CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

Règlement européen sur la protection des données : ce qui change

19 avril 2017

Plan de la présentation

Liste des abréviations

- LIL = Loi Informatique et Libertés
- RGPD = règlement général sur la protection des données
- *GDPR = general data protection regulation*

- CIL = Correspondant Informatique et Libertés
- DPD = délégué à la protection des données
- *DPO = data protection officer*

- RT = Responsable de traitement
- ST = Sous-traitant

- G29 = groupe des CNIL de l'Union européenne (groupe de travail de l'article 29 de la directive 95/46/CE)
- EM = Etat membre (de l'Union européenne)
- LD = lignes directrices *(guidelines)*

I. INTRODUCTION GENERALE

1. Contexte d'adoption et évolutions par rapport à la directive 95/46/CE

- Proposition de la Commission européenne **en janvier 2012** (plus de 4 ans de négociations, près de 4.000 amendements devant le Parlement européen)

- RGPD adopté par le Parlement européen et le Conseil le 27 avril 2016 et publié au Journal officiel de l'Union européenne du 4 mai 2016

- **Applicable à partir du 25 mai 2018** => les traitements déjà mis en œuvre à cette date devront d'ici cette date être mis en conformité avec les dispositions du RGPD

- Pour les traitements à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuite et d'exécution de sanctions pénales : directive 2016/680 du 27 avril 2016 (transposition par les EM avant le 6 mai 2018)

https://www.cnil.fr/fr/le-reglement-europeen

1. Contexte d'adoption et évolutions par rapport à la directive 95/46/CE

Evolutions par rapport à la directive 95/46/CE

Directive 95/46/CE	RGPD
Champ d'application territorial fondé sur la localisation du RT au sein de l'UE	Champ d'application territorial fondé sur l'établissement du RT ou du ST au sein de l'UE ou si ciblage de résidents européens
Champ d'application matériel aux RT et non aux ST	Renforcement des obligations du ST
Transposition diverse dans les EM de l'UE	Texte unique directement applicable dans les mêmes termes dans tous les EM de l'UE
Pas adaptée à l'univers numérique (conçue pour des traitements stables dans le temps)	Adapté à l'univers numérique et à l'évolution des traitements
Dyptique 1- Formalités préalables 2- Contrôles *a posteriori*	**Tryptique** 1- Fin des déclarations/diminution du champ des autorisations 2- Responsabilité/*Accountability* (l'organisme se pose la question de savoir s'il assure en continu la conformité des traitements) 3-Maintien de la chaîne répressive et crédibilisation des sanctions (plafond commun pour toutes les autorités)

2. Cas de renvois aux droits nationaux

Le RGPD prévoit la possibilité pour les EM de prévoir des règles plus spécifiques dans le respect des garanties fixées par le RGPD

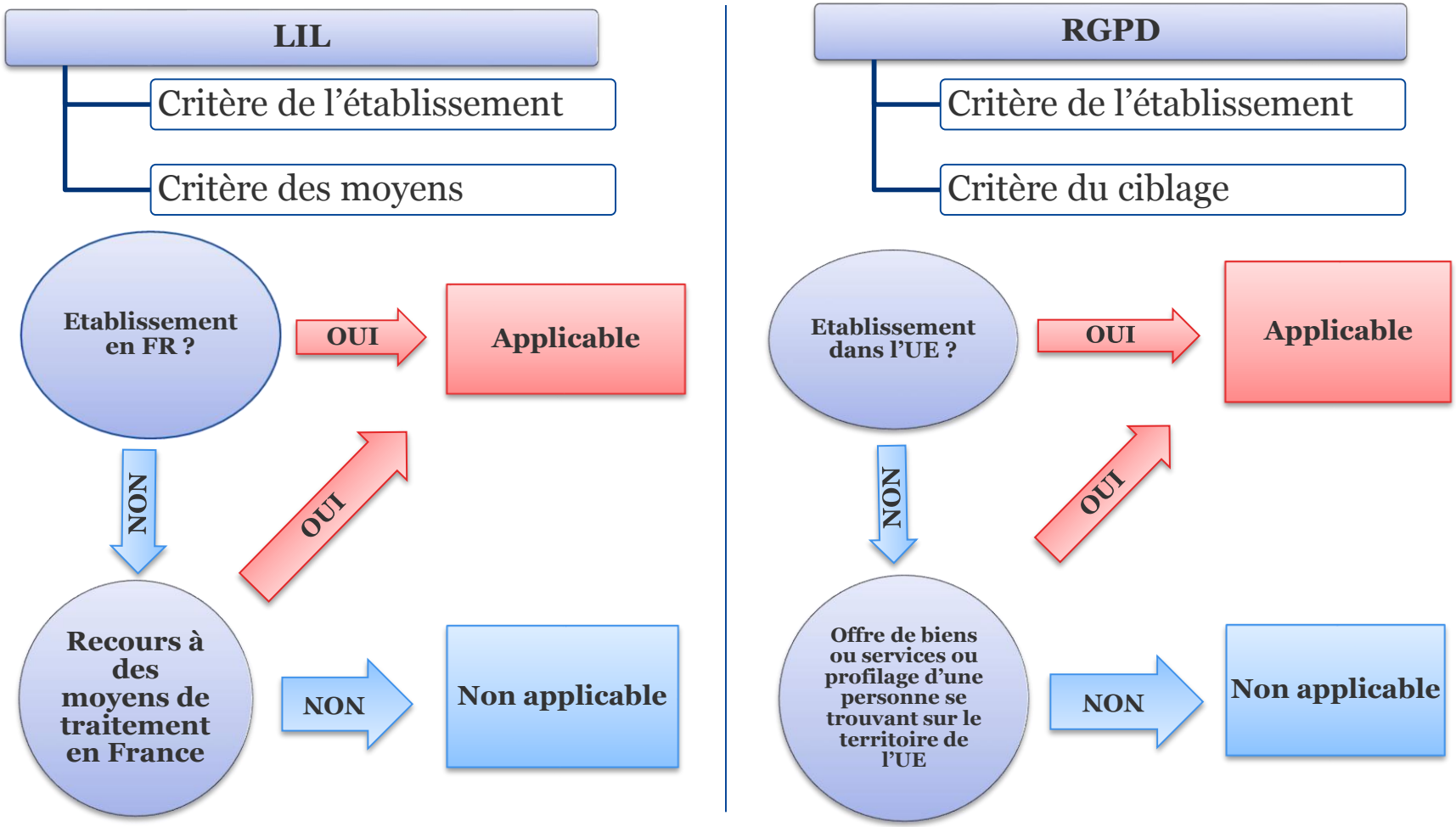
- Traitements relatifs à la santé (article 9.4)
  - ✓ Maintien ou introduction de conditions supplémentaires, y compris des limitations pour les données biométriques, génétiques ou de santé
- Traitement du numéro d'identification national (article 87)
  - ✓ Précision des conditions spécifiques du traitement du NIR
- Traitements de données en matière d'emploi (article 88)
  - ✓ Règles plus spécifiques notamment aux fins du recrutement, de l'exécution du contrat de travail, de l'organisation du travail, de la santé et de la sécurité au travail
- Traitements nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique (articles 6.2 et 86)
  - ✓ Limitation de la portée et des droits des personnes
  - ✓ Limitation aux principes de base de traitement des données
- Traitements à des fins d'archivage, de recherche scientifique ou historique ou statistiques (article 89)
  - ✓ Possible dérogations aux droits des personnes

