

GDPR : Par où commencer ?

@Bernard_Lamon

Sommaire

- ◆ Qui sommes-nous ?
- ◆ Objectifs et moyens de la réforme, quand ?
- ◆ S'applique à quoi ?
- ◆ Qui ? RT et ST, le DPO.
- ◆ Todo list : étude d'impact, bonnes pratiques, sécurité à garantir et à notifier, privacy by design.
- ◆ Droits des personnes,
- ◆ Hors UE ?
- ◆ Labels et bonne conduite,
- ◆ Sanctions.

Qui sommes-nous ?

- ◆ Mission : protéger, valoriser et défendre vos actifs immatériels,
- ◆ Les avocats du Nouveau Monde : immatériel,
- ◆ Cabinet de niche, 5 personnes, Paris/Rennes,
- ◆ Clients : éditeurs, op internet, telcos, sociétés innovantes.
- ◆ Ex3 : experts, expérimentés, exclusifs. Nous ne faisons que cela,
- ◆ Modèle tarifaire : 1^{er} rendez-vous gratuit.

Objectifs et moyens

Harmoniser

Responsabiliser

Big Data

Protéger la vie
privée

Transfert des
données

Prise en compte de
l'évolution
technologique
(profilage)

Quand ?

**25 mai 2018 : entrée en vigueur
du GDPR.**

Are you ready ? PAC study.

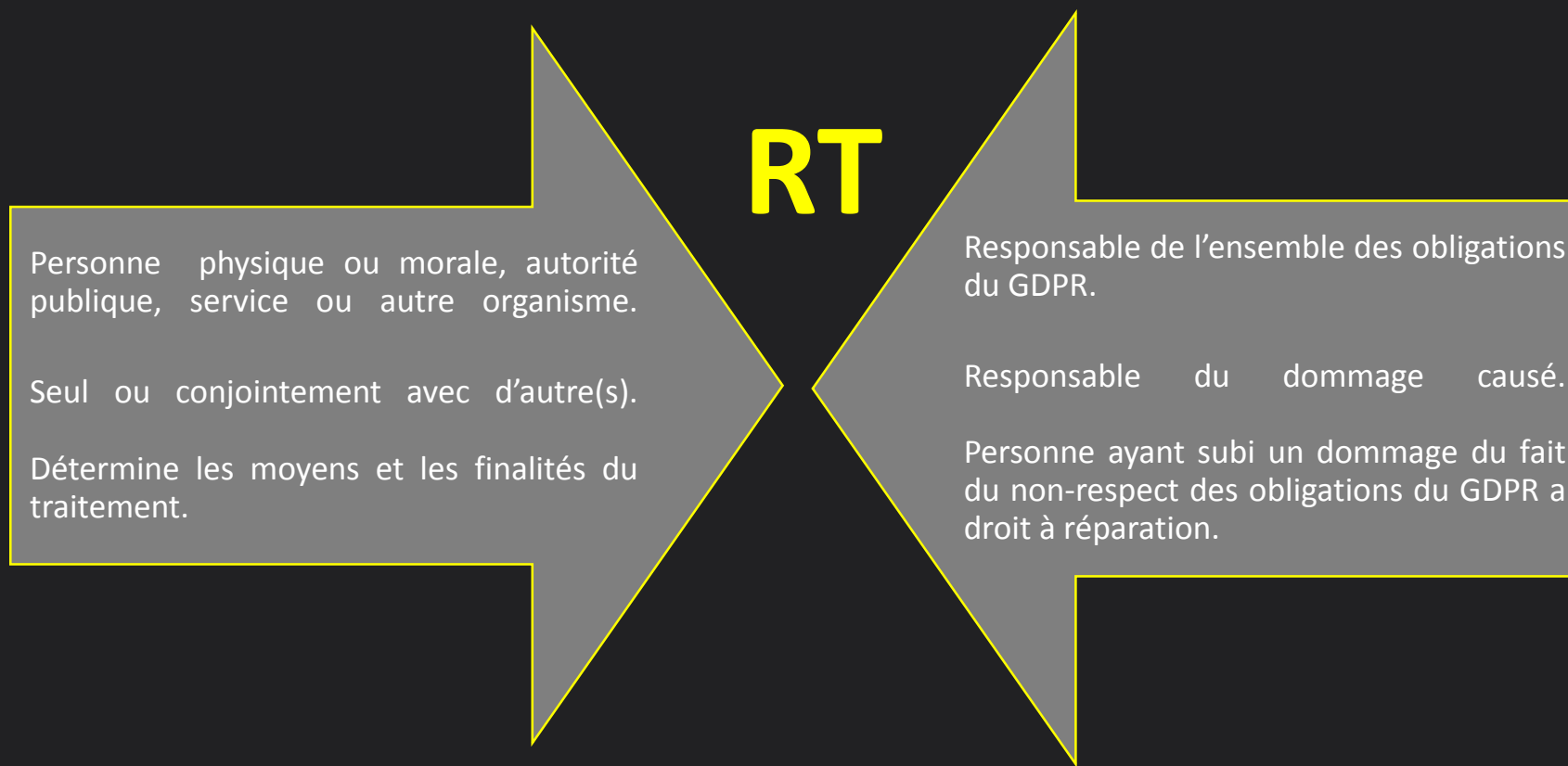
⇒ Application immédiate / pas de loi de transposition.

