Présentation RGPD

Maître Oriana Labruyère

29 mai 2018

Association Française des Tierces Parties Marketing

Champ d'application

Un champ d'application large

Le règlement s'applique *« au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier […]».*

Le principe d'extraterritorialité

Sa vocation est d'apporter une protection :

- aux personnes résidentes d'un pays de l'UE dont les données personnelles font l'objet d'une collecte et d'un traitement quelle que soit la localisation (UE ou hors UE) ;
- aux résidents non UE pouvant aussi bénéficier d'une protection sur la collecte et traitements réalisés au sein de l'UE.

Les exceptions

Les institutions, organes et agences de l'Union Européenne.

Les personnes physiques dans le cadre d'une activité personnelle ou domestique.

Les autorités publiques à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, d'exécution de sanctions pénales ou de protection contre des menaces pour la sécurité publique et de prévention de telles menaces.

Les Etats membres dans le cadre de la politique étrangère et de la sécurité commune.

Principes clés

Principe 1
Collecte loyale et transparente (dont renforcement du consentement).

Principe 2
"Finalité" du traitement des données (légitime, explicite et spécifique).

Principe 3
Proportionnalité des données (adéquates, pertinentes et non excessive). La quantité de DCP détenues est adaptée aux finalités pour lesquelles elle est traitée.

Principe 4
Responsabilité des tiers.

Principe 5
Conservation des données personnelles limitée dans le temps.

Principe 6
Gestion des droits des individus (accès, portabilité, modification, oubli).

Principe 7
Mise en place de mesures de sécurisation organisationnelles et techniques des données.

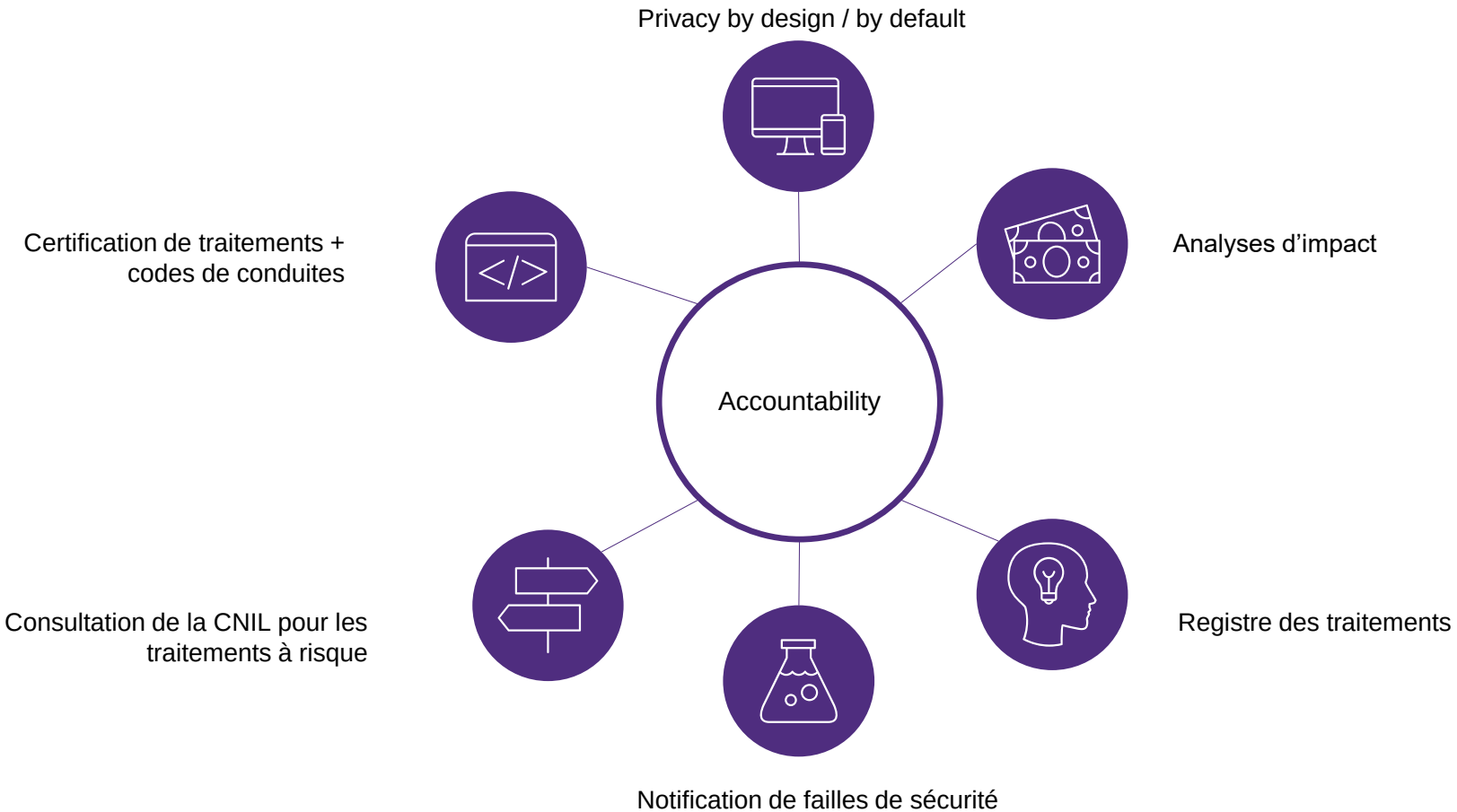
Principe 8
Gestion des flux internes et externes au sein ou hors Union Européenne.