3. Application territoriale élargie

Article 3

- Le RGPD s'applique :
  - **aux traitements effectués dans le cadre des activités de RT ou de ST établis sur le territoire de l'UE**, qu'ils aient ou non lieu dans l'UE *(**critère de l'établissement**)*
  - mais aussi **aux traitements effectués par des RT ou des ST non établis sur le territoire de l'UE dès lors qu'ils visent des personnes se trouvant sur le territoire de l'UE** dans le cadre des activités suivantes *(**critère du ciblage**)* :
    - offre à ceux-ci de biens ou de services ou
    - suivi de leur comportement au sein de l'UE

3. Application territoriale élargie



4. Réseau d'autorités de protection des données

Mécanisme du « guichet unique » et autorité chef de file
(article 56 et lignes directrices du G29)

- Si **traitement transfrontalier** (*traitement d'établissements d'un RT ou d'un ST* ***dans plusieurs EM*** *ou si traitement d'un établissement unique d'un RT ou d'un ST* ***mais qui affecte ou est susceptible d'affecter sensiblement des personnes dans plusieurs EM***), alors l'autorité de contrôle chef de file est celle de **l'établissement principal** ou de **l'établissement unique**

- Cette autorité sera le seul interlocuteur du RT ou du ST (« **guichet unique** »)

- Notion **d'établissement principal** = en principe lieu de son **administration centrale** (là où sont prises les décisions sur les moyens et finalités du traitement) **sauf si décisions prises dans un autre établissement de l'Union** (*voir critères du G29 pour identifier l'établissement principal*)

  - **Exemple** : une banque dont le siège social est en Allemagne mais dont le département assurance est localisé en Autriche où sont prises les décisions sur les traitements en matière d'assurance.
    - L'autorité de protection des données allemande sera l'autorité chef de file pour contrôler les traitements en matière bancaire
    - L'autorité de protection des données autrichienne sera l'autorité chef de file pour contrôler les traitements en matière d'assurance

4. Réseau d'autorités de protection des données

Mécanisme du « guichet unique » et autorité chef de file (article 56 et lignes directrices du G29)

- Chaque autorité de contrôle reste compétente pour traiter une réclamation introduite auprès d'elle si l'objet concerne uniquement l'établissement sur son territoire ou si affecte sensiblement les personnes de cet EM
  - **Exemple** : Une entreprise de marketing ayant son établissement principal en France décide de lancer un produit affectant uniquement les personnes résident au Portugal => les autorités française et portugaises peuvent décider de confier le dossier de plainte concernant ce traitement à l'autorité portugaise.

- Une autorité de contrôle peut être « **concernée** » par un traitement :
  - Si le RT ou le ST est établi sur son territoire
  - Si les personnes résidant sur son territoire sont sensiblement affectées par le traitement (ou susceptibles de l'être) ou
  - Si une réclamation a été introduite auprès de cette autorité.

- **Mécanisme de coopération** entre l'autorité de contrôle chef de file et les autres autorités de contrôle concernées (article 60)

- Si pas de consensus entre autorités => mécanisme de contrôle de la cohérence pouvant conduire le Comité européen de protection des données (**CEPD**) à rendre un avis

II. CE QUI CHANGE POUR LES PERSONNES CONCERNÉES

1. Renforcement de la transparence et exercice des droits facilité

- Renforcement des droit existants :
  - obligation générale de **faciliter** l'exercice des droits : information concise, transparente, compréhensible et aisément accessible (article 12)
  - **information** renforcée : coordonnées du délégué, durée de conservation, icônes normalisées… (articles 13 et 14)
  - droit **d'accès** précisé (article 15) et droit de rectification maintenu (article 16)
  - droit à **l'effacement** (« droit à l'oubli ») reconnu (article 17)
  - droit à être informé d'une **violation** des données en cas de risques élevés pour les intéressés (article 34)
  - droit **d'opposition** renforcé : le RT doit prouver l'existence d'un intérêt légitime supérieur à celui de la personne concernée (article 21)
- Nouveaux droits :
  - droit à la **limitation** du traitement (article 18)
  - droit à la **portabilité** des données (article 20)

1. Renforcement de la transparence et exercice des droits facilité

Modalités d'exercice des droits

- Les **délais** de réponse :
  - « *dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande* »
  - prolongation du délai de 2 mois compte tenu de la complexité et du nombre de demandes et sous réserve d'informer la personne de cette prolongation et des motifs du report dans un délai d'un mois à compter la réception de la demande

- **En cas de doutes** raisonnables sur l'identité de la personne, le RT peut demander des informations supplémentaires en vue de confirmer son identité.

- Modalités de **transmission** des informations & droits :
  - par écrit ou par d'autres moyens, y compris électroniques lorsque c'est approprié/possible
  - oralement à la demande de la personne et à condition que l'identité de la personne soit démontrée par d'autres moyens

1. Renforcement de la transparence et exercice des droits facilité

Modalités d'exercice des droits

- **Possibilité de refuser** de faire droit à la demande :
  - si le RT démontre qu'il n'est pas en mesure d'identifier la personne concernée
  - si les demandes sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif
  - pour une autre raison mais le RT informe alors la personne sans tarder et au plus tard dans un délai d'un mois à compter de la réception de la demande des motifs de son inaction et de la possibilité d'introduire une réclamation auprès de l'autorité de contrôle et de former un recours juridictionnel

- Pas de possibilité d'exiger un **paiement** sauf en cas de demandes manifestement infondées ou excessives ou pour toute copie supplémentaire (article 12 et article 15).

- Obligation de **notifier** à tout destinataire des données les rectifications, effacements ou limitations de traitement (article 19).

2. Consentement des mineurs

Consentement des enfants en ce qui concerne les services de la société de l'information (article 8)

- Conditions :
  - l'offre directe de services de la société de l'information à des enfants
  - le consentement constitue la condition de licéité dudit traitement

- L'âge de l'enfant :
  - consentement valide à partir de **16 ans** et possiblement moins dans la limite de 13 ans
  - en dessous de cet âge, le consentement doit être donné par le titulaire de la responsabilité parentale

- Obligation de raisonnablement vérifier, compte tenu des moyens technologiques disponibles, que ce consentement est donné par le titulaire de la responsabilité parentale.

