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

## Data controller and processor

Alexandra Guerin-François

Paris, 19 September 2022

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

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

# Des notions au « rôle capital »

- Des obligations et des responsabilités spécifiques
  - Registre / DPO
- Au regard de la transparence due aux personnes concernées
- Des conséquences sur le « business model »

→ réutilisation ou non des données / rendre des comptes (sécurité, gestion des demandes etc. )

→ Dans les sanctions de la CNIL

RGPD

## CHAPITRE IV - Responsable du traitement et sous-traitant

Section 1 - Obligations générales

Article 24 - Responsabilité du responsable du traitement
Article 25 - Protection des données dès la conception et protection des données par défaut
Article 26 - Responsables conjoints du traitement
Article 27 - Représentants des responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union.
Article 28 - Sous-traitant
Article 29 - Traitement effectué sous l'autorité du responsable du traitement ou du sous-traitant
Article 30 - Registre des activités de traitement
Article 31 - Coopération avec l'autorité de contrôle

Section 2 - Sécurité des données à caractère personnel

Article 32 - Sécurité du traitement
Article 33 - Notification à l'autorité de contrôle d'une violation de données à caractère personnel
Article 34 - Communication à la personne concernée d'une violation de données à caractère personnel

Section 3 - Analyse d'impact relative à la protection des donnés et consultation préalable

Article 35 - Analyse d'impact relative à la protection des données
Article 36 - Consultation préalable

Section 4 - Délégué à la protection des données

Article 37 - Désignation du délégué à la protection des données
Article 38 - Fonction du délégué à la protection des données
Article 39 - Missions du délégué à la protection des données

Section 5 - Codes de conduite et certification

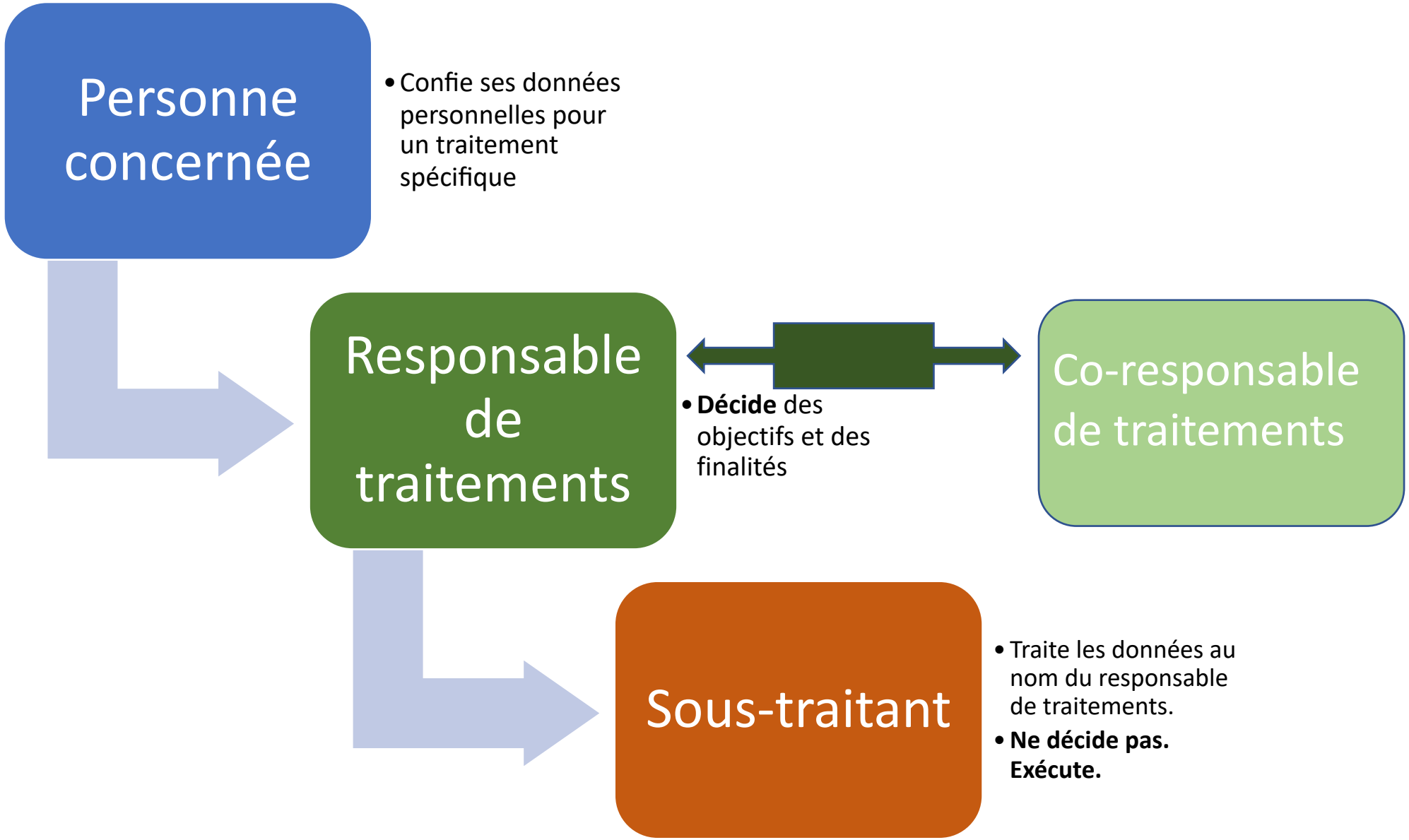
# Définition (art.4 RGPD)

**Responsable de traitements (art. 4 §7 RGPD)**
*la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui,* ***seul ou conjointement*** *avec d'autres,* ***<u>détermine les finalités et les moyens du traitement</u>***

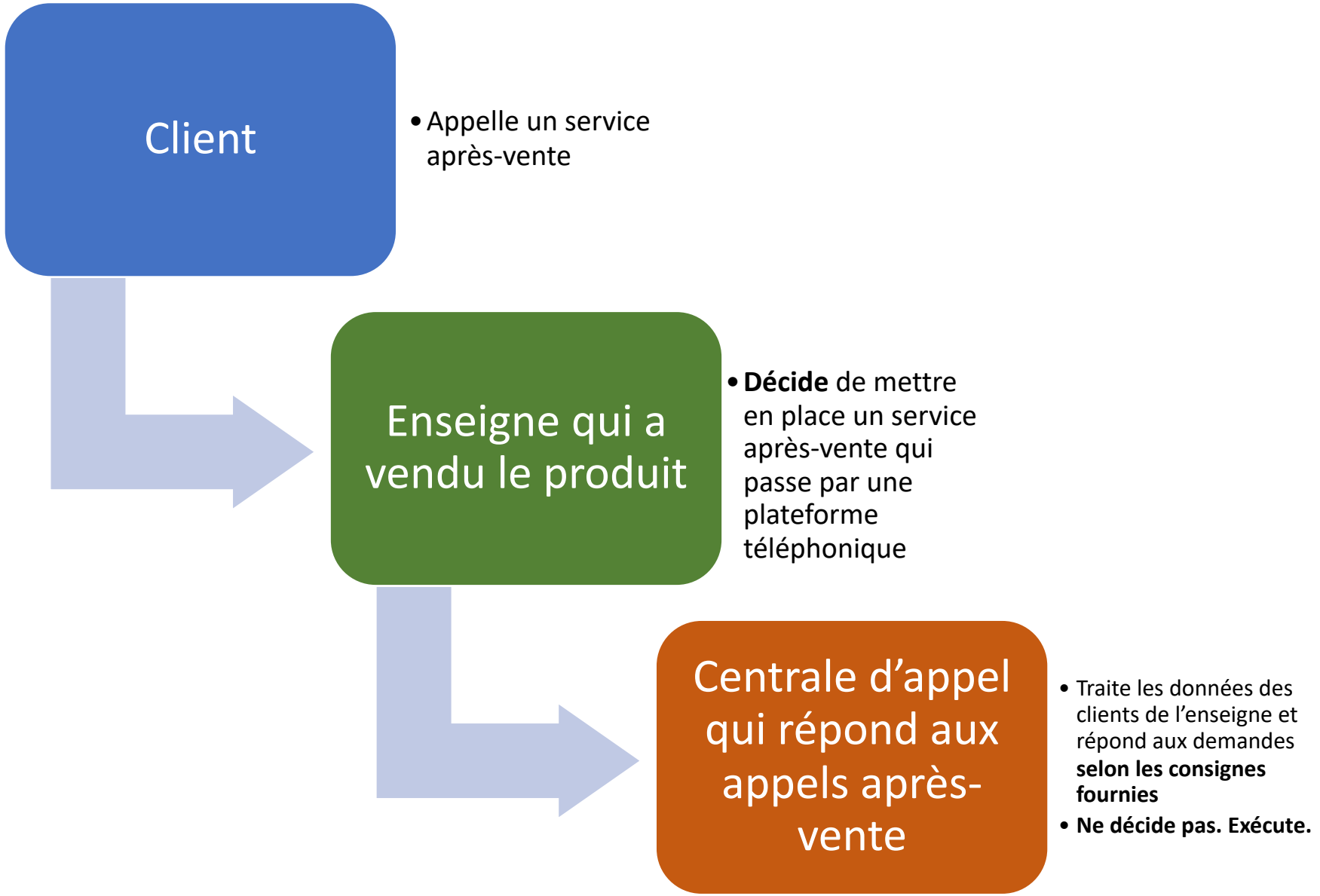
→ « *le responsable de traitement est la personne qui détermine les finalités du traitement mis en œuvre, c'est-à-dire* ***le résultat attendu ou recherché****, et les moyens de ce traitement, c'est-à-dire* ***la façon de parvenir à ce résultat*** » (CNIL, Monsanto, 26/07/2021)

**Sous-traitant (art. 4 §8 RGPD)**
*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*
→ aspects plus pratiques (« moyens non essentiels ») peuvent être à la discrétion du ST (EDPB, 07/2020)

Vocabulaire : prestataire / fournisseur / sous-traitant
Distinction : destinataire / tiers (art.4)


Personne concernée
• Confie ses données personnelles pour un traitement spécifique
Responsable de traitements
• **Décide** des objectifs et des finalités
Co-responsable de traitements
Sous-traitant
• Traite les données au nom du responsable de traitements.
• **Ne décide pas. Exécute.**

