

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.



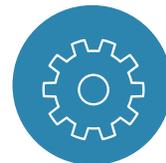
Principe 4

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

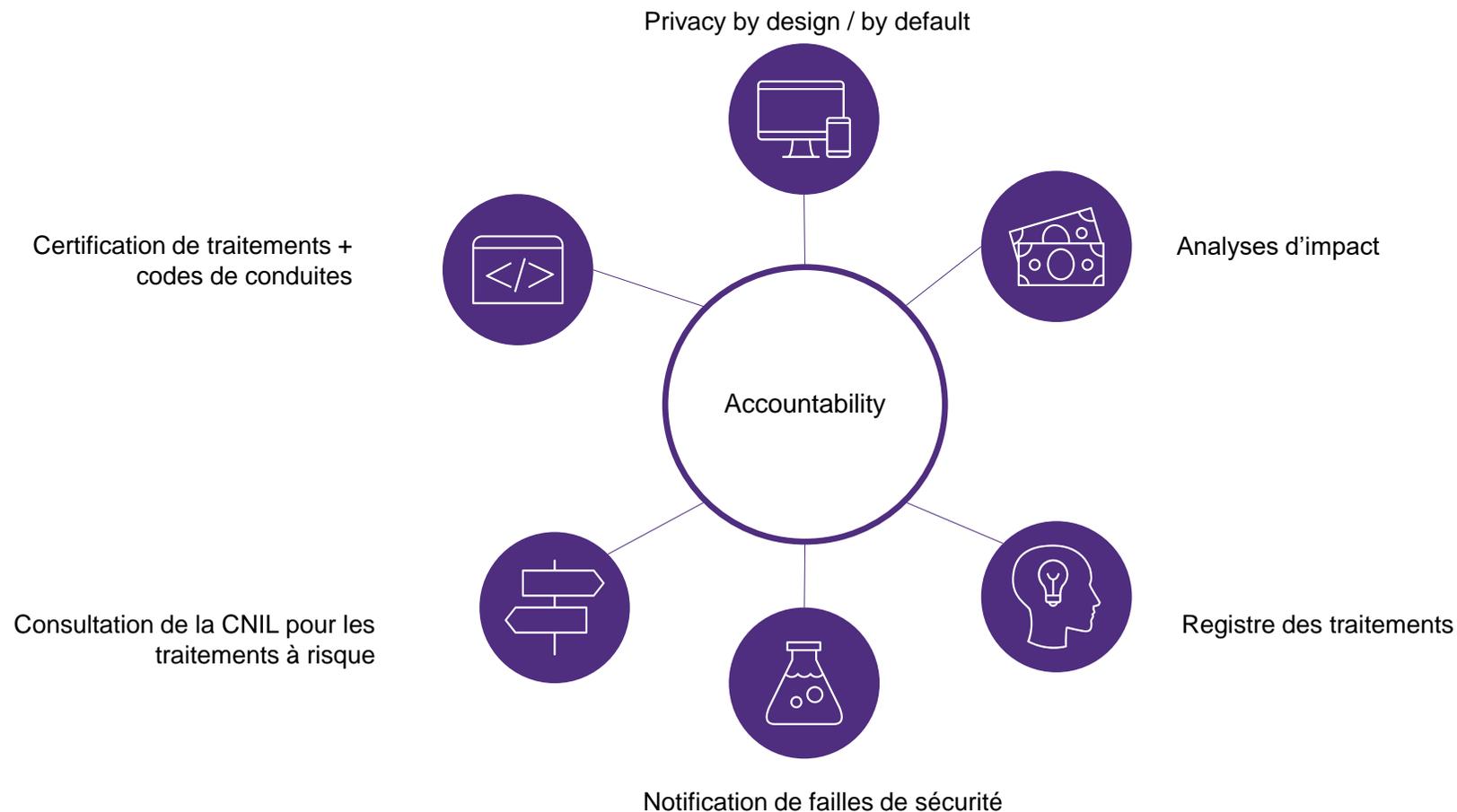
Gestion des flux internes et externes au sein ou hors Union Européenne.

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 réglementation.