⇒ Traite 80% des sujets. 20% laissés aux Etats membres.

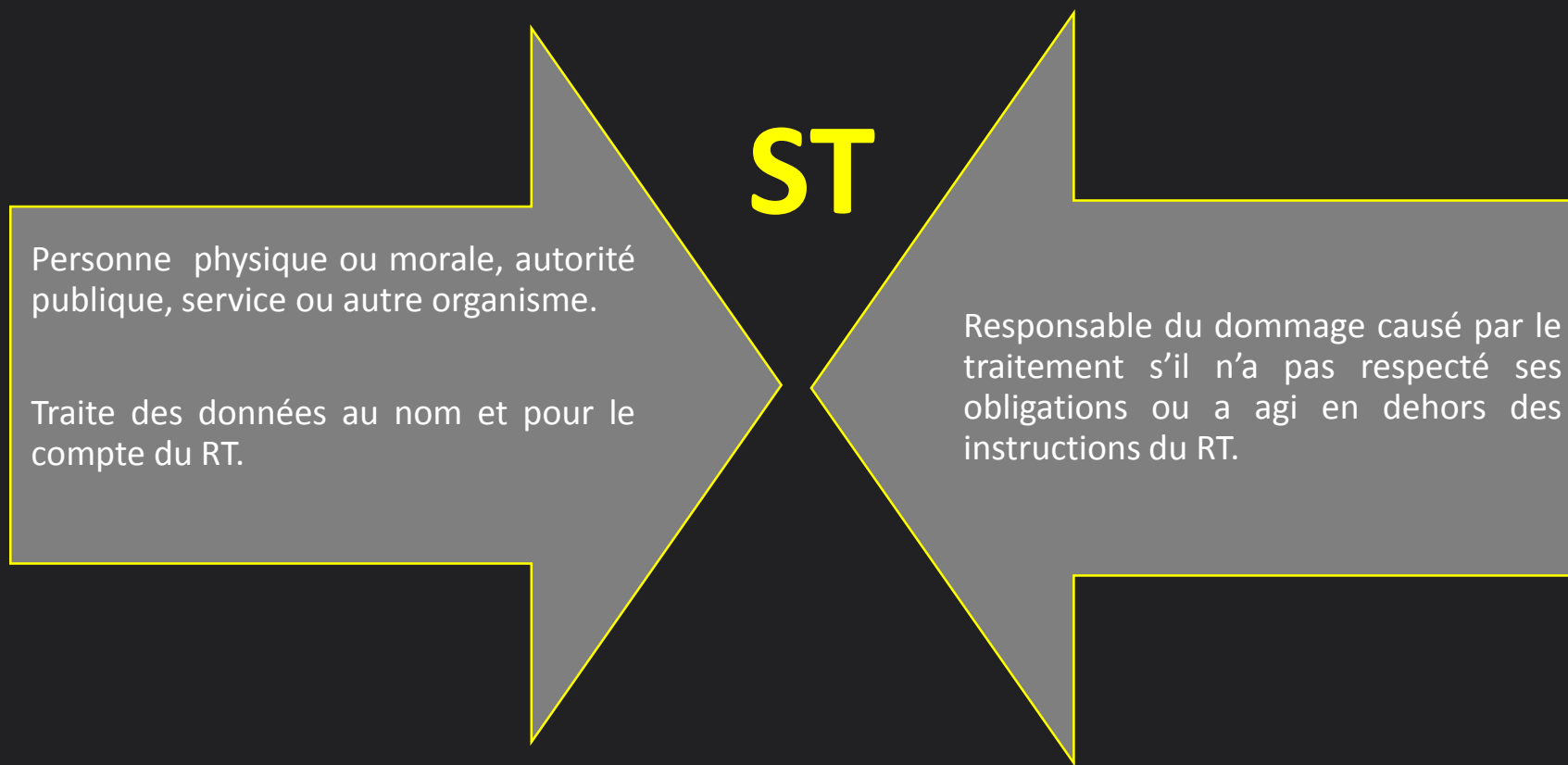
Quoi

Matériel	Territorial
Traitement de données personnelles.	Etablissement du responsable de traitement (RT) ou du sous-traitant (ST) au sein de l'UE.
Personne physique.	
Exclusion des activités personnelles.	Peu importe que traitement ait lieu ou non dans l'UE.
	<u>RT ou ST non établi dans l'UE (vente de profilage).</u>

Les acteurs



Les acteurs



Le ST

- ◇ Inversion du principe précédent : plus de Ponce Pilate,
- ⇒ Obligation d'assurer la confidentialité et la sécurité des données,
- ⇒ Tenue d'un registre,
- ⇒ Pas de sous-sous-traitance sans autorisation et transfert des mêmes contraintes,
- ⇒ Organisation technique (pseudonymisation, chiffrement des données, résilience, PAQ).

Clauses **du contrat** exigées par le RGDP :

- Instructions documentées du RT ;
- Devoir d'information du STT à l'égard du RT ;
- Devoir de confidentialité ;
- Obligations :
 - de justifier de l'orga,
 - De la sécu,
 - suppression et destruction des données.

Le CIL-DPO

Désignation obligatoire	Modalités	Statut	Missions
➤ Autorité ou entité publique ; ➤ Activités principales qui impliquent des traitements induisant un <i>contrôle régulier et systématique des personnes à grande échelle</i> ; ➤ traitements à grande échelle des catégories particulières de données (données sensibles...) et des données relatives à des condamnations et infractions.	➤ Salarié ou consultant ; ➤ DPO mutualisé ; ➤ Obligation de communiquer à la Cnil et aux personnes fichées les coordonnées du DPO.	