de nouveaux accords de cooperation entre Europol et Eurojust**, d'une part, et les pays tiers, d'autre part;
- **S'engager dans des négociations avec le Japon** en vue de modifier l'accord d'entraide mutuelle existent entre l'EU et le Japon afin d'assurer des garanties appropriées en matière de protection des données;
- Poursuivre et conclure la négociation d'un **accord bilatéral avec les Etats-Unis** sur **l'accès transfrontalier aux preuves électroniques** pour la coopération judiciaire en matière pénale, y compris en complétant les dispositifs de protection des données garantis par l'accord cadre UE-US;
- Explorer la possibilité de conclure des accords **cadres de protection des données** pour le traitement des données dans le domaine du droit pénal avec d'importants partenaires d'exécution du droit pénal, en s'appuyant sur l'exemple de l'accord cadre UE-US.

* https://eucrim.eu/news/commission-presented-first-evaluation-report-on-data-protection-law-enforcement-directive/

I – Le domaine de la directive

C – Evaluation de la directive et de la biométrie

Biométrie : CJUE 26 janvier 2023 C-205/21 : Décision préliminaire

- – Limitation de l'objectif
- – **Minimisation des données**
- – **Distinction Claire entre les données à caractère personnel des différentes categories de personnes concernées**
- **– Traitement des données biométriques et des données génétiques**
- – Concept de **"traitement autorisé par le droit des Etats members"**
- – Concept de **"strictement necessaire"**
- – Discrétion
- – Droit à une protection judiciaire effective
- – Infractions pénales intentionnalles faisant l'objet de **poursuites publiques**
- – **Collecte de données photographiques et dactyloscopiques** afin qu'elles soient saisies dans un enregistrement et prélèvement d'un **échantillon biologique** dans le but de **créer un profil ADN**
- – Nature **systématique** de la **collecte**

*https://www.eurogersinfo.com/la-cour-de-justice-de-lunion-europeenne-precise-la-protection-des-donnees-personnelles

II – Les impacts de la directive

A – Résumons : Concernant le RGPD

1. Même domaine

II – Les impacts de la directive

A – Concernant le RGPD

1. Même domaine

Les différences entre la directive et le RGPD :

- La directive s'applique aux activités de traitement des données à caractère personnel aux fins de **prévention et détection des infractions pénales**, tandis que le **RGPD s'applique à tous les types de traitement des données**
- La directive contient des **dispositions spécifiques pour la sécurité et les autorités judiciaires**, tandis que le **RGPD s'applique à toutes les entreprises et organisations** qui traitent des données
- La directive **permet aux Etats membres d'adopter des lois nationales** dérogeant à certaines dispositions de la directive pour des raisons de sécurité nationale, tandis que la **RGPD ne prévoit pas de telles dérogations**.
- La directive **permet aux Etats membres de prévoir des exceptions à certaines obligations**, telles que l'obligation d'informer les personnes concernées, lorsque cela compromettrait l'efficacité d'une enquête ou d'une poursuite, tandis que le **RGPD ne prévoit pas de telles exceptions**
- La **directive prévoit des règles spécifiques pour le transfert de données à caractère personnel** vers les pays tiers ou des organisations internationales, tandis que le **RGPD contient des dispositions similaires mais plus générales**

Pour aller plus loin :

- https://www.cnil.fr/fr/directive-police-justice-de-quoi-parle-t
- http://formations-geomatiques.developpement-durable.gouv.fr/NAT009/ADL/Aspects_Juridique/co/d5_RGPD_1.html

II – Les impacts de la directive

A – Concernant le RGPD

2. Droit d'accès

4 objectifs principaux :

- **Transparence** : permet la personne concernée de **superviser**

- Légalité et réaction aux **illégalités dans le traitement :** Gatekeepers : prérequis et facilitateur pour l'exercice des **droits d'informations** restants

- Surveiller si une certaine illégalité a été effectivement corrigée et quand

- Déclencher des actions politiques, judiciaires et de prise de décision : Safe Harbor, Privacy Shield et New Privacy Shield

Dans la directive :

Focus sur : **personne concernée par rapport au responsable de traitement**

Pour aller plus loin :

- https://pure.uvt.nl/ws/portalfiles/portal/31965938/pdh18_dd_the_right_to_access_police_directive_Medina_Mitrakas_Rannenberg_.pdf
- https://www.demarches.interieur.gouv.fr/particuliers/fichiers-informatiques-donnees-personnelles

II – Les impacts de la directive

A – Concernant le RGPD

Informations sur le sujet des données en vertu du droit d'accès
Confirmation : les données sont traitées par le responsable de traitement
But du traitement + Base légale du traitement
Catégories de données à caractère personnel
(Catégories de) destinataires
Période de stockage envisagée /critères du stockage
Droits de rectification, d'effacement ou de restriction du traitement
Droit de déposer une plainte auprès de l'autorité de contrôle + Coordonnées de l'autorité de surveillance
Données à caractère personnel en cours de traitement + Informations sur l'origine des données
Confirmation que les données ont été transmises / divulguées

Quels sont les réels changements ?