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	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, etc.)		
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 nationale unique (NIR pour la France)		
Catégories de personnes concernées		
Catégorie de personnes 1		
Catégorie de personnes 2		
Destinataires	Description	Type de destinataire
Destinataire 1		
Destinataire 2		
Destinataire 3		
Destinataire 4		
Destinataire 5		
Destinataire 6		
Destinataire 7		
Destinataire 8		
Destinataire 9		
Destinataire 10		
Destinataire 11		
Destinataire 12		
Destinataire 13		
Destinataire 14		
Destinataire 15		
Destinataire 16		
Destinataire 17		
Destinataire 18		
Destinataire 19		
Destinataire 20		
Destinataire 21		
Destinataire 22		
Destinataire 23		
Destinataire 24		
Destinataire 25		
Destinataire 26		
Destinataire 27		
Destinataire 28		
Destinataire 29		
Destinataire 30		
Destinataire 31		
Destinataire 32		
Destinataire 33		
Destinataire 34		
Destinataire 35		
Destinataire 36		
Destinataire 37		
Destinataire 38		
Destinataire 39		
Destinataire 40		
Destinataire 41		
Destinataire 42		
Destinataire 43		
Destinataire 44		
Destinataire 45		
Destinataire 46		
Destinataire 47		
Destinataire 48		
Destinataire 49		
Destinataire 50		
Destinataire 51		
Destinataire 52		
Destinataire 53		
Destinataire 54		
Destinataire 55		
Destinataire 56		
Destinataire 57		
Destinataire 58		
Destinataire 59		
Destinataire 60		
Destinataire 61		
Destinataire 62		
Destinataire 63		
Destinataire 64		
Destinataire 65		
Destinataire 66		
Destinataire 67		
Destinataire 68		
Destinataire 69		
Destinataire 70		
Destinataire 71		
Destinataire 72		
Destinataire 73		
Destinataire 74		
Destinataire 75		
Destinataire 76		
Destinataire 77		
Destinataire 78		
Destinataire 79		
Destinataire 80		
Destinataire 81		
Destinataire 82		
Destinataire 83		
Destinataire 84		
Destinataire 85		
Destinataire 86		
Destinataire 87		
Destinataire 88		
Destinataire 89		
Destinataire 90		
Destinataire 91		
Destinataire 92		
Destinataire 93		
Destinataire 94		
Destinataire 95		
Destinataire 96		
Destinataire 97		
Destinataire 98		
Destinataire 99		
Destinataire 100		
Destinataire 101		
Destinataire 102		
Destinataire 103		
Destinataire 104		
Destinataire 105		
Destinataire 106		
Destinataire 107		
Destinataire 108		
Destinataire 109		
Destinataire 110		
Destinataire 111		
Destinataire 112		
Destinataire 113		
Destinataire 114		
Destinataire 115		
Destinataire 116		
Destinataire 117		
Destinataire 118		
Destinataire 119		
Destinataire 120		
Destinataire 121		
Destinataire 122		
Destinataire 123		
Destinataire 124		
Destinataire 125		
Destinataire 126		
Destinataire 127		
Destinataire 128		
Destinataire 129		
Destinataire 130		
Destinataire 131		
Destinataire 132		
Destinataire 133		
Destinataire 134		
Destinataire 135		
Destinataire 136		
Destinataire 137		
Destinataire 138		
Destinataire 139		
Destinataire 140		
Destinataire 141		
Destinataire 142		
Destinataire 143		
Destinataire 144		
Destinataire 145		
Destinataire 146		
Destinataire 147		
Destinataire 148		
Destinataire 149		
Destinataire 150		
Destinataire 151		
Destinataire 152		
Destinataire 153		
Destinataire 154		
Destinataire 155		
Destinataire 156		
Destinataire 157		
Destinataire 158		
Destinataire 159		
Destinataire 160		
Destinataire 161		
Destinataire 162		
Destinataire 163		
Destinataire 164		
Destinataire 165		
Destinataire 166		
Destinataire 167		
Destinataire 168		
Destinataire 169		
Destinataire 170		
Destinataire 171		
Destinataire 172		
Destinataire 173		
Destinataire 174		
Destinataire 175		
Destinataire 176		
Destinataire 177		
Destinataire 178		
Destinataire 179		
Destinataire 180		
Destinataire 181		
Destinataire 182		
Destinataire 183		
Destinataire 184		
Destinataire 185		
Destinataire 186		
Destinataire 187		
Destinataire 188		
Destinataire 189		
Destinataire 190		
Destinataire 191		
Destinataire 192		
Destinataire 193		
Destinataire 194		
Destinataire 195		
Destinataire 196		
Destinataire 197		
Destinataire 198		
Destinataire 199		
Destinataire 200		
Destinataire 201		
Destinataire 202		
Destinataire 203		
Destinataire 204		
Destinataire 205		
Destinataire 206		
Destinataire 207		
Destinataire 208		
Destinataire 209		
Destinataire 210		
Destinataire 211		
Destinataire 212		
Destinataire 213		
Destinataire 214		
Destinataire 215		
Destinataire 216		
Destinataire 217		
Destinataire 218		
Destinataire 219		
Destinataire 220		
Destinataire 221		
Destinataire 222		
Destinataire 223		
Destinataire 224		
Destinataire 225		
Destinataire 226		
Destinataire 227		
Destinataire 228		
Destinataire 229		
Destinataire 230		