# Ex : centrale d’appel



# Exemples

## Recours à un sous-traitant

- Activité ponctuelle
  Ex: envoi d'un mailing
- Activité décentralisée
  Ex: gestion de la paie
  Ex: maintenance informatique
- Même sans avoir « réellement » accès aux données nominatives (EDPB 07/2020)
  Ex: laboratoire pharmaceutique en essais cliniques

## Pas Sous-traitant

- Outil sans décision sur les données
  Ex : un éditeur de logiciel, un fournisseur de matériel
- Mission qui ne porte pas sur le traitement des données
  Ex: avocat : mandat sur la représentation en justice et non sur le traitement

# Des qualifications parfois complexes

« ***appréciation concrète*** *prenant en compte l'ensemble des éléments permettant d'attribuer cette qualité à une entité. » (CNIL / EDPB)*

# Faisceau d'indices pour qualifier le RT au sein d'un groupe

**CNIL, n°SAN-2022-015 du 7 juillet 2022 concernant la société UBEEQO INTERNATIONAL**

La société Ubeeqo International détermine les finalités et les moyens des traitements relatifs à la création d'un compte utilisateur sur les applications mobiles ou le site web ubeeqo.com et à la collecte de données de géolocalisation des véhicules loués car :

- dans **sa politique de confidentialité** : RT.
- la société **détermine notamment, pour l'ensemble des filiales, les catégories de données** qui sont collectées lors du parcours d'inscription, telles que **les données de contact**.
- les traitements relatifs aux données de géolocalisation, sont de traitements **communs à l'ensemble des filiales** et que la société en a déterminé les différentes finalités (maintenance et performance du service, etc.)
- **une politique de durées de conservation des données unique, applicable tant à la société qu'à ses filiales**
- **deux systèmes d'informations, Inovia et Phoenix, qui sont chacun utilisés par plusieurs filiales**, et la **société peut accéder aux données à caractère personnel stockées dans ces deux systèmes.**

*Au demeurant, **l'éventualité d'une responsabilité conjointe de ses filiales est sans influence sur sa responsabilité propre à l'égard des traitements en cause**.*
***En effet, la présente délibération porte sur la responsabilité d'Ubeeqo International pour les manquements visés et non sur celle de ses éventuels responsables conjoints de traitements**.*

# Une société : plusieurs qualifications

*Exemple :* **CNIL, SLIMPAY, 28 décembre 2021**

*SLIMPAY : essentiel de son activité = services de paiements récurrents, mandats SEPA, etc.*

- ✓ ***la société SLIMPAY : ST*** *pour les traitements mis en œuvre dans le cadre des services fournis aux marchands, responsables de traitement, dans la mesure où la société ne détermine pas les finalités de traitement des données.*
  - → *la société fait elle-même appel, dans le cadre des services fournis aux marchands, aux services de sous-traitants :* ***ST de second niveau*** *vis-à-vis des marchands.*
- ✓ ***la société SLIMPAY : RT*** *pour un un traitement de recherche interne concernant un mécanisme de lutte contre la fraude, dont elle a déterminé seule les finalités et les moyens. La société indique d'ailleurs elle-même agir en tant que responsable de traitement, dans la notification complémentaire de violation de données qu'elle a transmise à la CNIL le 26 février 2020.* »

# Identifier les rôles en cas de silence des parties

**Faisceau d'indices pour qualifier le RT / le sous-traitant**

**CNIL, n°SAN-2021-012 du 26 juillet 2021 concernant la société MONSANTO COMPANY**

Evaluation in concreto

- ✓ **le suivi des tâches** réalisées par FLEISHMAN-HILLARD, et notamment l'organisation **d'échanges quotidiens** entre les équipes, de points hebdomadaires, mensuels et trimestriels permettant à la société MONSANTO de suivre l'avancée des tâches confiées à FLEISHMAN-HILLARD et la livraison du travail réalisé ou en cours de réalisation.
- ✓ **c'est le fait pour la société MONSANTO, société donneuse d'ordre, de décider d'accepter la proposition faite par la société FLEISHMAN-HILLARD, et de lui demander contractuellement de réaliser des opérations pour son compte en tant que prestataire, qui a permis au traitement d'exister**

Non pertinent dans l'évaluation :

- ✓ ne ne pas avoir finalement utilisé le fichier établi
- ✓ le fait que FLEISHMAN-HILLARD gère les demandes d'accès

**Conséquence** : rôles non définis dans le contrat → requalification en RT/ DT → sanction pour défaut de clause contractuelle art. 28

# La réutilisation

***Le sous-traitant*** *et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel,* ***ne peut pas traiter ces données, excepté sur instruction du responsable du traitement,*** *à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre*. Art. 29 RGPD

**Principe :** Le sous-traitant qui réutiliserait les données de sa propre initiative **serait qualifié de responsable de ce traitement** et **passible de sanctions** pour ne pas avoir agi dans le respect des instructions du responsable du traitement initial.

**Exception : une autorisation du client (RT)**

- ✓ **déterminer si ce traitement ultérieur est compatible avec la finalité pour laquelle les données ont été initialement collectées test de compatibilité)**

  ex: hébergeur : amélioration : oui si anonymisation/ non si prospection commerciale

- ✓ **autorisation spécifique et écrite (non préalable et générale)**
- ✓ **information des personnes**

cf/ **Sous-traitants : la réutilisation de données confiées par un responsable de traitement (CNIL, janvier 2022)**

# Relation RT/ST encadrée par l'art. 28 GDPR : le DPA

Le RT *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. (***Art. 28 RGPD)**

Des obligations listées dans l'article 28 :

- **Description du traitement** : Définition de l'objet, la durée, la nature et la finalité du traitement, et des catégories de données à caractère personnel et des catégories de personnes concernées.
- **Obligation de transparence** : Conditions pour le recours à un **sous-traitant ultérieur** : autorisation au cas par cas ou générale (liste des ST dans le registre du ST) / Agir sur **instructions documentées** / prévoir la fin : restitution ou destruction des données / possibilité d'**audit**
- **Obligation de garantir la sécurité :** prendre les mesures nécessaires/ former les salariés/ notifier toutes violations
- **Obligation de collaboration, d'alerte et de conseil avec le RT** : droits des personnes / PIA / contrôle
- **Le cas du transfert hors UE**

Clauses contractuelles types (CCT) entre les responsables de traitement et les sous-traitants publiées par la Commission européenne (4 juin 2021)

# Une conformité contractuelle et réelle

- Le contrat doit comporter **l'ensemble des clauses art. 28**

**CNIL, SLIMPAY, 28 décembre 2021 (sanction : 180.000 euros)**

- ✓ Sanction car **pas les mentions prévues par l'article 28 §3 du RGPD** (partiellement ou totalement)
- ✓ négociations en cours pour se mettre en conformité : preuve que **pas en conformité au moment des investigations** menées par la CNIL
- ✓ le **questionnaire** envoyé est complété par les sous-traitants ultérieurs est insuffisant.

*le questionnaire n'a qu'une valeur déclarative : il ne constitue pas un acte juridique contraignant par lequel* ***le sous-traitant ultérieur s'engage à respecter les éléments définis.***

- **Pas seulement une « reproduction » de l'article 28 / inclure des « informations plus spécifiques et concrètes sur la manière dont les conditions sont remplies et le niveau de sécurité requis » (EDPB, lignes directrices 07/2020)**

# Qui est responsable du contrat?

« *le fait que* ***l'obligation résultant de l'article 28, paragraphe 3,*** *du RGPD incombe* ***tant au responsable de traitement qu'au sous-traitant*** *est sans incidence sur l'existence d'une* ***responsabilité propre du sous-traitant****.*

→ *c'est la société elle-même qui transmet aux laboratoires* ***ses propres conditions générales de vente qui font office d'encadrement contractuel*** *au titre du RGPD.* »

**CNIL, n° SAN-2022-009 du 15 avril 2022 concernant la société DEDALUS BIOLOGIE**

« ***le déséquilibre entre le pouvoir contractuel*** *d'un petit responsable du traitement et celui de grands prestataires de services ne devrait* ***pas être considéré comme une justification*** *permettant au responsable du traitement d'accepter des clauses et des conditions contractuelles non conformes à la législation en matière de protection des données, pas plus qu'il n'exonère le responsable du traitement de ses obligations en la matière.* » lignes directrices EDPB 07/2020

# Le suivi du ST à la charge du RT

Le ST : « ***met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect*** *des obligations prévues au présent article* ***et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits***. » Art 28 h) RGPD

- « *la circonstance selon laquelle une violation de données ait pu avoir* ***pour origine une erreur commise par un sous-traitant est sans influence sur l'obligation pesant sur le responsable de traitement d'assurer un suivi rigoureux*** *des actions menées par ce dernier.* » **sanction CNIL 6 septembre 2018**

- « *la circonstance que des opérations de traitement de données soient confiées à des sous-traitants* ***ne décharge pas le responsable du traitement de la responsabilité qui lui incombe de préserver la sécurité des données […]****; que* ***la seule mention, dans le contrat*** *liant la société Orange à son prestataire, la société Gutenberg,* ***d'une obligation de sécurité mise à la charge de cette dernière et de ses sous-traitants ne dispensait pas la société Orange de prendre des mesures destinées à s'assurer elle-même que la sécurité de ses données était préservée*** » **CE 30 décembre 2015**

# Par des mesures de contrôle

- « *la société Orange n'avait* ***pas fait procéder à un audit de sécurité*** *sur l'application qui avait été spécialement définie pour la prospection commerciale de ses clients* »

  **CE 30 décembre 2015 Orange**

- « *Bien que l'organisme ait donné des instructions spécifiques en matière d'anonymisation et de sécurité à son sous-traitant, il apparaît qu'il n'a* ***pas suivi l'exécution de ces instructions et n'a pas exercé un contrôle satisfaisant et régulier*** *sur les mesures techniques et organisationnelles mise en œuvre par son sous-traitant pour assurer la conformité au RGPD et, notamment pour assurer l'anonymisation et la sécurité des données à caractère personnel traitées* »

  **CNIL Infogreffe 8 septembre 2022**

# Le ST aussi peut être sanctionné

- S'il **traite des données au-delà des instructions** données par les responsables de traitement (art. 29 RGPD)

« *la société ne saurait se prévaloir d'un outil inadapté pour justifier d'avoir* ***outrepassé les instructions*** *des responsables de traitement. Elle aurait pu, par exemple, opter pour un autre outil lui permettant de respecter les instructions données par ses clients, comme elle indique le faire désormais, ou a minima supprimer toutes les données qui n'auraient pas dû être extraites.* » **CNIL, n° SAN-2022-009 du 15 avril 2022 concernant la société DEDALUS BIOLOGIE (1,5 millions€)**