Pour aller plus loin :

- https://pure.uvt.nl/ws/portalfiles/portal/31965938/pdh18_dd_the_right_to_access_police_directive_Medina_Mitrakas_Rannenberg_.pdf

- **L'accès direct devient la règle**, l'accès indirect l'exception
- **Le responsable de traitement doit communiquer avec la personne concernée de manière intelligible** et dans un délai convenable

Y a-t-il toujours un problème ?

1. Le droit **ne comprend pas d'informations essentielles** telles que les mesures de profilage et le **destinataire** des données;
2. Le fait que le droit soit exercé contre le responsable de traitement dans un monde avec de nombreux responsables de traitement pourrait rendre difficile l'obtention d'une vision complète de ses données à la personne concernée;
3. Les différents responsables de traitement sont sujets à différents cadres légaux et procédurau, ce qui cause une fragmentation

II – Les impacts de la directive

B – Concernant les autres domaines

- **Impacts sur le travail et la sécurité sociale :** http://ilo.org/dyn/natlex/natlex4.detail?p_lang=fr&p_isn=101948&p_country=EEU&p_count=906
- **Impacts sur la justice :** https://www.justice.fr/donnees-personnelles
- **Impacts sur les droits fondamentaux et les libertés :** Art. 8 Convention européenne
- **Impacts sur la coopération policière :** la directive facilite l'échange d'informations entre la police nationale et les autorités judiciaires afin d'améliorer la coopération dans la lutte contre le terrorisme et d'autres crimes graves en Europe.
- **Impacts sur la santé :** https://www.departement-information-medicale.com/blog/2016/05/10/reglement-europeen-relatif-a-la-protection-des-donnees-personnelles/
- **Impacts sur la directive PNR :** https://info.haas-avocats.com/droit-digital/directive-pnr-la-cjue-recadre-le-traitement-des-donnees-de-passagers-aeriens
- **Interactions avec la directive sur les preuves électroniques et le problème de l'accès aux données en dehors de l'UE:** https://eucrim.eu/news/edpb-criticises-e-evidence-proposals/
- **Intéractions avec l'IA**

III – Comment les Etats membres appliquent-ils cette directive ?

A - France

<u>Question</u> :

"M. Lionel Tardy attire l'attention du Ministre de la Justice sur l'état de la transposition des directives européennes. Il demande de communiquer le nombre de directives sous la responsabilité de son ministère qui sont **en attente de transposition**, en distinguant parmi celles pour lesquelles le **délai de transposition est passé**."

<u>Réponse</u> : En matière pénale, aucune directive européenne n'est soumise à un retard de transposition.