3. Consécration du droit à l'oubli

Droit à l'effacement (« droit à l'oubli ») (article 17)

- Le droit à **l'effacement** trouve à s'appliquer dans 6 cas :
  - les données ne sont plus nécessaires au regard des finalités pour lesquelles elles sont collectées ou traitées
  - la personne a retiré son consentement au traitement de ses données
  - la personne a exercé son droit d'opposition et il n'existe pas de motif légitime impérieux pour le traitement
  - le traitement est illicite
  - l'effacement correspond au respect d'une obligation légale
  - les données ont été collectées dans le cadre de l'offre de services de la société de l'information pour les mineurs
- La **notification** du droit :
  - le RT qui a rendu des données publiques est tenu, compte tenu des technologies, d'informer les RT qui traitent ces données « *qu'il convient d'effacer tout lien vers ces données* », toute copie ou reproduction de celles-ci
- Les **exceptions** au droit à l'effacement :
  - liberté d'expression et d'information
  - respect d'une obligation légale
  - motif d'intérêt public dans le domaine de la santé
  - fins archivistiques dans l'intérêt public à des fins de recherche scientifique ou historique ou à des fins statistiques
  - constatation, exercice ou défense de droits en justice (référence à l'article 8 de la LIL)

4. Nouveaux droits

Droit à la portabilité (article 20 et lignes directrices du G29)

- Nouveau droit permettant à toute personne :
  - de **récupérer** les données la concernant qu'elle a fournies à un RT dans un format structuré, couramment utilisé et lisible par machine
  - de les **transmettre** à un autre RT ou de demander la transmission directement d'un RT à un autre RT si techniquement possible

- Objectif :
  - permettre aux personne de **contrôler** davantage leurs données, faciliter la libre circulation des données et stimuler la concurrence entre RT

- Conditions :
  - le traitement se fonde sur le **consentement** de la personne ou sur un **contrat** (*donc pas applicable si traitement fondé sur l'intérêt public ou intérêt légitime du RT*)
  - le traitement est effectué à l'aide de procédés automatisés

4. Nouveaux droits

Droit à la portabilité (article 20 et lignes directrices du G29)

- Données concernées :
  - données **fournies sciemment** et activement par la personne (ex : adresse, nom, âge…)
  - données **générées par son activité** et données observées (ex : données brutes générées par un compteur intelligent, données de localisation, rythme cardiaque…)
- Données exclues :
  - données **anonymes**
  - données **déduites ou dérivées** (ex : analyse des données brutes d'un compteur intelligent, cote de solvabilité, résultat d'une appréciation relative à la santé d'un utilisateur, profil)
- Le droit à la portabilité ne doit pas porter atteinte aux droits et libertés des tiers.

4. Nouveaux droits

Droit à la limitation du traitement (article 18)

- La limitation du traitement peut être demandée dans **4 cas**, lorsque :
  - le RT doit vérifier l'exactitude des données relatives à la personne concernée qui la conteste
  - le RT doit apprécier la légitimité des motifs légitimes d'une demande d'opposition de la personne concernée
  - sur le point d'être effacées, les données *« sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice »*
  - le traitement est illicite mais que la personne concernée préfère la limitation de l'utilisation des données la concernant à leur effacement

- La limitation entraine le **gel temporaire** du traitement des données qui ne peuvent plus faire l'objet que d'une conservation sauf si :
  - la personne concernée donne son consentement à une autre forme de traitement
  - leur traitement est nécessaire à *« la constatation, l'exercice ou la défense de droits en justice (…), la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public de l'Union ou d'un État membre »*

- Le RT doit **informer** la personne concernée avant la levée de cette mesure.

III. CE QUI CHANGE POUR LES ORGANISMES

A - Les nouvelles responsabilités

1. Logique de responsabilisation de tous les acteurs
2. Responsabilité conjointe des RT
3. Responsabilité spécifique des ST
4. Sanctions et voies de recours

A - Les nouvelles responsabilités

1. Logique de responsabilisation de tous les acteurs

- **Axe central du RGPD** : **responsabilisation de l'ensemble des organismes impliqués dans les traitements de données ciblant des résidents européens,** qu'ils soient ou non établis au sein de l'UE et qu'ils agissent en qualité de RT ou ST

  ⇒ Rééquilibrage des situations juridiques des RT et ST qui voient leurs obligations « égalisées » et leur responsabilité susceptible d'être conjointement engagée

- **Obligations partagées de mise en conformité dynamique (« *accountability* » - articles 24 et suiv.)** : mise en place et actualisation autant que nécessaire de mesures techniques et organisationnelles propres à garantir, et à démontrer à tout moment, le respect des principes « Informatique et Libertés »

  - Application des principes de protection des données dès la conception/par défaut (article 25)

  - Recours à divers outils de conformité, à moduler notamment en fonction des risques pour les personnes concernées : désignation d'un délégué à la protection des données (article 37), tenue d'un registre des activités de traitement (article 30), réalisation d'analyses d'impact sur la vie privée et les libertés (article 35), consultation préalable de l'autorité de contrôle (article 36), notification à celle-ci des violations de données (article 33), adhésion à des codes de conduite (article 40), certification de traitements (article 42)

A - Les nouvelles responsabilités

1. Logique de responsabilisation de tous les acteurs

- **Corollaires de cette nouvelle approche**
  - Allègement des obligations en matière de formalités préalables
    - suppression des déclarations
    - consultation de la CNIL pour les traitements les plus sensibles soumis à une analyse d'impact
    - champ des autorisations réduit (transferts hors UE fondés sur des CCT ad hoc + domaines d'intervention du droit national : traitements d'intérêt public, utilisation du NIR, etc.)
  - Nécessité de documenter les actions pour pouvoir prouver la conformité
    - registre des traitements
    - contrats de sous-traitance
    - analyses d'impact
    - politiques de confidentialité, procédures de gestion des réclamations, des violations de données, etc.
  - Accompagnement des autorités de contrôle dans les démarches des RT et ST
    - adoption de clauses types de sous-traitance
    - intervention en matière d'analyse d'impact (identification des cas obligatoires, délivrance de conseils), d'élaboration de codes de conduite, de mécanismes de certification, de labels et de marques en matière de protection des données
  - Renforcement des sanctions en cas de manquement
    - jusqu'à 20 millions d'euros ou 4% du CA mondial
    - autres sanctions possibles (recours juridictionnels)

A - Les nouvelles responsabilités

2. Responsabilité conjointe des RT

- **Pas d'évolution dans la définition du RT mais (ré)introduction de la notion de « responsables conjoints du traitement » (article 26) :**
  - lorsque plusieurs personnes/organismes déterminent conjointement les finalités et moyens d'un seul et même traitement
    - cf. avis du G29 sur les notions de RT et de ST évoquant cette notion figurant déjà dans la directive de 95 et illustrant la variété des situations où une telle « coresponsabilité » pourrait être admise
    - cf. recommandations de la CNIL sur le recours à des solutions de « cloud computing », qui reconnaît la possibilité que le prestataire soit considéré comme conjointement responsable en vertu de cette directive
  - doivent définir de façon transparente leurs obligations respectives par voie d'accord, sauf si elles résultent du droit de l'UE ou de l'EM
    - accord reflétant *dûment* les rôles de chacun des RT et mis à disposition des intéressés
    - fait notamment état des procédures en matière d'information et de respect des droits des personnes
  - les personnes concernées pourront exercer leurs droits à l'égard et à l'encontre de chacun d'entre eux

    => peu importe les termes de l'accord !