➤ Compétences techniques, juridiques et organisationnelles ; ➤ Indépendance ; ➤ Absence de conflits d'intérêts ; ➤ Confidentialité / secret professionnel.	➤ Informer et conseiller ; ➤ Contrôler le respect de la réglementation (audit) ; ➤ Superviser les PIA (études d'impact) ; ➤ Former / sensibiliser ; ➤ Point de contact avec la Cnil.

Accountability.

- Principe de responsabilité.
- Traçabilité : registre de traitement.
- PAQ : PIA (privacy impact assessment) + formation + Code de bonne conduite + Audit + Certification, etc.
- Obligation de documentation.

Etude d'impact (PIA)

Cas d'ouverture

- Profilage / segmentation ;
- Traitement à grande échelle de catégories particulières de données sensibles;
- Surveillance systématique à grande échelle d'une zone accessible au public.
- Listes établies par les Cnil nationales.

Contenu

- Description opérations, finalités, intérêts légitimes du RT ;
- Évaluation de la nécessité et de la proportionnalité ;
- Évaluation des risques ;
- Mesures adoptées.

Privacy by design/default

Privacy by design	Privacy by default
➤ Conception des services tenant compte du respect de la vie privée. ➤ Respect du principe de minimisation des données et de limitation des finalités. ➤ Haut standard de sécurité depuis la conception. ➤ Documentation des mesures techniques et opérationnelles.	➤ Mise en œuvre des mesures techniques et organisationnelles pour garantir que par défaut, seules les données personnelles nécessaires à la finalité du traitement sont traitées (ex. quantité, accès limité aux seules personnes y ayant intérêt, etc.). ➤ Documentation des mesures techniques et opérationnelles.