Principe d'accountability

Le responsable du traitement est considéré comme acteur économique responsable. C'est à lui de prendre les mesures techniques et organisationnelles visant à garantir le respect de la règlementation.

Il n'a plus à déclarer son traitement, ni à solliciter une autorisation préalable. En revanche, il se doit de tout documenter afin d'être en mesure de démontrer la conformité de l'entreprise en cas de demande du régulateur.

Quels outils ?



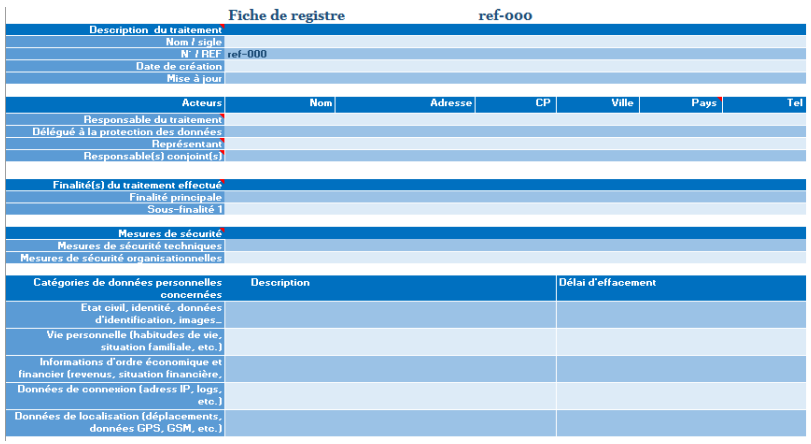
Registre des traitements

- Les entreprises et organisations soumises au RGPD comptant plus de **250 employés** doivent tenir à jour un registre des activités de traitements en lien avec les données à caractère personnel.

- Ce registre doit contenir, à minima :
  - ✓ la description du traitement;
  - ✓ les acteurs associés (responsable du traitement, représentant et/ou DPO, …);
  - ✓ les finalités du traitement effectué;
  - ✓ les catégories de DCP concernées;
  - ✓ les catégories de personnes concernées (collaborateurs, clients, fournisseurs, …)
  - ✓ les outils et les prestataires liés (y/c dans le cas d'hébergements des données);
  - ✓ les destinataires des données (inter et hors UE) en cas de flux de données.

- Dans le cas d'activités de traitements réalisées pour le compte d'un tiers (sous-traitance), un registre spécifique aux activités de traitements réalisées pour le compte d'un client doit être mis en place. Ce registre doit contenir, à minima :
  - ✓ l'identité et les coordonnées du sous-traitant et de son représentant et du DPO;
  - ✓ les catégories de traitements;
  - ✓ les transferts de données hors UE et références aux garanties associées;
  - ✓ la description générale des mesures de sécurité techniques et organisationnelles mises en œuvre.

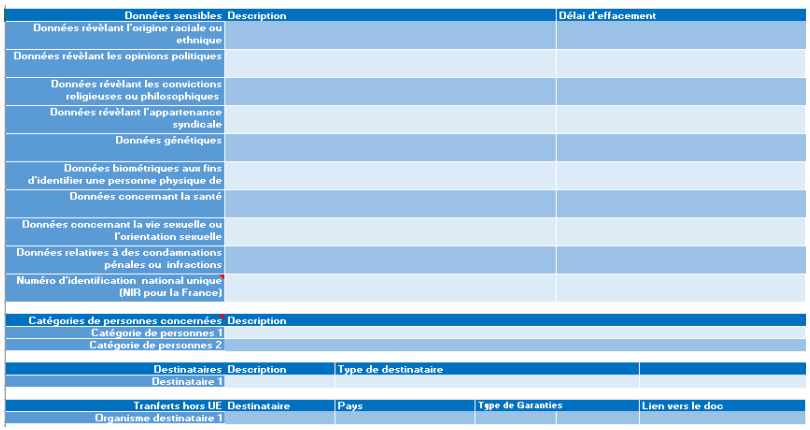
- Exemple de registre de traitements publié par la CNIL en avril 2017