A- Les nouvelles responsabilités

3. Responsabilité spécifique des ST

- **Evolution dans la définition du cadre contractuel régissant ses relations avec le RT, élargissement du champ de ses obligations et introduction d'une responsabilité spécifique (articles 28 et suiv.) :**

  - ne traite que sur instruction *documentée* du RT et prend toutes les mesures de sécurité requises

  - ne (re)sous-traite pas sans
    - autorisation écrite du RT (spécifique ou générale avec info préalables sur les changements)
    - s'être assuré qu'il présente des garanties suffisantes pour assurer le respect des obligations en matière d'« *accountability* » (ex. : application d'un code de conduite/mécanisme de certification approuvé)
    - rappel des obligations du ST

  - aide le RT à garantir le respect de ses diverses obligations (droits des personnes, violations de données, analyses d'impact, consultation préalable de la CNIL, etc.)
    - compte tenu de la nature du traitement, dans toute la mesure du possible et par la mise en place de mesures techniques et organisationnelles appropriées
    - mise à disposition du RT de toutes les informations nécessaires pour démontrer le respect des obligations et contribution à la réalisation de tous les audits souhaités
    - information immédiate du RT en cas d'instruction paraissant illicite

  - doit désigner un délégué à la protection des données dans certains cas et tenir un registre des catégories de traitements effectués pour le compte du RT

=> A l'instar du RT, le ST pourra se voir imposer des mesures correctrices, infliger des sanctions administratives et être poursuivi en justice par les personnes concernées

A- Les nouvelles responsabilités

4. Sanctions et voies de recours

- **Pouvoirs reconnus aux « CNIL » (articles 58 et 83) : adoption de diverses « mesures correctrices » et/ou d'amendes administratives**
  - Un champ d'application élargi : RT + ST
  - Des nouvelles modalités décisionnelles : mécanisme de coopération pour les traitements transfrontaliers et application uniforme d'une seule et même décision
  - Des critères d'appréciation précisés pour le prononcé d'amendes : nature, gravité, durée de l'infraction ; intention ou négligence, catégories de données, degré de responsabilité, mesures d'atténuation du dommage, niveau de coopération avec l'autorité de contrôle, etc.
  - Des niveaux de sanction considérablement renforcés et gradués en fonction de catégories d'infraction : de 10 à 20 millions d'euros ou, pour une entreprise, de 2 à 4% du chiffre d'affaires mondial, le montant le plus élevé étant retenu

- **Chaque « CNIL »est compétente (a minima en tant qu' « autorité concernée »)** dès lors que le RT/ST est établi dans l'EM dont elle relève ou que des personnes résidant sur celui-ci sont impactées (**articles 55 et 56**)

=> l'autorité « chef de file » est par principe celle de l'établissement principal ou unique du RT ou ST (cf. lignes directrices du G29 sur le sujet)

A- Les nouvelles responsabilités

4. Sanctions et voies de recours

- **Des voies de recours déclinées au profit des personnes concernées**
  - Droit d'introduire une réclamation auprès d'une autorité de contrôle, notamment auprès de celle de l'EM où se trouve sa résidence (article 77)
    - Possibilité de saisir la CNIL du lieu de travail ou du lieu de commission du manquement
    - Obligation pour la CNIL saisie d'informer plaignant de l'état d'avancement et de l'issue de la réclamation dans un délai de 3 mois, et de la possibilité d'un recours juridictionnel en cas de manquement à cette obligation
  - Droit à un recours juridictionnel contre un RT et/ou un ST, en particulier pour obtenir réparation du préjudice subi (articles 79 à 82)
    - Au choix : juridiction de l'EM où RT/ST est établi ou celle de sa résidence, sauf pour autorités publiques
    - Tout RT est responsable du dommage (matériel ou moral) causé par le traitement
    - ST responsable qu'en cas de non respect de ses obligations propres ou d'agissements en dehors des instructions licites de celui-ci
    - Exonération possible si RT/ST apporte la preuve qu'on ne peut lui imputer le fait générateur
    - Responsabilité solidaire avec action récursoire possible

B - Les acteurs, obligations et outils de la conformité

1. Délégué à la protection des données
2. Registre des traitements
3. L'analyse d'impact
4. Notification des violations de données
5. Certification et codes de conduite

B - Les acteurs, obligations et outils de la conformité

1. Délégué à la protection des données

Considérant 97 et articles 37 à 39

Lignes directrices du G29 (groupe des « CNIL » européennes) sur le délégué à la protection des données et « FAQ » adoptées dans leur version finale le 5 avril 2017 (LD G29)

Lien vers les Lignes directrices délégué

Lien site CIL - Devenir Délégué

- Devient un véritable pilote de la conformité interne
- Désignation obligatoire dans certains cas
- Est « *une personne possédant des connaissances spécialisées de la législation et des pratiques en matière de protection des données [qui] devrait aider le responsable du traitement ou le sous-traitant à vérifier le respect, au niveau interne, du présent règlement* » (cons. 97)
- Statut et responsabilités similaires à ceux du CIL
- Qualifications, prérogatives et missions renforcées
- Sanction en cas de non-respect des dispositions relatives au délégué

B - Les acteurs, obligations et outils de la conformité

1. Délégué à la protection des données

3 cas de désignation obligatoire pour les RT ou les ST

1. Pour toute **autorité publique** ou tout **organisme public** (collectivités territoriales, Etat, établissements publics, etc.), quel que soit la nature du traitement
   - Désignation recommandée par le G29 pour les organismes privés chargés d'une mission de service public

2. Si les **activités de base** de l'organisme consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un **suivi régulier et systématique à grande échelle des personnes concernées**
   - « Activités de base » = cœur de métier, activités clés pour atteindre les objectifs de l'organisme (pas les activités auxiliaires telles que support informatique et traitements RH)
   - « Grande échelle » = impossibilité de fixer un seuil chiffré, analyse à mener au regard de facteurs tels que le nombre de personnes, le volume de données, la durée ou l'étendue géographique du traitement (ex. : traitement de données clients par une société d'assurance, traitement de données de circulation d'un individu utilisant un transport public urbain)
   - « Suivi régulier et systématique » = continu, récurrent, constant, périodique, préétabli, organisé ou méthodique (ex. : profilage, lutte contre la fraude, publicité comportementale, appareils connectés, etc.)