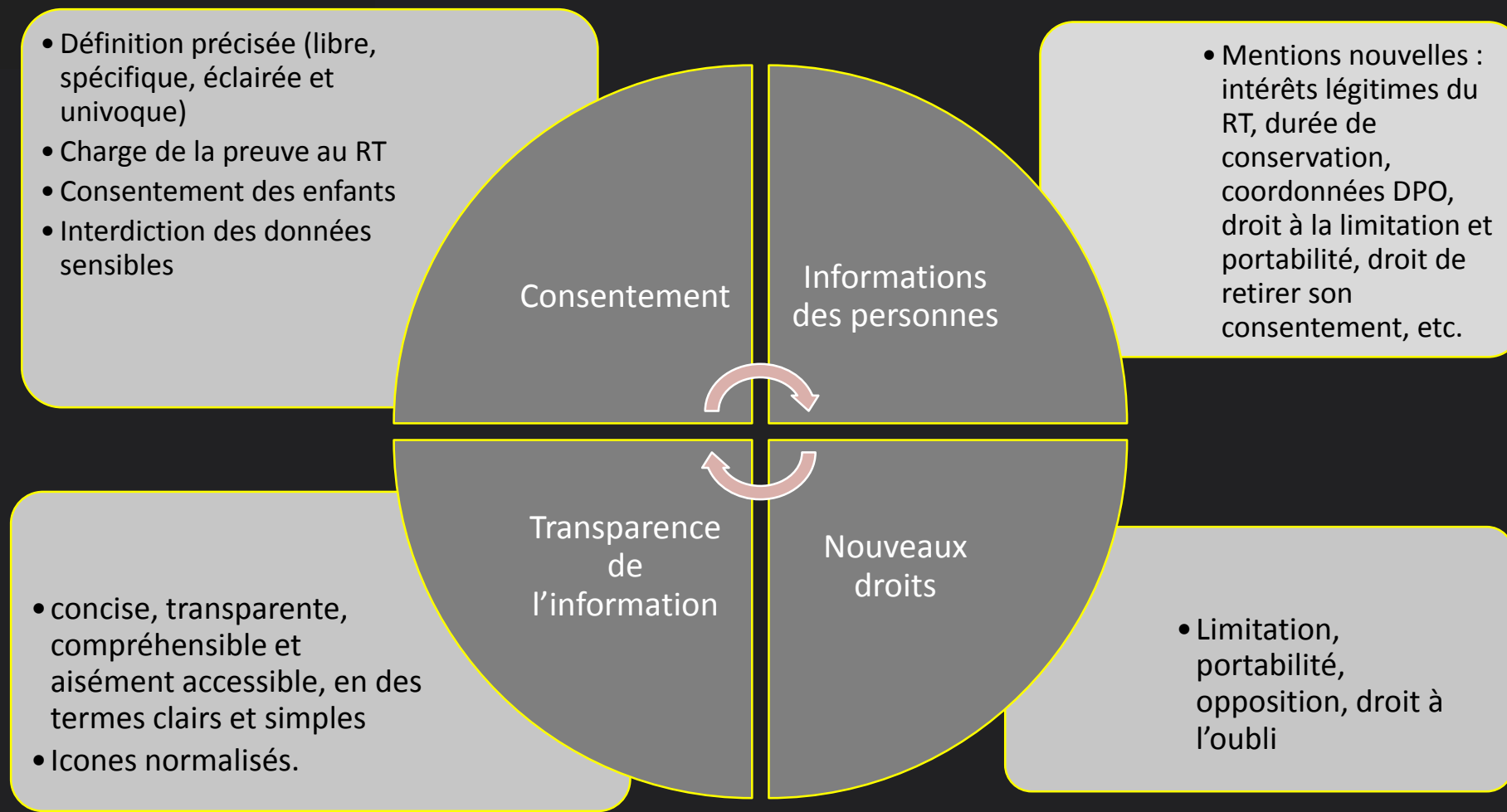
Notification des failles de sécurité.