Destinataire 231		
Destinataire 232		
Destinataire 233		
Destinataire 234		
Destinataire 235		
Destinataire 236		
Destinataire 237		
Destinataire 238		
Destinataire 239		
Destinataire 240		
Destinataire 241		
Destinataire 242		
Destinataire 243		
Destinataire 244		
Destinataire 245		
Destinataire 246		
Destinataire 247		
Destinataire 248		
Destinataire 249		
Destinataire 250		
Destinataire 251		
Destinataire 252		
Destinataire 253		
Destinataire 254		
Destinataire 255		
Destinataire 256		
Destinataire 257		
Destinataire 258		
Destinataire 259		
Destinataire 260		
Destinataire 261		
Destinataire 262		
Destinataire 263		
Destinataire 264		
Destinataire 265		
Destinataire 266		
Destinataire 267		
Destinataire 268		
Destinataire 269		
Destinataire 270		
Destinataire 271		
Destinataire 272		
Destinataire 273		
Destinataire 274		
Destinataire 275		
Destinataire 276		
Destinataire 277		
Destinataire 278		
Destinataire 279		
Destinataire 280		
Destinataire 281		
Destinataire 282		
Destinataire 283		
Destinataire 284		
Destinataire 285		
Destinataire 286		
Destinataire 287		
Destinataire 288		
Destinataire 289		
Destinataire 290		
Destinataire 291		
Destinataire 292		
Destinataire 293		
Destinataire 294		
Destinataire 295		
Destinataire 296		
Destinataire 297		
Destinataire 298		
Destinataire 299		
Destinataire 300		
Destinataire 301		
Destinataire 302		
Destinataire 303		
Destinataire 304		
Destinataire 305		
Destinataire 306		
Destinataire 307		
Destinataire 308		
Destinataire 309		
Destinataire 310		
Destinataire 311		
Destinataire 312		
Destinataire 313		
Destinataire 314		
Destinataire 315		
Destinataire 316		
Destinataire 317		
Destinataire 318		
Destinataire 319		
Destinataire 320		
Destinataire 321		
Destinataire 322		
Destinataire 323		
Destinataire 324		
Destinataire 325		
Destinataire 326		
Destinataire 327		
Destinataire 328		
Destinataire 329		
Destinataire 330		
Destinataire 331		
Destinataire 332		
Destinataire 333		
Destinataire 334		
Destinataire 335		
Destinataire 336		
Destinataire 337		
Destinataire 338		
Destinataire 339		
Destinataire 340		
Destinataire 341		
Destinataire 342		
Destinataire 343		
Destinataire 344		
Destinataire 345		
Destinataire 346		
Destinataire 347		
Destinataire 348		
Destinataire 349		
Destinataire 350		
Destinataire 351		
Destinataire 352		
Destinataire 353		
Destinataire 354		
Destinataire 355		
Destinataire 356		
Destinataire 357		
Destinataire 358		
Destinataire 359		
Destinataire 360		
Destinataire 361		
Destinataire 362		
Destinataire 363		
Destinataire 364		
Destinataire 365		
Destinataire 366		
Destinataire 367		
Destinataire 368		
Destinataire 369		
Destinataire 370		
Destinataire 371		
Destinataire 372		
Destinataire 373		
Destinataire 374		
Destinataire 375		
Destinataire 376		
Destinataire 377		
Destinataire 378		
Destinataire 379		
Destinataire 380		
Destinataire 381		
Destinataire 382		
Destinataire 383		
Destinataire 384		
Destinataire 385		
Destinataire 386		
Destinataire 387		
Destinataire 388		
Destinataire 389		
Destinataire 390		
Destinataire 391		
Destinataire 392		
Destinataire 393		
Destinataire 394		
Destinataire 395		
Destinataire 396		
Destinataire 397		
Destinataire 398		
Destinataire 399		
Destinataire 400		
Destinataire 401		
Destinataire 402		
Destinataire 403		
Destinataire 404		
Destinataire 405		
Destinataire 406		
Destinataire 407		
Destinataire 408		
Destinataire 409		
Destinataire 410		
Destinataire 411		
Destinataire 412		
Destinataire 413		
Destinataire 414		
Destinataire 415		
Destinataire 416		
Destinataire 417		
Destinataire 418		
Destinataire 419		
Destinataire 420		
Destinataire 421		
Destinataire 422		
Destinataire 423		
Destinataire 424		
Destinataire 425		
Destinataire 426		
Destinataire 427		
Destinataire 428		
Destinataire 429		
Destinataire 430		
Destinataire 431		
Destinataire 432		
Destinataire 433		
Destinataire 434		
Destinataire 435		
Destinataire 436		
Destinataire 437		
Destinataire 438		
Destinataire 439		
Destinataire 440		
Destinataire 441		
Destinataire 442		
Destinataire 443		
Destinataire 444		
Destinataire 445		
Destinataire 446		
Destinataire 447		
Destinataire 448		
Destinataire 449		
Destinataire 450		
Destinataire 451		
Destinataire 452		
Destinataire 453		
Destinataire 454		
Destinataire 455		
Destinataire 456		
Destinataire 457		
Destinataire 458		
Destinataire 459		
Destinataire 460		
Destinataire 461		
Destinataire 462		
Destinataire 463		
Destinataire 464		
Destinataire 465		
Destinataire 466		
Destinataire 467		
Destinataire 468		
Destinataire 469		
Destinataire 470		
Destinataire 471		
Destinataire 472		