- **Pour défaut la sécurité (art.32 Dedalus)**

- **Pour manquement à l'obligation d'encadrer par un acte juridique formalisé les traitements effectués pour le compte du responsable de traitement (article 28 du RGPD)**

- **Pour manquement liés à des obligations qui lui sont propres** : le registre du ST / la désignation d'un DPO

# La responsabilité conjointe

**Critères** : une **décision commune** prise par deux entités ou plus, ou des **décisions convergentes** adoptées par deux entités ou plus au sujet des finalités et des moyens **essentiels** du traitement

→ « inextricablement lié » cf. EDPB

**Exemple**: voyage à forfait avec plateforme commun (agences de voyages, compagnie aérienne, hôtels)

**Conséquence** : **Définir de manière transparente les obligations respectives** des responsables conjoints du traitement aux fins d'assurer le respect des exigences du RGPD **sous la forme d'un accord contraignant**

→ Principes généraux de la protection des données, base juridique, mesures de sécurité, obligation de notification, AIPD, recours à des ST, transferts, contacts pour les personnes et les autorités (cf. EDPB 07/2020)

*ATTENTION*

*« Si l'entité impliquée dans le traitement **ne poursuit aucune finalité propre** dans le cadre du traitement, mais est simplement rémunérée pour les services rendus, elle agit comme sous-traitant plutôt que comme responsable conjoint du traitement. » (lignes directrices de l'EDPB 07/2020 RT, ST)*

Attention : les autorités de contrôle ne sont pas liés par l'accord sur la qualité de RT conjoints / contact désigné (cf. EDPB 07/2020)

# Une notion large

**Le fait que l'une des parties n'ait pas accès aux données à caractère personnel traitées ne suffit pas à exclure une responsabilité conjointe du traitement**

CJUE, l'affaire Témoins de Jéhovah, C-25/17 (10/07/2018)

« *une communauté religieuse doit être considérée comme étant responsable, conjointement avec ses membres prédicateurs, des traitements de données à caractère personnel effectués par ces derniers dans le cadre d'une activité de prédication de porte-à-porte* ***organisée, coordonnée et encouragée par cette communauté***

*…* ***pas nécessaire que ladite communauté ait accès aux données*** *ou qu'il devait être établi qu'elle avait* ***donné à ses membres des lignes directrices écrites ou des consignes relativement à ces traitements.*** »

# L’exemple des réseaux sociaux

**Le fait que les données ne soient pas traitées pour la même finalité mais des finalités étroitement liées ou complémentaires ne suffit pas à exclure une responsabilité conjointe du traitement.**

**CJUE Fan page Wirtschaftsakademie Schleswig-Holstein, 5 juin 2018**

*« le traitement de données à caractère personnel au moyen de statistiques établies à partir des visites sur une page fan visent à permettre, d’une part, à* ***Facebook*** *d’améliorer son système de publicité qu’il diffuse à travers son réseau et, d’autre part, à* ***l’administrateur de la page fan*** *d’obtenir des statistiques à des fins de gestion de la promotion de son activité. Dans cette affaire,* ***chaque entité poursuit son propre intérêt, mais les deux parties participent à la détermination des finalités (et des moyens) du traitement des données à caractère personnel des visiteurs de la page fan*** *»*

*A NOTER : la responsabilité conjointe de plusieurs acteurs pour un même traitement, en vertu de cette disposition, ne présuppose pas que* ***chacun d’eux ait accès aux données à caractère personnel concernées***

**CJUE Fashion ID** C-40/17, 29 juillet 2019

*« L’exploitant d’un site Internet participe à la détermination des finalités (et des moyens) du traitement en intégrant un plug-in social dans un site Internet afin d’optimiser la publicité pour ses produits en les rendant plus visibles sur le réseau social.*

*→ les opérations de traitement de données à caractère personnel dont* ***Fashion ID est susceptible de déterminer, conjointement avec Facebook Ireland, les finalités et les moyens*** *sont […] la collecte et la* ***communication par transmission des données à caractère personnel des visiteurs de son site Internet****.* ***E***

***En revanche****, au regard desdites informations, il apparaît, de prime abord, exclu que Fashion ID détermine les finalités et les moyens des opérations de traitement de données à caractère personnel* ***ultérieures, effectuées par Facebook Ireland après leur transmission à cette dernière, de sorte que Fashion ID ne saurait être considérée comme étant responsable de ces opérations****»*

# Ressources

- ✓ Guide sous-traitant de la CNIL (2017)
- ✓ Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD
- ✓ Décision d'exécution (UE) 2021/915 de la Commission du 4 juin 2021 relative aux clauses contractuelles types entre les responsables du traitement et les sous-traitants au titre de l'article 28, paragraphe 7, du règlement (UE) 2016/679 du Parlement européen et du Conseil et de l'article 29, paragraphe 7, du règlement (UE) 2018/1725 du Parlement européen et du Conseil (Texte présentant de l'intérêt pour l'EEE)

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

## Introduction to the GDPR

Anne Fontanille

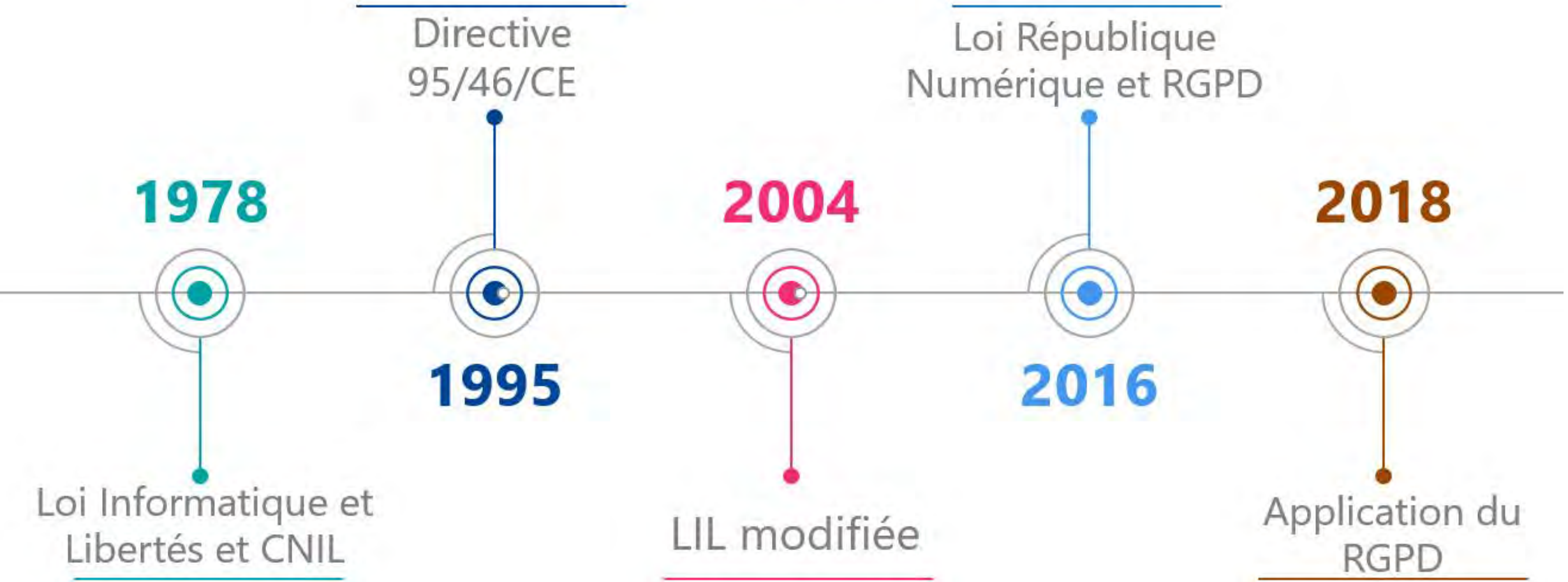
Paris, 19 September 2022

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

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

# Genèse et évolution



# Champ d'application

1. Un traitement de données personnelles...

2. ...effectués par un RT ou un ST...

établi sur le territoire de l'UE *critère de l'établissement*

ou

visant des personnes sur trouvant dans l'UE *critère du ciblage*

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

# Les principes clés

01 Licéité

Finalité 02

03

Minimisation

Exactitude

04

05

Durée de conservation

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

# Logique de responsabilisation de tous les acteurs

1. Formalités allégées
2. Documenter
3. Accompagnement des autorités de contrôle
4. Sanctions renforcées

# Principes généraux en cas de transfert

- **Principe de libre circulation des données au sein de l'Union européenne** = niveau de protection des droits et libertés des personnes à l'égard du traitement de données équivalent dans tous les États membres de l'UE

- **Principe d'interdiction des transferts** de données en dehors de l'Espace Economique Européen (EEE = UE + Islande, Norvège, Liechtenstein)

- **Exception** : … sauf si le pays ou l'entreprise destinataire **assure un niveau de protection suffisant et approprié**

https://www.cnil.fr/fr/transferer-des-donnees-hors-de-lue

# Comment assurer un niveau de protection suffisant ?

## RGPD : une boîte à outils renouvelée et diversifiée pour les transferts internationaux de données

*Outils de transfert sans autorisation préalable de la CNIL*

**BCR**
Approuvées
(art. 47 du RGPD)

**Certification**
Approuvée
(art. 42 et 46-2 (f) du RGPD)

**Code de conduite**
Approuvé
(art. 40 et 46-2 (e) du RGPD)

**Décisions d'adéquation**
(art.45 du RGPD)

**Clauses**
Contractuelles types
*Adoptées par la Commission européenne*
(art. 46-2(c) du RGPD)

**Clauses**
Contractuelles types
*Adoptées par les autorités*
(art. 46-2(d) du RGPD)

**Instruments**
juridiquement contraignants et exécutoires entre autorités organismes publics
(art. 46-2(a) du RGPD)

**Dérogations**
(art. 49 du RGPD)

*Outils de transfert avec autorisation préalable de la CNIL*

**Clauses contractuelles ad hoc**
(art. 46.3.a du RGPD)

**Dispositions intégrées**
dans les arrangements administratifs entre autorités/organismes publics
(art. 46.3.b du RGPD)

**Légende**

- Outil existant
- Référentiel mis à jour RGPD
- Nouvel outil

# Les outils proposés par la CNIL

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

## Le MOOC de la CNIL est de retour dans une nouvelle version enrichie

*27 juin 2022*

*L'atelier RGPD est une formation en ligne gratuite, illimitée et ouverte à tous (Mooc). Elle permet de sensibiliser les professionnels à la protection des données et d'accompagner leur mise en conformité. Dans cette nouvelle version, la CNIL propose un nouveau module dédié aux collectivités territoriales.*