Fiche de registre ref-000

Description du traitement						
Nom / sigle						
N° REF	ref-000					
Date de création						
Mise à jour						
Acteurs	Nom	Adresse	CP	Ville	Pays	Tel
Responsable du traitement						
Délégué à la protection des données						
Représentant						
Responsable(s) conjoint(s)						
Finalité(s) du traitement effectué						
Finalité principale						
Sous-finalité 1						
Mesures de sécurité						
Mesures de sécurité techniques						
Mesures de sécurité organisationnelles						

Catégories de données personnelles concernées	Description	Délai d'effacement
Etat civil, identité, données d'identification, images…		
Vie personnelle (habitudes de vie, situation familiale, etc.)		
Informations d'ordre économique et financier (revenus, situation financière,		
Données de connexion (adress IP, logs, etc.)		
Données de localisation (déplacements, données GPS, GSM, etc.)		



Données sensibles	Description	Délai d'effacement
Données révélant l'origine raciale ou ethnique		
Données révélant les opinions politiques		
Données révélant les convictions religieuses ou philosophiques		
Données révélant l'appartenance syndicale		
Données génétiques		
Données biométriques aux fins d'identifier une personne physique de		
Données concernant la santé		
Données concernant la vie sexuelle ou l'orientation sexuelle		
Données relatives à des condamnations pénales ou infractions		
Numéro d'identification national unique (NIR pour la France)		

Catégories de personnes concernées	Description
Catégorie de personnes 1	
Catégorie de personnes 2	

Destinataires	Description	Type de destinataire	
Destinataire 1			

Tranferts hors UE	Destinataire	Pays	Type de Garanties	Lien vers le doc
Organisme destinataire 1				

DPO or not DPO ?

- Le Délégué à la Protection des Données (DPD ou Data Protection Officer en anglais) est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisation qui l'a désigné, s'agissant de l'ensemble des traitements mis en œuvre par cette organisation et ses sous-traitants.

- La désignation d'un DPO n'est obligatoire que pour certaines organisations et sous certaines conditions :

    1. Les autorités ou les organismes public (ou si l'organisation effectue une mission de service public) ;

    2. Les organisations dont les activités de base les amènent à réaliser un **suivi régulier et systématique des personnes à grande échelle** ;

    3. Les organisations dont les activités de base les amènent à traiter à grande échelle des données dites "sensibles" ou relatives à des condamnations pénales et infractions.

- L'organisation doit formaliser une fiche de poste ou une lettre de mission à l'attention du DPO.

- Les organisations peuvent toutefois désigner un DPO interne ou externe à leur structure. Il peut également être mutualisé entre plusieurs entités à condition de demeurer facilement joignable à partir de chaque lieu d'établissement.

Data Protection Impact Assessment (DPIA)

Les analyses d'impacts sont obligatoires pour tous les traitements susceptibles d'engendrer un "risque élevé" pour les droits et libertés des personnes physiques.

1. Le traitement est réalisé à grande échelle
2. Le traitement consiste en une évaluation systématique de la personne (profilage)
3. Le traitement consiste en une surveillance publique à large échelle

- Elles doivent contenir :
  - ✓ La description du traitement envisagé ainsi que sa finalité ;
  - ✓ L'évaluation de la nécessité de ce traitement ainsi que de la proportionnalité ;
  - ✓ L'évaluation du risque sur les droits et libertés des personnes concernées ;
  - ✓ Les mesures envisagées pour remédier aux risques.

- L'autorité de contrôle doit être consultée au préalable par le DPO si le traitement demeure à risque et si la mise en œuvre de mesures destinées à réduire ce risque est inenvisageable. L'autorité de contrôle consultée dispose d'un délai de 2 mois pour répondre à l'organisation (extensible à 3,5 mois).

Flux de données hors UE

- Le RGPD prévoit désormais une boîte à outils renouvelée et diversifiée permettant de rendre plus souple mais de sécuriser les conditions de transferts internationaux.