B - Les acteurs, obligations et outils de la conformité

1. Délégué à la protection des données

3. Si les **activités de base** de l'organisme consistent en des traitements à **grande échelle** de **données sensibles** (article 9) ou de **données relatives aux condamnations et infractions spéciales** (article 10)

- **Ces cas de désignation obligatoire s'appliquent que l'organisme soit RT ou ST, sous peine de sanction** (jusqu'à 2% du chiffre d'affaires annuel mondial ou 10.000.000 € - article 83.4)

- **Les EM peuvent prévoir d'autres cas**

- **Recommandations du G29**
  - Documenter l'analyse menée pour déterminer si un délégué doit obligatoirement être désigné
  - Hors cas de désignation obligatoire, la désignation d'un délégué est recommandée
  - Si un délégué est désigné sur une base volontaire et qu'il porte le titre de « délégué à la protection des données », sa désignation, sa fonction et ses missions sont soumises aux articles 37 à 39
  - Le délégué est désigné pour l'ensemble des traitements mis en œuvre par l'organisme

B - Les acteurs, obligations et outils de la conformité

1. Délégué à la protection des données

Mutualisation et externalisation (article 37 et sections 2.3 et 2.5 des LD G29)

- **Mutualisation possible : flexibilité laissée aux organismes**
  - Dans le secteur privé : même délégué pour un groupe d'entreprise à condition qu'il soit « *facilement joignable à partir de chaque lieu d'établissement* »
  - Dans le secteur public : même délégué pour plusieurs organismes « *compte tenu de leur structure organisationnelle et de leur taille* »
  - Recommandation du G29 : le délégué doit être en mesure de communiquer efficacement avec les personnes concernées et l'autorité de contrôle (coordonnées accessibles, communication dans la langue de la personne ou de l'autorité, joignable physiquement ou via un numéro dédié ou d'autres moyens de communication sécurisés)

- **Externalisation possible sur la base d'un contrat de service**
  - Disparition de la limite actuelle prévue par le décret de 2005
  - Externalisation auprès d'un individu ou d'un organisme
  - Recommandations du G29 si externalisation auprès d'un organisme :
    - chaque membre de l'organisme exerçant les fonctions de délégué doit remplir les exigences de la section 4 (ex : absence de conflit d'intérêts)
    - spécifier dans le contrat de service la répartition des missions au sein de l'équipe et désigner une personne en tant que contact principal et personne en charge du client

B - Les acteurs, obligations et outils de la conformité

1. Délégué à la protection des données

Qui peut être délégué ? (articles 37.5 et 38 et sections 2.5 et 3.5 des LD G29)

- **Exigence de qualification du délégué**, désigné « *sur la base :*
  - *de ses qualités professionnelles ,*
  - *en particulier de ses connaissances spécialisées de la législation et des pratiques en matière de protection des données,*
  - *et de sa capacité à accomplir les tâches énumérées à l'article 39* »

- **Recommandations du G29**
  - Niveau d'expertise adapté à la sensibilité, la complexité et le volume de données traitées par l'organisme
  - Connaissance du secteur d'activité et de l'organisation du RT ou du ST
  - Compréhension suffisante des opérations de traitement, des SI et des besoins de l'organisme en termes de sécurité et de protection des données
  - Solide connaissance des règles et procédures administratives s'agissant d'une autorité ou d'un organisme public
  - Capacité à accomplir ses missions = qualités personnelles (intégrité, haut niveau d'étique professionnelle), connaissances et bon positionnement au sein de l'organisme
  - Localisation au sein de l'UE

- **Absence de conflit d'intérêts**
  - Le délégué ne peut occuper une fonction au sein de l'organisme qui le conduit à déterminer les finalités et les moyens d'un traitement, appréciation au cas par cas (voir exemples dans les LD G29)

B - Les acteurs, obligations et outils de la conformité

1. Délégué à la protection des données

Les missions du délégué (article 39 et section 4 des LD G29)

- **Informe** et **conseille** l'organisme ainsi que les salariés/agents sur les obligations qui lui incombent en vertu du RGPD et d'autres dispositions de l'Union ou de l'EM concerné

- **Contrôle le respect du RGPD**, d'autres dispositions de l'UE ou de l'EM concerné et des règles internes du RT ou du ST (sensibilisation, formation du personnel, audits,…)

  - Le délégué n'est pas personnellement responsable en cas de non-conformité avec le RGPD. Le respect des règles en matière de protection des données relève de la responsabilité du RT ou du ST.

- Dispense des **conseils** en ce qui concerne **l'analyse d'impact** relative à la protection des donnée et **vérifie son exécution**

  - Recommandations du G29 :

    - le conseil du délégué peut porter sur les questions suivantes : nécessité ou non d'effectuer une analyse d'impact, méthode à utiliser, recours ou non à un prestataire, types de garanties à appliquer pour atténuer les risques, évaluation de la bonne exécution de l'analyse et de la conformité des conclusions
    - si le RT n'est pas d'accord avec le conseil du délégué, la documentation relative à l'analyse d'impact justifie par écrit les raisons pour lesquelles son conseil n'a pas été pris en compte
    - préciser clairement les missions du délégué s'agissant de l'analyse d'impact dans le contrat/lettre de mission du délégué et dans l'information des employés

B - Les acteurs, obligations et outils de la conformité

1. Délégué à la protection des données

Les missions du délégué (article 39 et section 4 des LD G29)

- **Coopère avec l'autorité de contrôle** et fait office de **point de contact pour les personnes concernées** sur toute question en lien avec les traitements
  - Le délégué facilite l'accès par les autorités aux documents et informations dans le cadre de l'exercice des missions et des pouvoirs de cette autorité (par exemple lors d'échanges avec l'autorité dans l'instruction d'une plainte, ou en cas besoin de précisions sur un projet en cours ou bien encore, dans le cadre d'un contrôle de l'autorité)
  - Les coordonnées du délégué devront figurer dans la mention d'information (article 13.1.b)
  - La notion de coordonnées inclut les informations permettant de joindre facilement le délégué (adresse postale, numéro de téléphone ou adresse électronique dédié)
  - En tant que bonne pratique, il est recommandé d'informer l'autorité de contrôle et les employés du nom et des coordonnées du délégué

- S'assure de la **bonne tenue de la documentation** relative aux traitements
  - La tenue du registre incombe au RT ou au ST (article 30)
  - En pratique, cette mission peut être confiée au délégué (le registre est un outil permettant au délégué de réaliser sa mission de contrôle de la conformité, d'information et de conseil du RT ou du ST). Le délégué peut également établir un bilan annuel de ses activités.