DÉCOUVREZ

**L'ATELIER RGPD**

pia | analyse d'impact sur la protection des données
privacy impact assessment

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

## The principle of consent

Florence Ivanier

Paris, 19 September 2022

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. Focus sur le caractère libre du consentement: déséquilibre des rapports de force & conditionnalité
5. 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
*The consecration  of consent, a corollary of informational self-determination*

## 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
*Consent is one of the 6 legal bases for processing*

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 (1/2)
*Characteristics and conditions of validity of consent*

*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 (2/2)
# Characteristics and conditions of validity of consent

## 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. Focus sur le caractère libre du consentement: déséquilibre des rapports de force & conditionnalité
*Focus on a consent freely given: power imbalance & conditionality*

**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. 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*

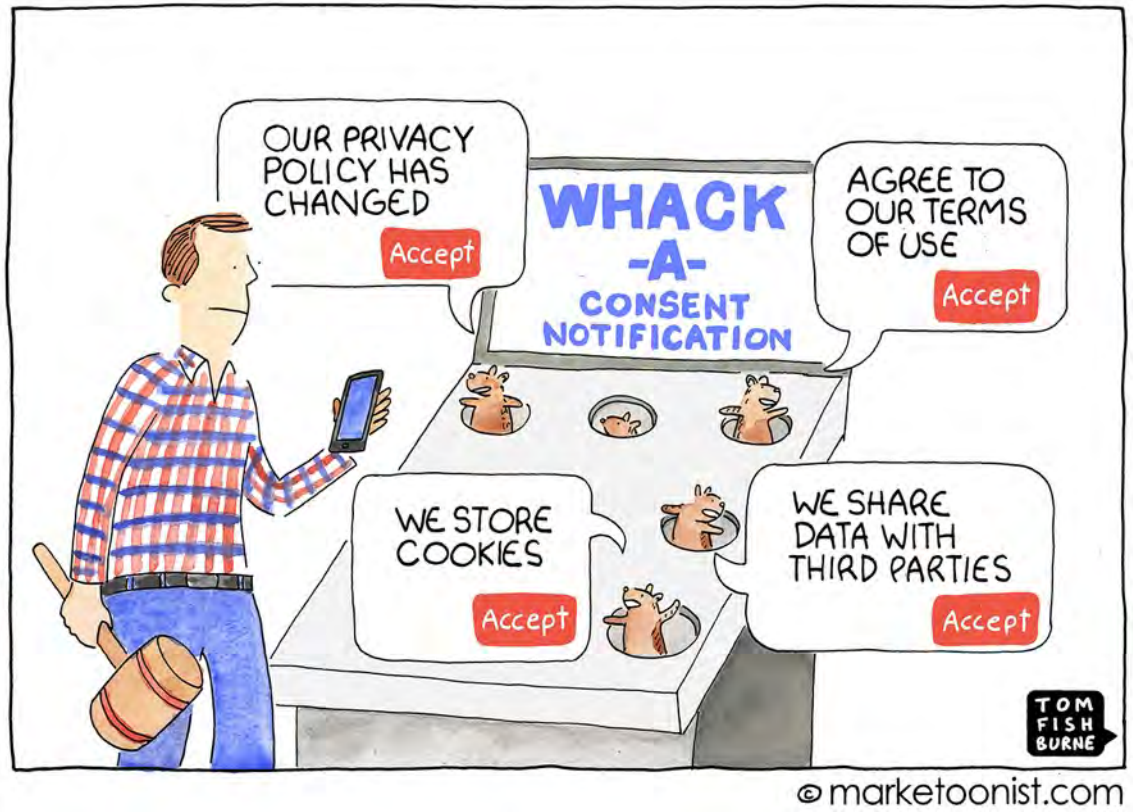
*2 exceptions:*

*- 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.

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

## Transfers of personal data to third countries

Jérôme Deroulez

Paris, 19 September 2022

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

# Transferts de données personnelles vers des pays tiers: le cadre juridique

Quels transferts?

- Le champ d'application matériel du RGPD (article 2) – voir les exceptions prévues, notamment en matière de prévention et de détection des infractions pénales ou le traitement de données par les institutions de l'Union
- champ d'application territorial du RGPD (article 3)

Article 3§1: Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, **que le traitement ait lieu ou non dans l'Union.**

Article 3§2: Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:

a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou

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

*Exemple: un sous-traitant hors de l'Union européenne dont les traitements entrent dans le champ de l'article 3 qui transfère ces données à un autre sous-traitant hors UE devra appliquer le cadre du RGPD à ces transferts*

# Transferts de données personnelles vers des pays tiers: le cadre juridique

Un cadre juridique hérité de la directive 45/46

Chapitre IV – Transferts de données personnelles vers des pays tiers

- Article 25 – Principes (transferts et principe d'adéquation) – procédure en vue de constater le niveau d'adéquation – article 31 (comité représentant les Etats membres et présidé par la Commission – dans le cadre des mesures d'exécution communautaires)
- Articles 26 – Dérogations (consentement, exécution d'un contrat, sauvegarde d'un intérêt public important, sauvegarde de l'intérêt vital de la personne, transfert intervenant au départ d'un registre public)

Et de la décision-cadre 2008/977 relative à la protection des données personnelles traitées dans le cadre de la coopération policière et judiciaire, en matière pénale – article 13 (transferts aux autorités compétentes d'Etats tiers ou à des instances internationales) et 14 (transmission à des personnes privées dans les Etats membres)

# Transferts de données personnelles vers des pays tiers: le cadre juridique

Un cadre repris et structuré par le RGPD

*Pour mémoire:*

- *Le RGPD a pour objet de permettre le respect du droit fondamental à la protection des données personnelles de toute personne (article 8§1 de la Charte des droits fondamentaux de l'Union européenne)*
- *Le traité de Lisbonne prévoir une procédure spécifique en matière de protection des données personnelles (article 16 TFUE, reprenant les dispositions de l'article 286 TCE et soulignant ce droit, la procédure applicable et le nécessaire contrôle par des autorités indépendantes)*

# Transferts de données personnelles vers des pays tiers: le cadre juridique

**Un cadre repris et structuré par le RGPD**

Chapitre V – transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales

Article 44 – Principe général applicable aux transferts

Article 45 – Transferts fondés sur une décision d'adéquation

Article 46 – Transferts moyennant des garanties appropriées

Article 47 – Règles d'entreprise contraignantes (BCR)

Article 48 – Transferts ou divulgations non autorisées par le droit de l'Union

Article 49 – Dérogations pour des situations particulières

Article 50 – Coopération internationale dans le domaine de la protection des données

# Transferts de données personnelles vers des pays tiers: le cadre juridique

**<u>Un cadre repris et structuré par le RGPD et qui doit s'apprécier en prenant en compte les aspects suivants:</u>**

- le contexte d'explosion des transferts de données
- le renforcement par le RGPD des obligations mises à la charge des responsables de traitement et des sous-traitants (respect des principes des articles 5 et 6 du RGPD notamment)
- le renforcement des compétences des autorités de contrôle et notamment en terme de coopération entre autorité chef de file et autres autorités
- des questions au quotidien pour les RT/ST

# Transferts de données personnelles vers des pays tiers: le cadre juridique

**Article 44 – <u>Principe général</u> applicable aux transferts**

**Un transfert**, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert **ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant**, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. **Toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis.**

# Transferts de données personnelles vers des pays tiers: le cadre juridique

**Article 44 – Principe général applicable aux transferts**

Un principe clé du RGPD et un enjeu d'effectivité du règlement

Une obligation mise à la charge du responsable de traitement et du sous-traitant (à voir sur les conséquences pratiques, notamment en terme de suivi des sous-traitants)

**Un objectif: assurer que le niveau de protection des personnes physiques prévu par le règlement ne soit pas compromis**

# Transferts de données personnelles vers des pays tiers: le cadre juridique

**Article 45 – Transferts fondés sur une décision d'adéquation**

Le principe: Un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un **niveau de protection adéquat**. Un tel transfert ne nécessite pas d'autorisation spécifique.

Une procédure prévue à l'article 45§2 (prise en compte de l'état de droit, de la législation pertinente, de l'existence et du fonctionnement d'autorités indépendantes, des engagements internationaux pris…) et la possibilité pour la Commission d'abroger, de modifier ou de suspendre sa décision d'adéquation (cf Royaume-Uni)

Etat des lieux : Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom under the GDPR and the LED, and Uruguay as providing adequate protection.

# Transferts de données personnelles vers des pays tiers: le cadre juridique

**Article 45 – Transferts fondés sur une décision d'adéquation**

Un outil clé pour les praticiens

Un outil de **soft power** (en matière de protection des données et au-delà)

Vers une norme RGPD/GDPR internationale

**Les décisions d'adéquation: un outil politique** (jurisprudence de la CJUE sur le Safe Harbor (arrêt du 6 octobre 2015) et le Privacy Shield (arrêt du 16 juillet 2020 – Annulation de la décision d'exécution de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-Etats-Unis ).