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

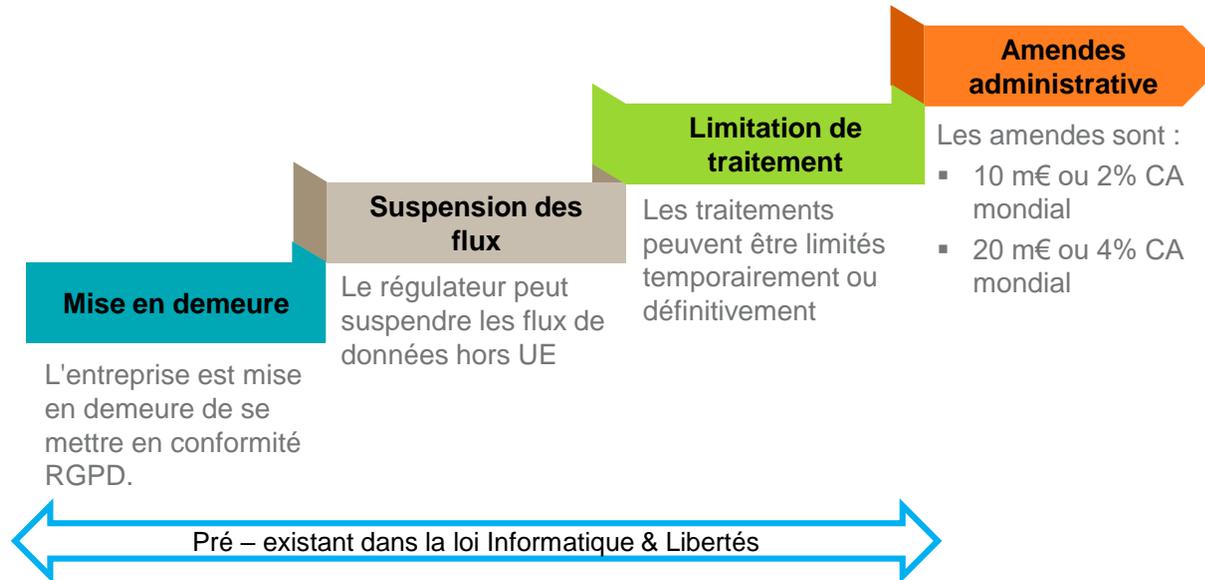
- Elles doivent contenir :
 - ✓ La description du traitement envisagé ainsi que sa finalité ;
 - ✓ L'évaluation de la nécessité de ce traitement ainsi que de la proportionnalité ;
 - ✓ L'évaluation du risque sur les droits et libertés des personnes concernées ;
 - ✓ Les mesures envisagées pour remédier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