Ces missions ne sont pas limitatives, le RT ou le ST peut lui en confier d'autres

B - Les acteurs, obligations et outils de la conformité

1. Délégué à la protection des données

Les moyens du délégué (article 38 et section 3 des LD G29)

- **Des moyens et ressources à obtenir de la part de l'organisme qui le désigne afin de permettre l'exercice effectif de ses missions**
  - **Associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données**

    ▪ Recommandations du G29 :
    - associer le délégué le plus tôt possible (protection des données dès la conception)
    - l'inviter à participer régulièrement aux réunions des cadres supérieurs
    - recommander sa présence pour la prise de décisions ayant des répercussions sur la protection des données
    - dûment prendre en compte de l'avis du délégué
    - documenter les raisons pour lesquelles l'avis du délégué n'a pas été suivi
    - consulter le délégué en cas de violation de données ou autre incident

  - **Doit disposer des ressources nécessaires à l'exécution de ses missions,** notamment accès aux données et aux traitements et au maintien de ses connaissances (formation continue)

    - Recommandations du G29 : soutien actif de la direction, temps suffisant, ressources financiers, infrastructures, personnel (équipe-réseau actif), communication officielle sur la désignation, accès aux autres services

B - Les acteurs, obligations et outils de la conformité

1. Délégué à la protection des données

Les moyens du délégué (article 38 et section 3 des LD G29)

- **Indépendance dans l'accomplissement de ses missions**

  - Recommandation du G29 : le délégué ne doit pas recevoir d'instruction sur la manière de traiter un sujet, d'instruire une plainte, sur le résultat qui doit être obtenu ou sur l'opportunité de consulter l'autorité de contrôle

- **Pas de sanction du fait de l'accomplissement de ses missions**

  - Recommandations du G29 :
  - le délégué doit bénéficier d'une protection suffisante dans l'exercice de ses missions
  - seules sont interdites les sanctions imposées en raison de l'exercice des missions de délégué (ex. : le délégué ne peut être relevé de ses fonctions s'il conseille au RT d'effectuer une analyse d'impact mais que le RT n'est pas d'accord avec l'analyse du délégué).
  - il peut être mis fin aux fonctions du délégué pour des raisons légitimes (ex. : vol, harcèlement, faute grave)

- **Fait directement rapport au niveau le plus élevé de l'organisme**

- **Sanction** en cas de non-respect des dispositions relatives au délégué => **amende jusqu'à 10.000.000 € ou 2% du chiffre d'affaires total mondial** (article 83.4)

B - Les acteurs, obligations et outils de la conformité

2. Registre

LIL : les CIL tiennent un registre des traitements mis en œuvre par l'organisme qui les ont désignés (art 48 du décret du 20 octobre 2005)

RGPD : 2 changements (article 30)

1 – Une obligation qui s'étend à tous les RT - avec ou sans délégué

Le contenu du registre du RT :

- nom et les coordonnées du RT et du délégué
- finalités du traitement
- catégories personnes concernées et les catégories de données
- catégories de destinataires
- dans la mesure du possible, les délais prévus pour l'effacement

Qu'est ce qui change par rapport au registre du CIL ?

- les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale
- dans la mesure du possible, une description des mesures de sécurité techniques et organisationnelles

B - Les acteurs, obligations et outils de la conformité

2. Registre

2 - Cette obligation s'étend aux ST qui devront tenir le registre des traitement qu'ils effectuent pour le compte de leurs client RT

Contenu du registre du ST :

- nom et les coordonnées du ou des ST
- nom et les coordonnées de chaque RT pour le compte duquel le ST agit
- catégories de traitements effectués pour le compte de chaque RT
- transferts de données vers un pays tiers ou à une organisation internationale
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles

B - Les acteurs, obligations et outils de la conformité

2. Registre

Pas d'obligation de tenir un registre pour les organismes ayant moins de 250 employés, **SAUF :**

- si le traitement comporte un risque pour les droits et des libertés des personnes concernées
- s'il n'est pas occasionnel
- s'il porte notamment sur les catégories particulières de données (santé, religions, condamnations pénales, infractions…)

B - Les acteurs, obligations et outils de la conformité

3. Analyse d'impact (PIA)

- **LIL : un concept qui existait déjà avec une orientation « sécurité »**

L'article 34 de la LIL impose au RT de prendre les mesures nécessaires pour préserver la sécurité des données. Ce qui implique identifier les risques engendrés par son traitement avant de déterminer les moyens adéquats pour les traiter.

3 guides PIA publiés par la CNIL
(en cours de révision)

- **RGPD : un outil de la conformité à part entière** (article 35)

L'analyse d'impact relative à la protection des données devient un outil important qui va permettre à un RT de bâtir un traitement de données à caractère personnel ou un produit respectueux de la vie privée, d'apprécier les impacts sur la vie privée des personnes concernées et de démontrer que les principes fondamentaux sont respectés.

- **Lignes directrices du G29** adoptées le 5 avril 2017 et soumises à consultation jusqu'au 23 mai 2017

B - Les acteurs, obligations et outils de la conformité

3. Analyse d'impact (PIA)

Enjeux

Analyser l'impact d'un traitement avec un changement de prisme

Passage de l'évaluation du risque pour un organisme (focus interne)

Évaluation du risque pour la vie privée des personnes concernées (focus externe)

B - Les acteurs, obligations et outils de la conformité

3. Analyse d'impact (PIA)

Qui est concerné ?

- **Les personnes physiques** dont les données font l'objet d'un traitement, car il s'agit d'identifier risques qu'elles encourent :

Exemple : Un responsable de traitement qui fait régulièrement livrer des colis chez ses clients stocke les adresses et les codes d'accès aux immeubles dans une base non sécurisée et accessible à tout son personnel :