# Transferts de données personnelles vers des pays tiers: le cadre juridique

## **Article 45 – Transferts fondés sur une <u>décision d'adéquation</u>** (CJUE - arrêt du 16 juillet 2020)

*Selon la Cour, les limitations de la protection des données à caractère personnel qui découlent de la réglementation interne des États-Unis portant sur l'accès et l'utilisation, par les autorités publiques américaines, de telles données transférées depuis l'Union vers ce pays tiers, et que la Commission a évaluées dans la décision 2016/1250,* ***ne sont pas encadrées d'une manière à répondre à des exigences substantiellement équivalentes à celles requises, en droit de l'Union, par le principe de proportionnalité****, en ce que les programmes de surveillance fondés sur cette réglementation ne sont pas limités au strict nécessaire*

***les personnes dont les données à caractère personnel sont transférées vers un pays tiers sur le fondement de clauses types de protection des données doivent bénéficier d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union par ce règlement, lu à la lumière de la Charte****. Dans ce contexte, elle précise que l'évaluation de ce niveau de protection doit prendre en compte tant les stipulations contractuelles convenues entre l'exportateur des données établi dans l'Union et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données ainsi transférées, les éléments pertinents du système juridique de celui-ci.*

*Quant à* ***l'exigence de protection juridictionnelle****, la Cour juge que, contrairement à ce que la Commission a considéré dans la décision 2016/1250, le mécanisme de médiation visé par cette décision ne fournit pas à ces personnes une voie de recours devant un organe offrant des garanties substantiellement équivalentes à celles requises en droit de l'Union, de nature à assurer tant l'indépendance du médiateur prévu par ce mécanisme que l'existence de normes habilitant ledit médiateur à adopter des décisions contraignantes à l'égard des services de renseignement américains. Pour toutes ces raisons, la Cour déclare la décision 2016/1250 invalide.*

# Transferts de données personnelles vers des pays tiers: le cadre juridique

## Article 46 – Transferts moyennant des garanties appropriées

Le principe: En l'absence de décision en vertu de l'article 45, paragraphe 3, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que s'il a prévu des garanties appropriées et **à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives**

Les outils:

- Un instrument juridiquement contraignant et exécutoire entre autorités
- Des règles d'entreprises contraignantes (BCR)
- Des clauses types de protection des données (adoptées par la Commission européenne ou une autorité de contrôle)
- Un code de conduite
- Un mécanisme de certification
- Sous réserve de l'autorisation de l'autorité compétente, des clauses contractuelles entre RT et ST ou des dispositions à intégrer dans des arrangements administratifs

# Transferts de données personnelles vers des pays tiers: le cadre juridique

**Article 46 – Transferts moyennant des garanties appropriées**

Le cas spécifique des clauses contractuelles types de la Commission européenne:

- Les précédentes décisions 2001/497/CE ([5]) et 2010/87/UE ([6]) de la Commission contenant des clauses contractuelles types visant à faciliter le transfert de données à caractère personnel d'un responsable du traitement établi dans l'Union à un responsable du traitement ou à un sous-traitant établi dans un pays tiers qui n'offre pas un niveau de protection adéquat (directive 95/46)

- Les nouvelles CCT de la Commission européenne (décision d'exécution du 4 juin 2021 - https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32021D0914&from=FR#d1e32-58-1) qui devront être utilisées après le 27 décembre 2022

- La mise en en place de 4 modules (RT-RT / RT-ST / ST-ST / ST-RT)

# Transferts de données personnelles vers des pays tiers: le cadre juridique

**Article 46 – Transferts moyennant des garanties appropriées**

Le cas spécifique des clauses contractuelles types de la Commission européenne:

- Un cadre formalisé qui ne prévient pas le responsable de traitement de ses obligations générales et notamment:
- Une obligation d'information des personnes concernées
- Une obligation de veiller au respect des droits des personnes concernées (minimisation, conservation, sécurité des données…)
- Une obligation de documentation des mesures

La Commission a apporté des clarifications sur le recours aux SCC (https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf ) et rappelé la nécessité de mener une analyse d'impact spécifique (point 21)

# Transferts de données personnelles vers des pays tiers: le cadre juridique

**Article 47 – Règles d'entreprise contraignantes / BCR**

Les BCR ont fait l'objet d'avis du G29 qui a eu un rôle actif dans leur mise en oeuvre (avis de 2003, 200, 2008 et 2017). Elles ont été formalisées par le RGPD.

Il s'agit de règles qui doivent être réellement contraignantes pour un groupe d'entreprises ou des groupes d'entreprises, qui confèrent des droits opposables aux personnes concernées et qui répondent aux critères de l'article 47§2 (les BCR doivent inclure des informations sur les transferts, la mise en œuvre des principes généraux du RGPD, les droits des personnes, l'information sur les BCR, les procédures de réclamation ou de coopération avec l'autorité de contrôle etc…).

Elles constituent une « bulle juridique » pour un groupe d'entreprise garantissant le respect des standards du RGPD.

Ces règles sont approuvées par l'autorité de contrôle compétente (mécanisme de contrôle de cohérence – article 63 RGPD)

# Transferts de données personnelles vers des pays tiers: le cadre juridique

## Article 49 - Dérogations pour les situations particulières

Existence de dérogations hors décision d'adéquation ou garanties appropriées:

- Consentement explicite
- Exécution d'un contrat
- Transfert nécessaire à l'exécution d'un contrat dans l'intérêt de la personne concernée
- Transfert nécessaire pour des motifs d'intérêt public
- Transfert nécessaire pour la constatation, l'exercice ou la défense de droits en justice
- Transfert nécessaire pour la sauvegarde des intérêts vitaux de la personne concernée
- Transfert au départ d'un registre destiné à ouvrir des informations au public

Un transfert peut encore avoir lieu dans des circonstances spécifiques – ARTICLE 49§1 (absence de caractère répétitif, nombre limité de personnes, contrôle des modalités et évaluation par le RT, information de l'autorité de contrôle de ce transfert, information de la personne concernée par le RT du transfert et des intérêts légitimes poursuivis).

# Transferts de données personnelles vers des pays tiers: conclusion

**A retenir:**

- **Un cadre évolutif (SCC et BCR notamment)**
- **Des transferts sous contrôle (CJUE notamment)**
- **Une vigilance nécessaire pour les RT/ST**
- **Un signal de l'exportation du RGPD dans le monde**
- **Quelle effectivité dans la vie des affaires?**

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

## Rights of the data subject, including rights in criminal investigations and proceedings

Michalis Kosmopoulos

Paris, 19 September 2022

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

# Data Subjects Rights

## 1) Regulation (EU) 2016/679 - GDPR

## Chapter III – Rights of the Data Subject

*Section 1 – Transparency and modalities (Article 12)*
*Section 2 – Information and Access to Personal Data (Articles 13-15)*
*Section 3 – Rectification and erasure (Article 16-20)*
*Section 4 – Right to object and automated individual decision-making (Article 21-22)*
*Section 5 – Restrictions (Article 23)*

## 2) Directive (EU) 2016/680 – Law Enforcement Directive

## Chapter III – Rights of the data subject

*Articles 12-18*

# Data Subjects Rights

## GDPR

*(Chapter III - art. 12-23)*

→ Right to be informed

→ Right of Access

→ Right to Rectification

→ Right to Erasure ("to be forgotten")

→ Right to Restriction of processing

→ Right to Data portability

→ Right to Object

→ Right not to be subject to a decision based solely on automated processing, including profiling

→ Right to Withdraw consent

→ Right to lodge a complaint with a supervisory authority

Data Subjects Rights

## Law Enforcement Directive

*(Chapter III, art. 12-18)*

- → Right to be informed
- → Right of Access
- → Right to Rectification
- → Right to Erasure
- → Right to Restriction of processing

***Article 18***

*Rights of the data subject in criminal investigations and proceedings*

*Member States may provide for the exercise of the rights referred to in Articles 13, 14 and 16 to be carried out in accordance with Member State law where the personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings.*

# Transparency and Modalities (art. 12)

- Communication and information in concise, transparent, intelligible and easily accessible form, using clear and plain language

- In writing, or by other means (electronic means or orally, if requested by the data subject)

- Controller shall facilitate the exercise of data subject rights and not refuse to act
Exception: not in a position to identify the data subject

- Information in one (1) month, extendable by two (2) months

- Controller shall inform the data subject for the reasons for delay or for not taking action and on the possibility of lodging a complaint with a supervisory authority or seek a judicial remedy

- Free of charge except if manifestly unfounded or excessive in particular because of their repetitive character, the controller may either:
(a) charge a reasonable fee taking into account the administrative costs
(b) refuse to act on the request

- Confirmation of identity

# Right to be informed (art. 13-14)

- At the time of data collection (13 par. 1 and 2)

- When processing changes purpose (art. 13 par. 3)

- At the time controller receives data from third party (art. 14)

- In one (1) month or first communication or first disclosure

- When data subject requests information (art. 15)

# Right to be informed (art. 13-14)

## THE PRIVACY NOTICE

### WHO
Controller, contact details, representative, DPO

### WHY
Purpose, legal basis legitimate interest

### TO WHOM
Recipients, Transfers

### DATA SUBJECT RIGHTS

### AUTOMATED DECISION MAKING
Logic, significance, consequences

### WHAT
Personal data

### HOW LONG
Retention

### CONSEQUENCES
Contract or law

### FROM WHERE
*S*ource – publicly accessible

The same level of information applies under the Law Enforcement Directive

# Right of Access

The right of access includes three different components:

- Confirmation as to whether data about the person is processed or not
- Access to this personal data and
- Access to information about the processing

*EDPB Guidelines 01/2022 on data subject rights - Right of access*
*Version 1.0, Adopted on 18 January 2022*

*The same requirements apply under the Law Enforcement Directive*

# Right of Rectification (art. 16)

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her

Notification to recipients of data. If this not possible inform data subject upon his request (Art. 19)

*The same requirements apply under the Law Enforcement Directive*

# Right of Erasure ("to be forgotten")

When shall personal data be deleted:

(a) the personal data are no longer necessary;
(b) the data subject withdraws consent and where there is no other legal ground for the processing;
(c) the data subject objects to the processing;
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with the law;
(f) the personal data have been collected in relation to the offer of information society services

# Right of Erasure ("to be forgotten")

Notification to recipients (Art. 19)

Where the controller has made the personal data public and is obliged to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data

*Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1), Version 2.0, Adopted on 7 July 2020*

*The same requirements apply under the Law Enforcement Directive*

# Right of Erasure ("to be forgotten")

Exceptions

(a) for exercising the right of freedom of expression and information;
(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing or
(e) for the establishment, exercise or defence of legal claims

# Right to restriction of Processing

**T**he data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject

If restricted, processing only (a) with consent or (b) for legal claims or (c) for protection of the rights of another person or (d) for public interest

Information to the data subject before the restriction of processing is lifted

Notification to recipients (Art. 19)

# Right to restriction of Processing

Under the Law Enforcement Directive, the controller shall restrict processing where:
(a) the accuracy of the personal data is contested by the data subject, and their accuracy or inaccuracy cannot be ascertained or
(b) The personal data must be maintained for the purposes of evidence

Where processing is restricted pursuant to point (a) above, the controller shall inform the data subject before lifting the restriction of processing