Responsable de traitement	Sous-traitant
➤ Obligation de notification étendue à l'ensemble des RT ; ➤ Contenu notification (catégories de données concernées, conséquences, mesures prises) ; ➤ Obligation d'alerter les individus si haut risque pour les droits et les libertés de l'individu (sauf mesures de protection appropriées prises).	➤ Obligation d'alerter et d'informer le RT de l'existence d'une violation de sécurité.

Sécurité

Pseudonymisation	Anonymisation
➤ Les données ne peuvent plus être attribuées à un individu sans avoir recours à des informations supplémentaires conservées de manière séparée afin de garantir qu'il ne soit plus identifié ou identifiable. ⇒ RÉVERSIBLE	➤ Technique consistant à supprimer tout caractère identifiant à un ensemble de données. ⇒ IRRÉVERSIBLE

Droits des personnes



Droits des personnes

Droit à l'oubli

- Droit à l'effacement de ses données dans les meilleurs délais ;
- Conditions : données plus nécessaires, retrait du consentement, opposition au traitement ;
- Exceptions : liberté d'expression et d'information, obligation légale, etc.

Droit à la limitation du traitement

- Contestation exactitude des données
- Traitement illicite et la personne préfère une limitation à un effacement
- Exception à la limitation (consentement, protection des droits d'une autre personne physique ou morale...)

Droit à la portabilité

- Extension du droit d'accès (données fournies à un RT)
- Interopérabilité (format structuré, couramment utilisé et lisible par machine)
- Transfert (à un autre RT)
- Restrictions (traitement de données automatisés,...)

Transfert des données hors UE

Interdiction des transferts de données en dehors UE sauf niveau adéquat de protection des données personnelles.

A défaut, il faut des garanties adéquates.

Accords internationaux (*Safe Harbor / Privacy Shield*)

Règles d'entreprise contraignante / Binding corporate rules (BCR)

Clauses contractuelles type adoptées par la Commission Européenne

Code de conduite ou certification

Dérogation limitées (consentement, exécution d'un contrat, etc.)

Labels et bonne conduite

Certification / labels

- Accordés par des organismes accrédités par les Autorités pour 3 ans, au plus, renouvelables
- Création de labels européens (« European Data Protection Seal »)
- Registre public tenu par le CEPD (Comité Européen de Protection des Données)

Code de bonne conduite

- Elaborés par des associations ou entités représentatives des RT/SST
- Approuvés par les Autorités
- Adhésion facultative, mais valeur contraignante
- Contrôle du respect des codes par un organisme accrédité par l'Autorité

GDPR

- Pouvoirs des autorités de contrôle :
 - Enquête, pièce, place, en ligne, sous forme d'audit,
 - Procéder à un examen des certifications,
- Agir en justice,
- Mécanisme de coopération et d'autorité en Europe,
- Pouvoirs de sanctions
- Renforcement des sanctions administratives : jusqu'à 20 m€ ou 4 % du CA annuel global ou simple avertissement.
- Sanction pénale applicable selon la législation nationale (France : 3 ans + 300 K).

Boîte à outils

- ◆ Désigner 1 pilote (internet/DPO),
- ◆ Cartographier,
- ◆ Prioriser les actions,
- ◆ Gérer les risques : PIA,
- ◆ Organiser les processus internes,
- ◆ Documenter la conformité.
- ◆ Cf [guide de la CNIL](#).

Ressources

- ◇ <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methode.pdf>
- ◇ [Guidelines sur le DPO du G29](#)
- ◇ [Guidelines sur le droit à la portabilité des données](#)
- ◇ [Avis du G29 sur les techniques d'anonymisation](#)
- ◇ [https://www.cnil.fr/sites/default/files/typo/document/Guide pratique Prise de fonction CIL.pdf](https://www.cnil.fr/sites/default/files/typo/document/Guide_pratique_Prise_de_fonction_CIL.pdf) ;
- ◇ <https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee#Article40-1>
- ◇ <https://www.cnil.fr/reglement-europeen-protection-donnees>

See you soon



Nouveau Monde Avocats

11 quai Chateaubriand 35000 Rennes

222 boulevard Saint-Germain 75007 Paris

0299230033

<https://www.nouveaumonde-avocats.com/>