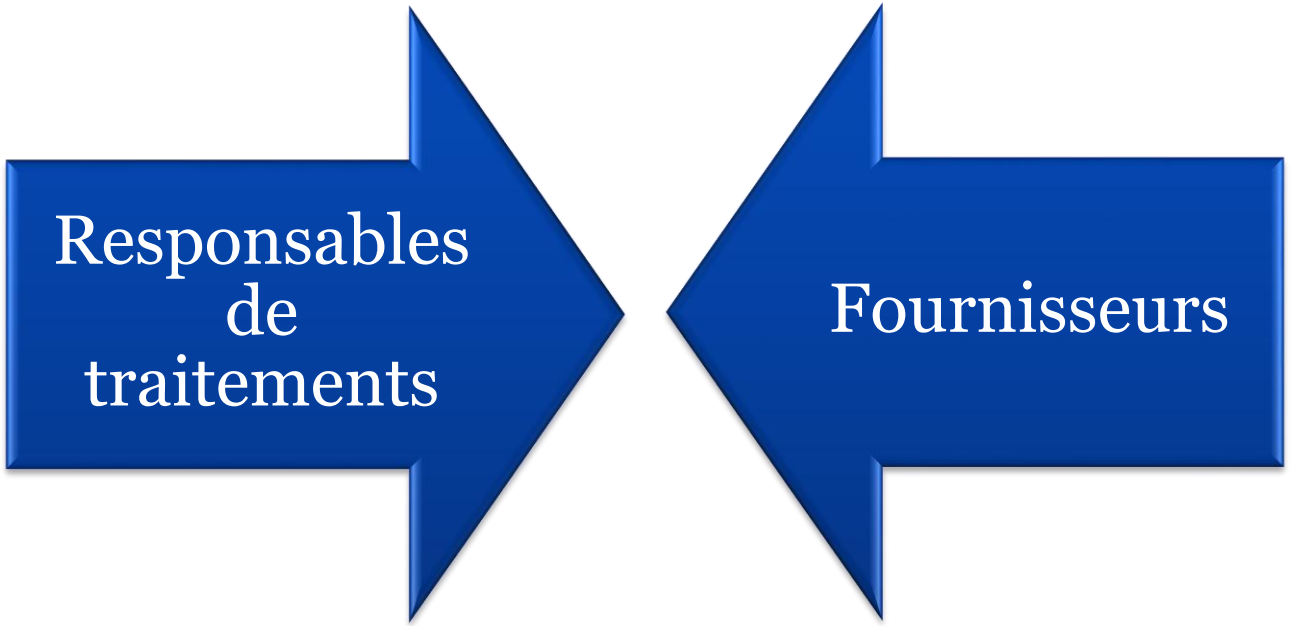
Vols de ces informations = série de cambriolages
Conséquence pour les clients = préjudice moral et financier

- Une analyse d'impact aurait permis au responsable de traitement d'identifier l'évènement redouté (le vol des informations) ainsi que les menaces qui le rendait possible (personnel interne, base non sécurisée). Il aurait pu estimer ce risque en termes de gravité et de vraisemblance et prendre les mesures nécessaires pour le traiter notamment au niveau de l'impact (cambriolage) potentiel pour ses clients.

B - Les acteurs, obligations et outils de la conformité

3. Analyse d'impact (PIA)

Qui réalise cette analyse ?



- **Le PIA est idéalement mené dans le cadre de la conception de leurs traitements de données à caractère personnel**

- **Le PIA est idéalement mené dans le cadre de la conception de leurs produits, les solutions seront utilisées dans de nombreux traitements**

B - Les acteurs, obligations et outils de la conformité

3. Analyse d'impact (PIA)

- DPIA obligatoire ?
  - Au moins 2 critères
    - Évaluation/*scoring*
    - Décision automatique avec effet légal
    - Surveillance systématique
    - Données sensibles
    - Large échelle
    - Croisement de données
    - Personnes vulnérables
    - Usage innovant
    - Transfert hors UE
    - Blocage d'un droit/contrat

- DPIA pas nécessaire ?
  - Pas susceptible d'engendrer des risques élevés
  - Déjà autorisé (tant que le traitement n'a pas changé et que les conditions de mise en œuvre sont respectées !)
    - Autorisations unitaires
    - Formalités simplifiées
  - Base légale

B - Les acteurs, obligations et outils de la conformité

3. Analyse d'impact (PIA)

Le RT doit :

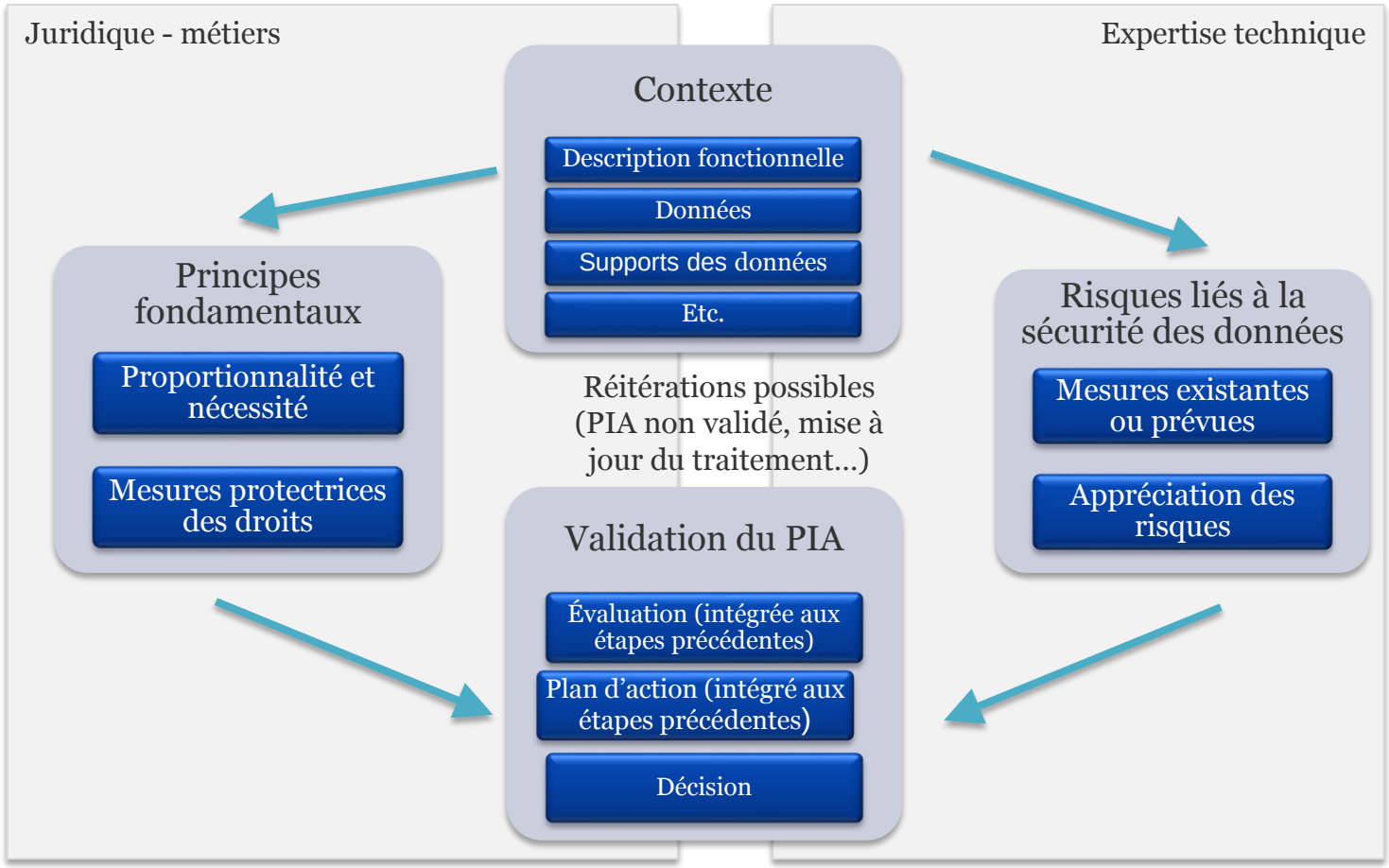
- tenir compte des codes de conduite existants (cf. 35.8)
- demander le conseil du DPO s'il existe (cf. 35.2)
- peut demander l'avis des personnes concernées ou de leurs représentants (cf. 35.9)
- évaluer si le traitement est conforme au PIA, au moins quand les risques évoluent (cf. 35.11)

Que contient-elle ?