# Right to Data Portability (art. 20)

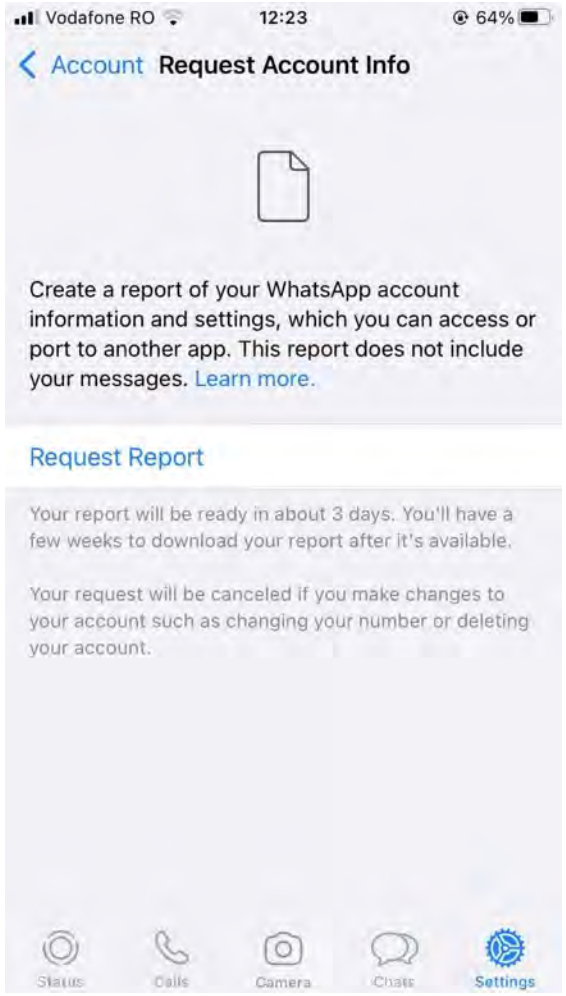
Receive personal data, which he or she has provided to a Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller, where processing is based on:
(a) consent or contract and
(b) the processing is carried out by automated means

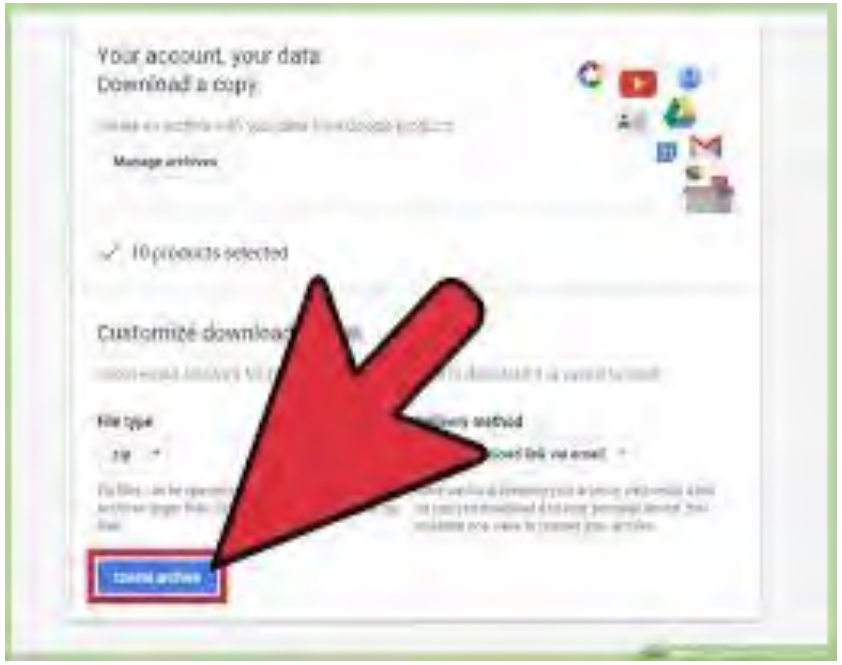
Right to have the personal data transmitted directly from one controller to another, where technically feasible

That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. - The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others

*Guidelines on the right to data portability , Adopted on 13 December 2016 , As last Revised and adopted on 5 April 2017*

# Right to Data Portability (art. 20)



# Right to Object (art. 21)

Objection to processing
(a) In the public interest or in the exercise of official authority (art. 6(1)(e))
(b) For legitimate interest (art. 6(1)(f))
*including profiling*

The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims

Direct marketing purposes: right to object at any time

Scientific or historical research purposes or statistical purposes: right to object, unless the processing is necessary for the performance of a task carried out for reasons of public interest

# Automated individual decision-making and profiling (art. 22)

Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her

Exceptions:

(a) conclusion or performance of a contract, (b) is authorised by law (safeguards);

(c) consent

Safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision

Special categories of personal data: No – except consent (art. 9(2)(a)) or public interest (art. 9(2)(g)) (safeguards)

*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017 - As last Revised and Adopted on 6 February 2018*

# Right to Withdraw Consent (art. 7 par. 3)

The data subject shall have the right to withdraw his or her consent at any time

The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal

Prior to giving consent, the data subject shall be informed thereof

It shall be as easy to withdraw as to give consent

# Restrictions (art. 23)

By way of a legislative measure such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
(f) the protection of judicial independence and judicial proceedings;
(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
(i) the protection of the data subject or the rights and freedoms of others;
(j) the enforcement of civil law claims

# Restrictions (art. 23)

The legislative measure shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;
(b) the categories of personal data;
(c) the scope of the restrictions introduced;
(d) the safeguards to prevent abuse or unlawful access or transfer;
(e) the specification of the controller or categories of controllers;
(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
(g) the risks to the rights and freedoms of data subjects; and
(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction

*Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 2.0, Adopted on 13 October 2021*

# Fines (art. 83 par. 5)

Infringements of the data subjects' rights are subject to administrative fines up to 20.000.000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher

*Guidelines 04/2022 on the calculation of administrative fines under the GDPR Version 1.0 Adopted on 12 May 2022*

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

## Comparative view: Data Protection Law Enforcement Directive (EU) 2016/80 and GDPR

Silvia Axinescu

Paris, 19 September 2022

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

# Comparative view Data Protection Law Enforcement Directive (EU) 2016/680 & GDPR

Silvia Axinescu, lawyer National Associations of Romanian Bars

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- Data Protection Law Enforcement Directive (EU) 2016/680 (LED)
  - Scope of LED
  - To which bodies LED applies
  - Key concepts

# What is personal data?

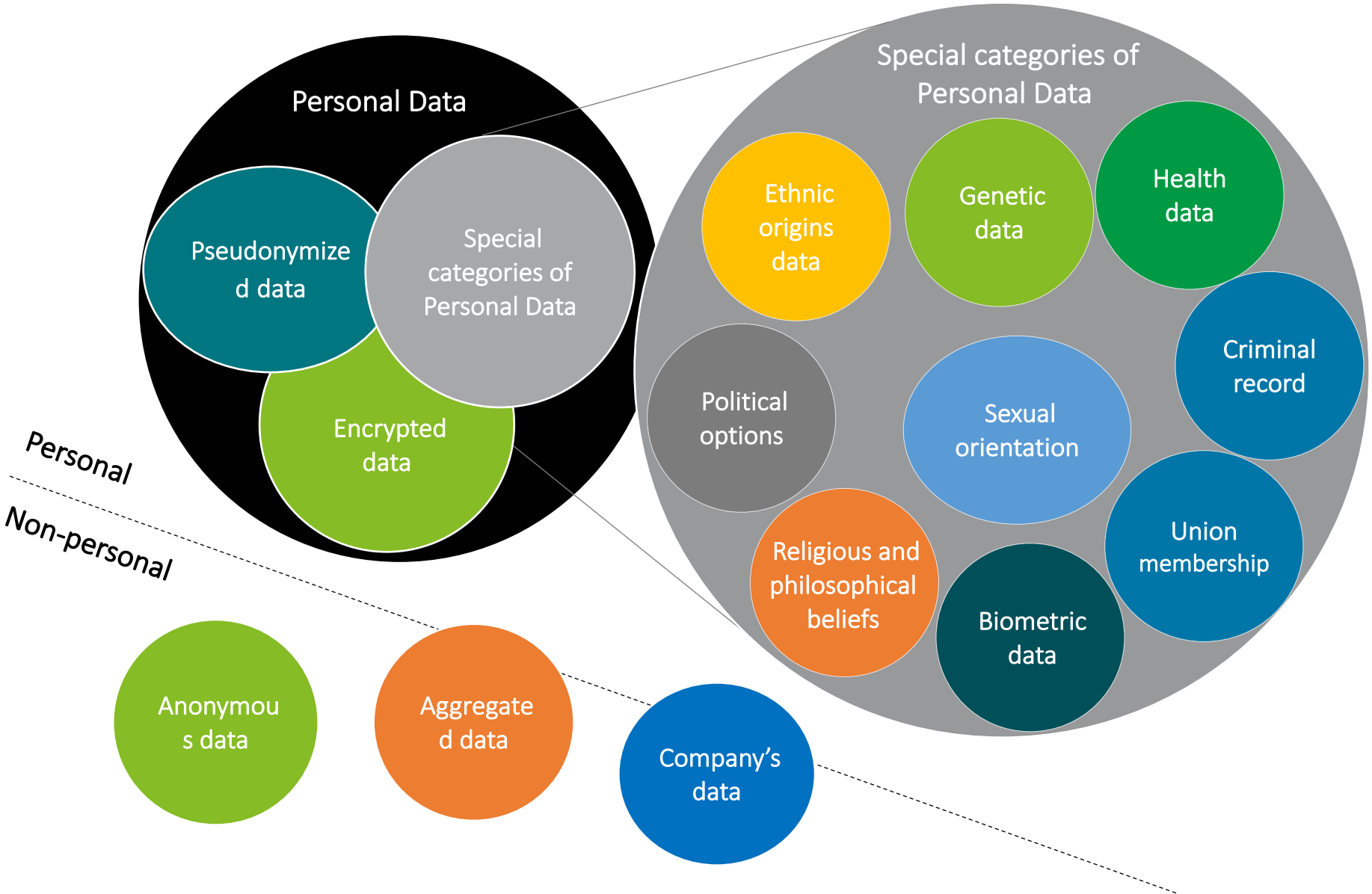
## Definition

**'personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

## Data which may be processed

- e-mail
- image
- Voice
- citizenship
- signature
- sex
- name and surname
- full name of family members
- address (home/residence)
- profession/job title
- training/diplomas/studies
- date and place of birth
- data on owned assets
- pension file no.
- telephone / fax
- nickname / alias
- geolocation data
- data from driver's license / certificate of registration
- physical / anthropometric data
- habits / preferences / behavior
- economic & financial situation
- family status
- military status
- civil status data
- bank data