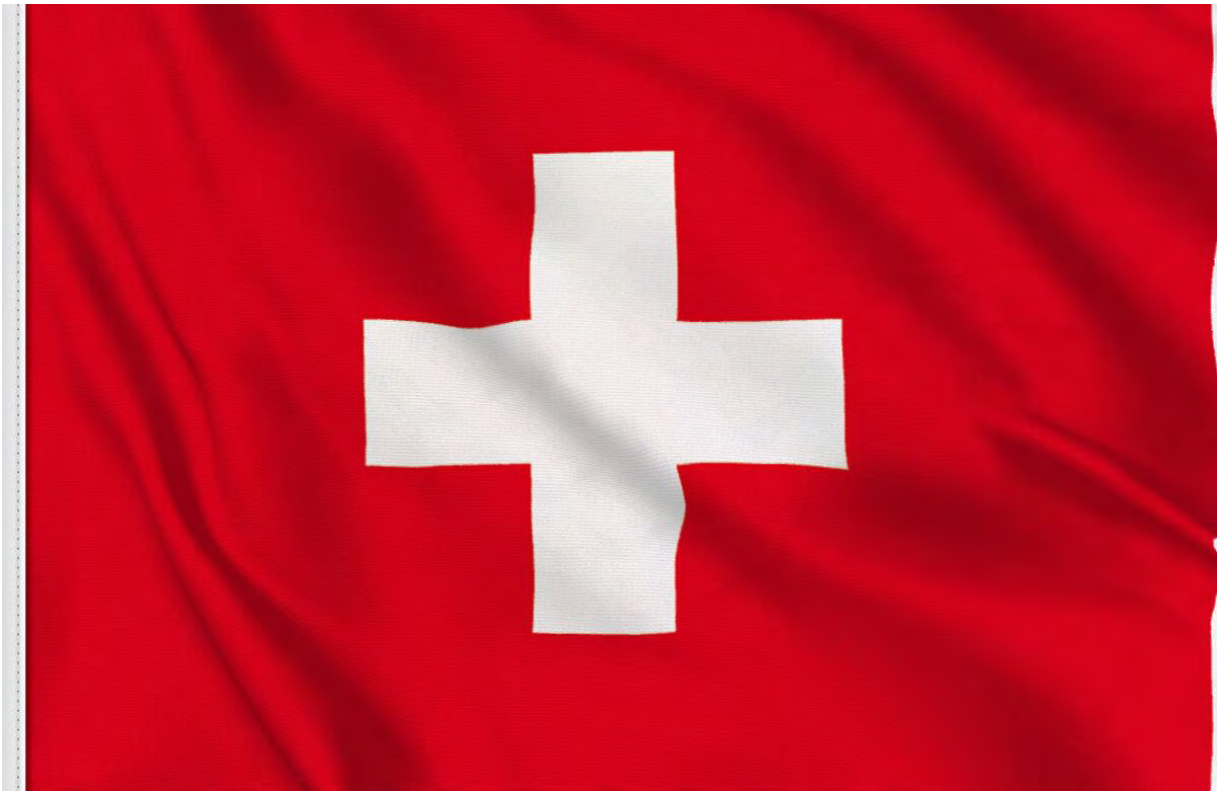
- https://www.senat.fr/ue/pac/EUR000007655.html
- https://questions.assemblee-nationale.fr/q14/14-81175QE.htm
- https://www.economie.gouv.fr/daj/lettre-de-la-daj-la-collecte-systematique-des-donnees-biometriques-et-genetiques-et-la
- https://www.laquadrature.net/files/applicabilit%C3%A9_2016_680.pdf
- https://docassas.u-paris2.fr/nuxeo/site/esupversions/5befab1b-68bd-4909-bd8c-94eb6f274d0d?inline
- https://www.dbfbruxelles.eu/wp-content/uploads/2020/05/LAVISDELEXPERTEUROPEEN6.pdf

III – Comment les Etats membres appliquent-ils cette directive ?

B - Suisse

Ajustements :

- Constitution
- Accord bilatéral entre la Suisse et l'UE
- Décision cadre



*Echange de notes du 1er septembre 2016 entre la Suisse et l'Union européenne concernant la reprise de la directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel 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 (Développement de l'acquis de Schengen

III – Comment les Etats membres appliquent-ils cette directive ?

C - Belgique

En Belgique, la police est même allée jusqu'à produire un **guide** :

https://polinfo.kluwer.be/NewsView.aspx?contentdomains=POLINFO&id=VS300641269&lang=fr

Commission pour le contrôle des dossiers de la police :

https://www.organedecontrole.be/organe-de-controle/r%C3%A9glementation

III – Comment les Etats membres appliquent-ils cette directive ?

D –Espagne

CJUE, 25 février 2021, C-658/19 :

La CJUE a condamné l'Espagne à payer **15 millions d'euros** et une pénalité journalière de 89,000€ **pour non-transposition au 6 mai 2018 des mesures necessaires pour executer à la directive** sur la protection des données à caractère personnel à des fins de prevention et de détection d'infractions pénales.

Dès lors: rapport de l'UE : normes acceptables mais les **autorités de contrôle ont besoin de plus de budget : des lignes directices du Comité européen de la protection des données sont nécessaires.**

Prochain rapport : 2026 😉

- https://www.abogacia.es/fr/actualidad/noticias/proteccion-de-datos-el-informe-de-la-comision-revela-un-alto-nivel-de-proteccion-de-los-derechos-de-las-personas-implicadas-en-procesos-penales/

Conclusion : ChatGPT

TH

La directive européenne 2016/680 pourrait-elle changer avec l'IA?

La directive européenne 2016/680 sur la protection des données pourrait être impactée par l'IA. L'IA soulève des défis en matière de protection de la vie privée, de consentement, de transparence et de responsabilité. Les technologies d'IA peuvent collecter et analyser de grandes quantités de données personnelles, ce qui nécessite une application rigoureuse des principes de protection des données. Les législateurs pourraient envisager d'adapter la directive existante pour inclure des dispositions spécifiques concernant l'utilisation de l'IA et les droits des individus. Cependant, il est important de noter que les modifications potentielles de la directive dépendent des décisions politiques et législatives prises par les autorités compétentes.

Merci

Maître Valérie Hayek

Hasperak Avocats

hayek.valerie@hasperakavocats.com

+33 7 61 82 21 53