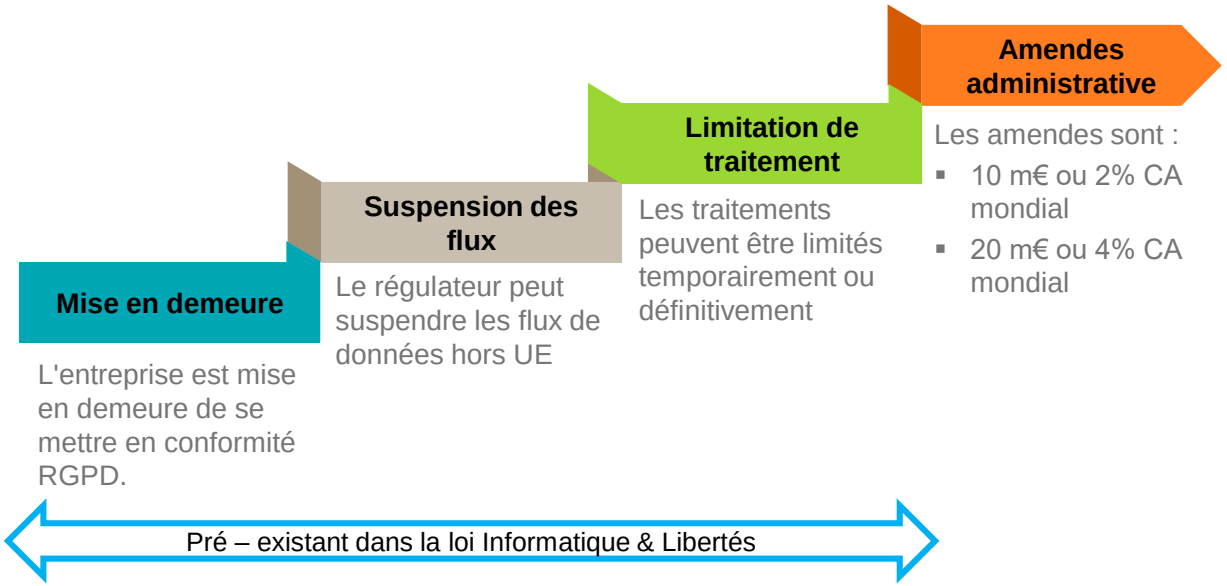
- Les principes préexistants :
  - ✓ Interdiction de transférer des données hors de l'UE ;
  - ✓ Transfert autorisé lorsque des garanties suffisantes sont apportées (niveau de protection adéquat, clauses contractuelle, …) ;
  - ✓ Des exceptions sont prévues lorsque des garanties n'encadrent pas le transfert.

- Les nouveaux outils de transferts
  - ✓ Règles d'entreprise contraignantes ou « Binding Corporate Rules (BCR) » ;
  - ✓ Codes de conduites et certifications ;
  - ✓ Instruments juridiquement contraignants et exécutoires entre les autorités ou organismes publics.

- Les flux hors UE sont donc autorisés à condition que le responsable de traitement soit en mesure de prouver la conformité de ses transferts au règlement (principe d'accountability).

Sanctions

Les sanctions prévues par le règlement sont encadrées, graduées et renforcées afin d'être dissuasives.



En cas de non-respect du RGPD par le responsable de traitement ou le sous-traitant, toute personne (physique ou morale) concernée par le traitement de données personnelles dispose de plusieurs **voies de recours**.

Recours juridictionnel contre le responsable de traitement ou le sous-traitant.

Recours juridictionnel contre une DPA (ex : CNIL)
lorsque la DPA ne traite pas sa réclamation ou ne l'informe pas, dans un délai de 3 mois, de l'état d'avancement de sa réclamation

Recours collectif / Actions de groupe.

Droit à réparation pour les usagers.

Sanctions

< 10 m€ ou 2% CA mondial	< 20 m€ ou 4% CA mondial
En fonction de la nature, gravité, durée de l'infraction, nombre de personnes concernées et niveau de dommage subi	
En fonction de la catégories de données concernées par l'infraction	
Organisation de la responsabilité conjointe	Caractère délibéré de l'infraction
Existence de mesures techniques et organisationnelles (DPO, Sécurité IT, DPIA, Privacy by design & by default, formation, …)	Absence de mesures techniques et organisationnelles
Encadrement de l'activité du sous-traitant, tenue du registre	Autres infractions déjà constatées
Application de codes de conduite approuvés ou de mécanismes de certification approuvés	Absence de codes de conduite approuvés ou de mécanismes de certification approuvés
Respect des principes de base d'un traitement (licéité, loyauté, proportionnalité, conditions applicables au consentement)	Non respect des principes de base d'un traitement (licéité, loyauté, proportionnalité, conditions applicables au consentement)
Notification de faille à la CNIL, communication de la faille à la personne lésée	Non respect des droits, encadrement des transferts, respect des dispositions nationales spécifiques
	Non respect des injonctions découlant des pouvoir des autorités de contrôle

Questions ?

Oriana Labruyère
+33 (0)6 49 43 26 75
avocat@labruyere.com