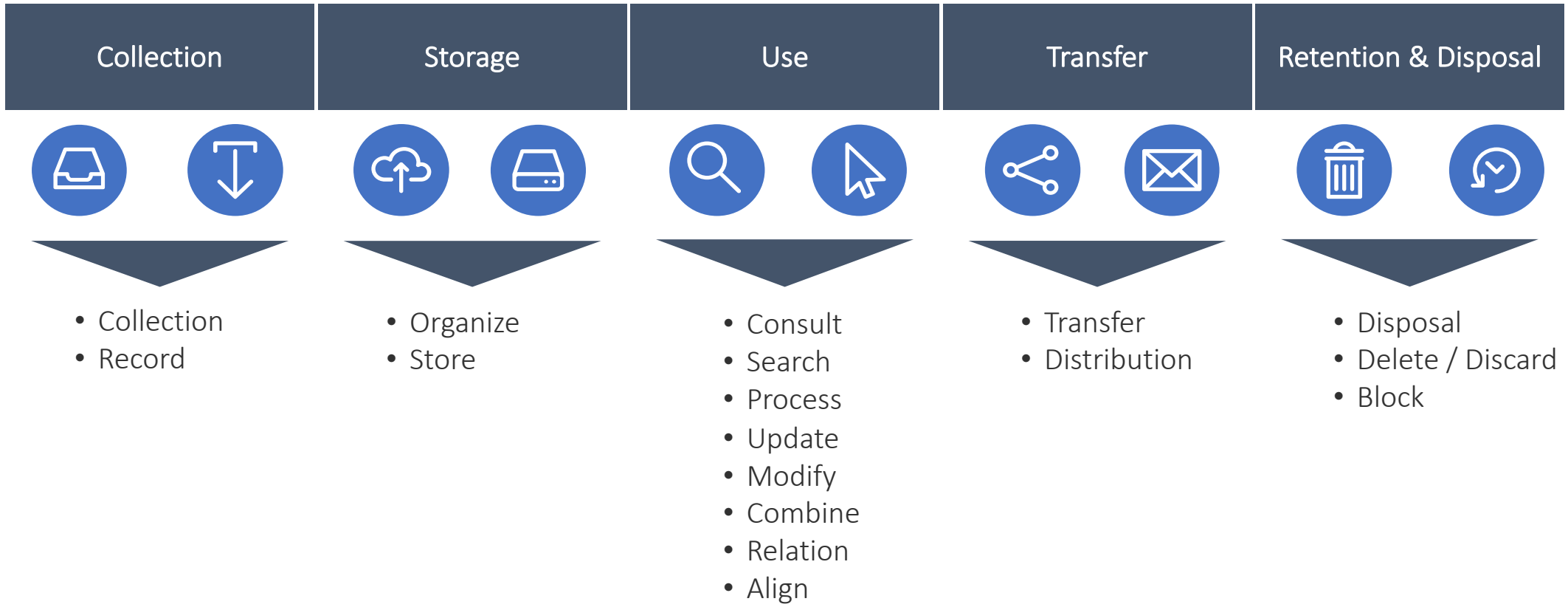
# Types of personal data



# Processing

**Processing:** any operation performed upon personal data (collecting, recording, organization, use, disclosure by transmission, alignment or combination, erasure or destruction)

## Personal Data lifecycle



# Other key concepts

01 Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

02 Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future.

03 Pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

04 Filling system means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

05 Controller means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

06 Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

# Data protection principles


- Lawfulness & fairness
- Purpose limitation
- Data minimization
- Storage limitation
- Security of data
- Accountability
- Processing personal data by the same or by another controller for a purpose other than that envisaged at the time of collection of the personal data, only certain conditions are met

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity & confidentiality
- Accountability

# Data protection rights

## Art. 12 & 13 LED

- Transparency (concise, intelligible and easily accessible form, using clear and plain language)
- Implementation of organizational, technical and procedural measures for the purpose of making available to the persons concerned the following categories of information
- When to communicate the mandatory minimum information: local law - upon request, unless otherwise provided by law
- Possibility to adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject
- Right of access – upon request and free of charge – limitations to the right of access

## Art. 12, 13 & 14 GDPR

- Transparency (concise, transparent, intelligible and easily accessible form, using clear and plain language)
- When to communicate the mandatory minimum information: at the time when personal data are obtained
- Right of access – generally, no exceptions from the right of access

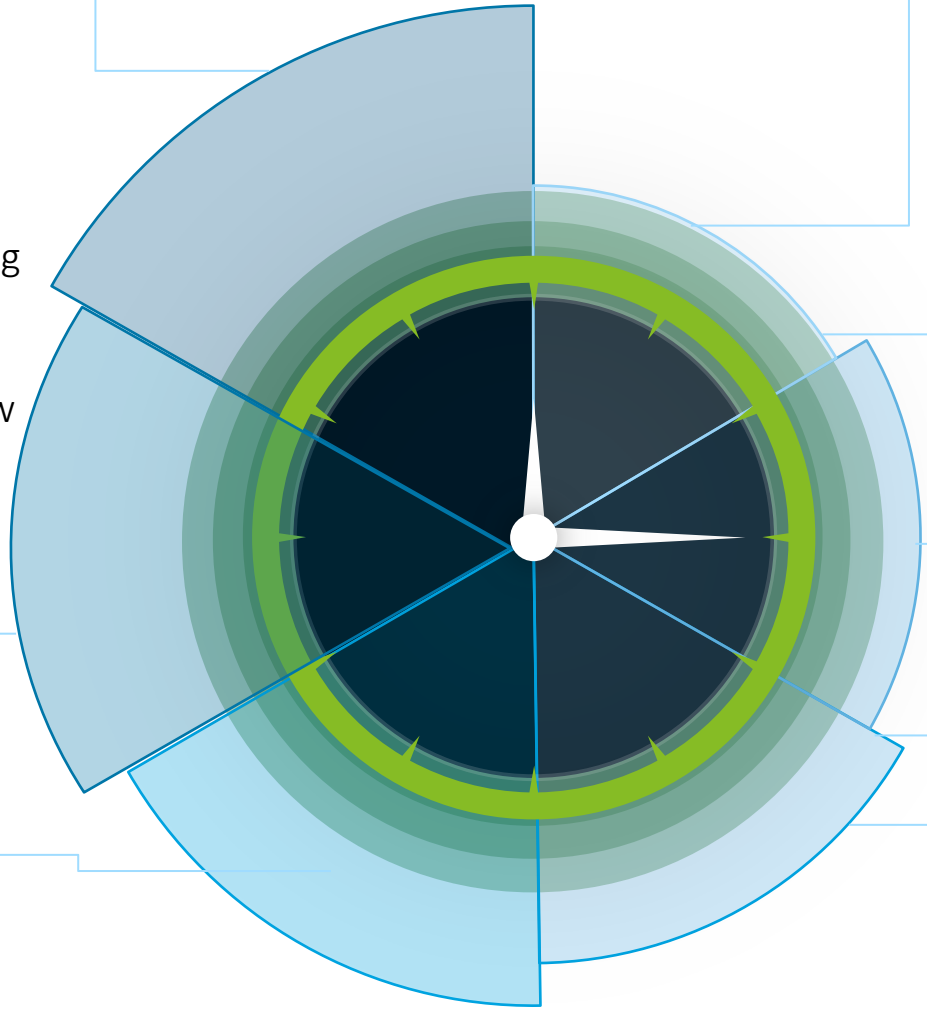
# Mirror provisions with the GDPR

Engagement of processors

- sufficient guarantees to implement appropriate technical and organizational measures
- prior specific or general written authorization by the controller.
- contract or other legal act binding on the processor with regard to the controller with mandatory minimum requirements (local law – written consent of the controller)

Records of processing

Appointment of a DPO



Logging

DPIA

Prior consultation with the DPA

Security of processing

Data breach notification

# Key take aways from the first report of the European Commission issued on LED

Positive impact on data subjects

Increased awareness of data protection within competent authorities

Improved data security but divergences in data breach notifications

Flexible instruments for international data transfers

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

## Principles on the processing of personal data

Valérie Hayek

Paris, 19 September 2022

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

CNIL.

PARTICULIER | PROFESSIONNEL

MA CONFORMITÉ AU RGPD | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL

# Traitement de données personnelles

Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement organisation, conservation, adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement).

Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

Un traitement de données doit avoir un **objectif**, une finalité déterminée préalablement au recueil des données et à leur exploitation.

*Exemples de traitements : tenue du registre des sous-traitants, gestion des paies, gestion des ressources humaines, etc.*

**Termes simplifiés à privilégier :** utilisation de données, système informatique, système d'information (selon le cas).

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

**Qu'est-ce qu'un traitement ?**

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

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Pourquoi effectuer un traitement ?

Audit de conformité*

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.

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

## Que doit inspirer un traitement ?

### Confiance

Le RGPD à 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*

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Quelles responsabilités pour un traitement ?

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

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

# 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

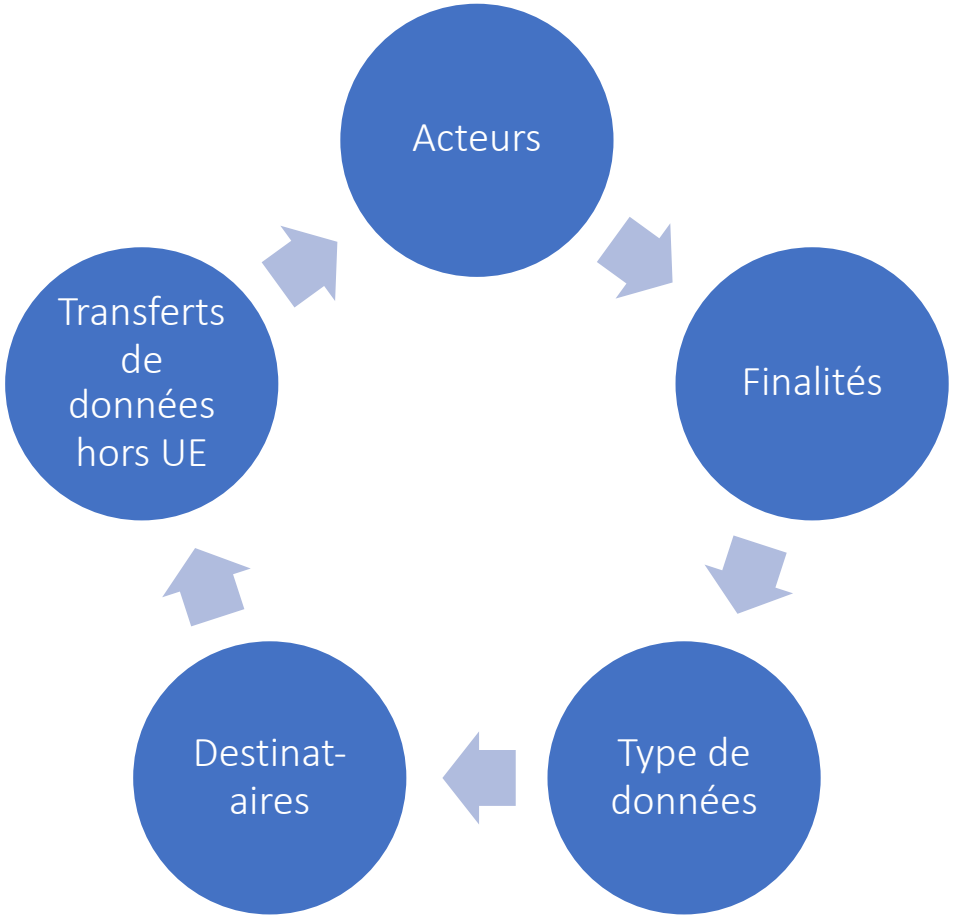
Nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou tout autre personne

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

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

# Cartographie des traitements



## Objectifs poursuivis

**Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.**

*Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.*
Cliquez ici.

## Catégories de personnes concernées

**Listez les différents types de personnes dont vous collectez ou utilisez les données.**

*Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.*

1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

## Catégories de données collectées

**Cochez et listez les différentes données traitées**

☐ État-civil, identité, données d'identification, images *(ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.)*
Cliquez ici.

☐ Vie personnelle *(ex. habitudes de vie, situation familiale, etc.)*
Cliquez ici.

☐ Vie professionnelle *(ex. CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)*
Cliquez ici.

☐ Informations d'ordre économique et financier *(ex. revenus, situation financière, données bancaires, etc.)*
Cliquez ici.

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Registre des traitements

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

**Des données sensibles sont-elles traitées ?**

*La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).*

☐ Oui ☐ Non

Si oui, lesquelles ? :
Cliquez ici.

## Durées de conservation des catégories de données

**Combien de temps conservez-vous ces informations ?**

Cliquez ici. Jours, Cliquez ici. Mois, Cliquez ici. Ans, Autre durée : Cliquez ici.

*Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement (par exemple, 3 ans à compter de la fin de la relation contractuelle).*
Cliquez ici.

**Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.**

## Catégories de destinataires des données

**Destinataires internes**

*(Exemples : entité ou service, catégories de personnes habilitées, direction informatique, etc.)*

1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

**Organismes externes**

*(Exemples : filiales, partenaires, etc.)*

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Registre des traitements

## Transferts des données hors UE

**Des données personnelles sont-elles transmises hors de l'Union européenne ?**

☐ Oui ☐ Non

Si oui, vers quel(s) pays :
Cliquez ici.

*Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD). Consultez le site de la CNIL.*

## Mesures de sécurité

**Cochez et décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.**

*Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.*

☐ Contrôle d'accès des utilisateurs

Décrivez les mesures :

Cliquez ici.

☐ Mesures de traçabilité

Précisez la nature des traces *(exemple : journalisation des accès des utilisateurs)*, les données enregistrées *(exemple : identifiant, date et heure de connexion, etc.)* et leur durée de conservation :

Cliquez ici.

☐ Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures :

Cliquez ici.

☐ Sauvegarde des données

Décrivez les modalités :

Cliquez ici.

☐ Chiffrement des données

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Registre des traitements

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

## Focus : Traitement des données à caractère personnel des salariés

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

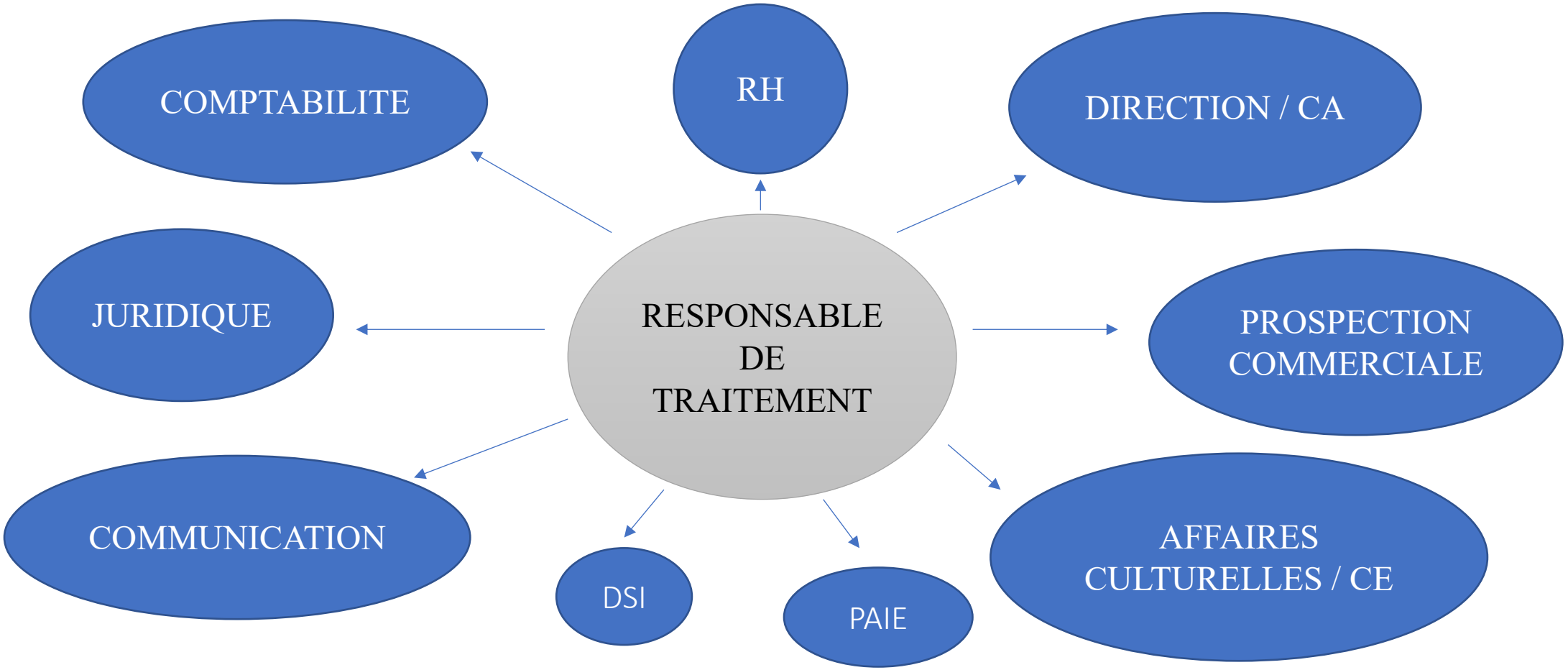
Préciser aux salariés leurs droits d'accès, de modification, d'opposition et d'effacement*.
Indiquer que ces droits peuvent s'exercer à tout moment

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

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

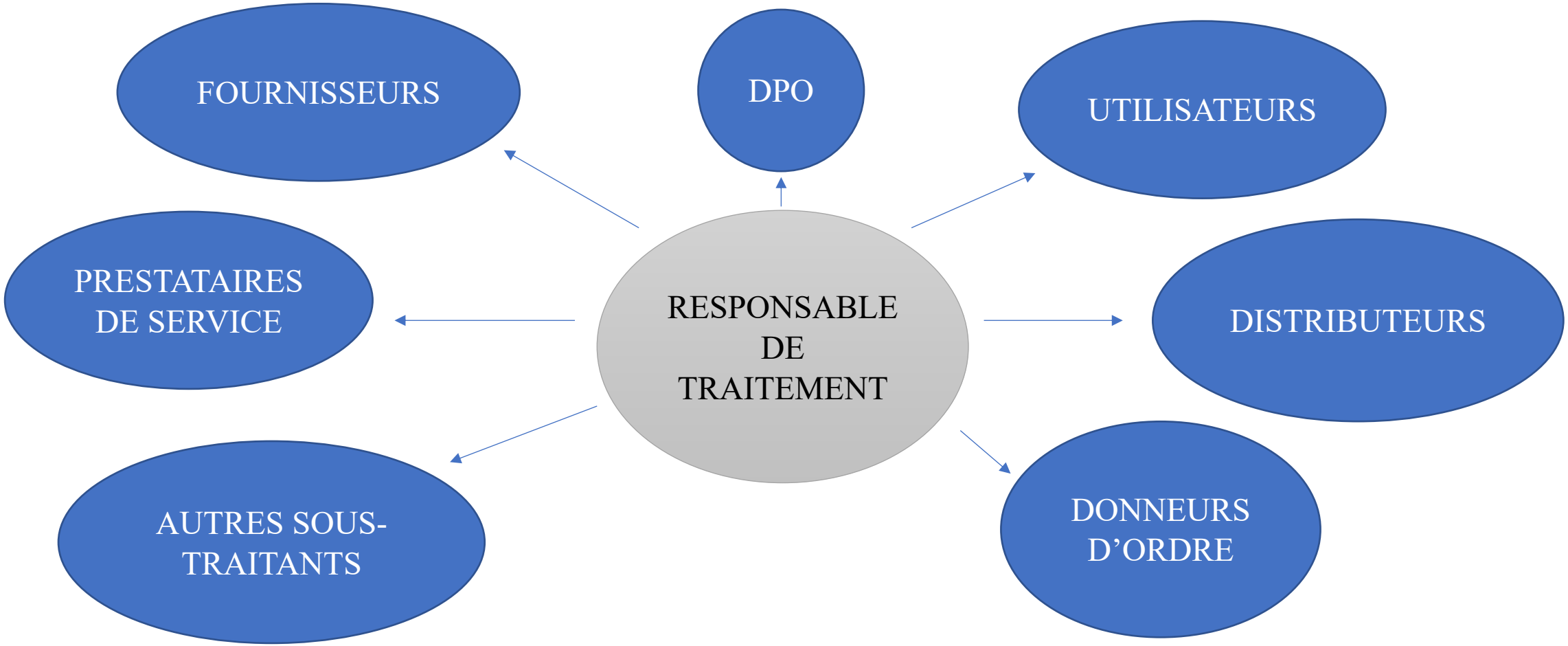
Traitements au sein de l'entreprise



Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Traitements effectués par les sous-traitants



Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

# Comment créer de l'implication face à un traitement ?

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

Coopérer avec le DPO et la DSI 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 !