- une description du traitement et de ses finalités
- une évaluation de la nécessité et de la proportionnalité
- une appréciation des risques sur les droits et libertés des personnes concernées,
- les mesures envisagées pour traiter ces risques et se conformer au règlement (cf. 35.7)

B - Les acteurs, obligations et outils de la conformité

3. Analyse d'impact (PIA)



B - Les acteurs, obligations et outils de la conformité

3. Analyse d'impact (PIA)

- Le PIA est un moyen de se mettre en conformité et de le démontrer (notion d'*accountability*)

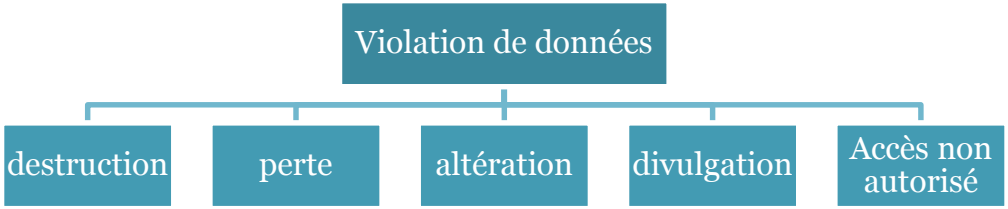
- Les principes et droits fondamentaux (finalité, information…), «non négociables », fixés par la loi, devant être respectés et ne pouvant faire l'objet d'aucune modulation

- La gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données

B - Les acteurs, obligations et outils de la conformité

4. Notification des violations de données

Article 33



Exemples :

Nom	Type du site/entreprise	Date	Assaillant	Type de données	nombre	victimes	impact
Ashley Madison	Site de rencontres adultérines	Août 2015	Impact Team – un groupe de hackers	Informations confidentielles à propos les utilisateurs du site, y compris les noms, adresses électroniques, lieu de résidence et préférences sexuelles	~31-33 million de profils	Utilisateurs du service et leurs familles	Au moins 4 suicides (1 confirmé), divorces (nombre inconnu), extorsions/chantage
Clouds pets (Spiral Toys)	Jouets en peluche connectés	Mars 2017	inconnu	2,2 millions de messages audio	~ 800 000 clients	Utilisateurs du service (enfants) et leurs familles	Demandes de rançon
Sony Playstation Network	Service en ligne	20 avril 2011	inconnu	Noms, e-mails, adresses, numéros, de cartes de crédit, histoires d'achat	77 millions de profils piratés, dont environ 12 millions étaient associés aux numéros de carte de crédit	Clients	58 sommations contre Sony, d'après lesquels les poursuivants ont subi des pertes financières

B - Les acteurs, obligations et outils de la conformité

4. Notification des violations de données

Qui	A qui	Quand	Contenu
RT **ST au RT**	Autorité	✓dans les meilleurs délais, et si possible dans les 72 heures de la connaissance de la violation ✓à moins que la violation ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes.	✓ nature de la violation ✓ nombre approximatif de personnes concernées ✓ mesures prises pour remédier à la violation ✓nom et coordonnées du délégué ou d'un autre point de contact ✓conséquences ✓mesures prises pour y remédier ou atténuer les conséquences
RT	Personne concernée	✓ dans les meilleurs délais ✓si la violation est susceptible d'engendrer un risque élevé pour la personne concernée ✓sauf si le RT a pris des mesures garantissant que le risque élevé n'est plus susceptible de se matérialiser (ex : recours à des données chiffrées) ou la notification représenterait un effort disproportionné pour le RT notamment au regard du nombre de personnes concernées (dans ce cas communication publique)	✓ nature de la violation et au moins ✓ mesures prises pour remédier à la violation ✓nom et coordonnées du délégué ou d'un autre point de contact ✓conséquences ✓mesures prises pour y remédier ou atténuer les conséquences

Sanction (article 83.4.a) **:** la violation de ces obligations peut faire l'objet d'une amende à hauteur de 10M€ ou, dans le cas d'une entreprise, de 2% du chiffre d'affaires mondial consolidé, le montant le plus élevé étant retenu

B - Les acteurs, obligations et outils de la conformité

5. Certification et codes de conduite

La certification est une procédure par laquelle une tierce partie (externe) donne l'assurance écrite qu'un produit, processus, service ou compétence est en conformité avec certaines normes.

Le code de conduite est le recueil des bonnes pratiques d'un secteur d'activités ou de catégories de traitement de données.

Un label (marque de confiance ou sceau) est un logo ou un symbole indiquant que la conformité à un référentiel a été vérifiée. L'utilisation du label est habituellement contrôlée par l'organe (interne ou externe) d'élaboration de normes.

L'homologation est l'approbation donnée par une autorité pour permettre la mise à exécution. Il s'agit donc d'une décision préalable à la mise en circuit d'un dispositif ou d'une procédure.

L'accréditation est la reconnaissance formelle de l'impartialité et de la compétence de l'organisme d'évaluation de la conformité (tiers certificateur).

B - Les acteurs, obligations et outils de la conformité

5. Certification et codes de conduite

• La certification comme preuve de la conformité	Art 24, 25, 28, 32 (et csdts)
• La certification comme garantie au transfert de DCP hors UE	Art 46
• Les tiers certificateurs	Art 43
• Les pouvoirs de l'autorité : mener des vérifications, retirer ou faire retirer la certification, approuver les critères d'accréditation et accréditer des tiers certificateurs, délivrer des labels et adopter des référentiels…	Art 58
• L'encouragement à l'adoption des certifications, labels et marques de protection des données (notamment au niveau européen)	Art42
• Les sanctions	Art 83

B - Les acteurs, obligations et outils de la conformité

5. Certification

Champ d'application	Contenu	Organisme de certification	Autorité
✓Association représentant des catégories de RT/ST ✓Les RT/ST non soumis au Règlement afin d'encadrer leurs transferts et de fournir des garanties appropriées dans ce cadre	Certification du traitement mis en œuvre par le RT/ST Certification délivrée par ✓L'organisme de certification ou ✓L'autorité de protection ✓ Certification délivrée pour une durée maximale de 3 ans	✓Accrédité par les autorités ou un organisme national d'accréditation ✓Délivre la certification ✓Retire la certification	✓Elabore et approuve les critères de certification ✓Retire la certification ✓Elabore et approuve les critères d'accréditation des organismes de certification ✓Retire l'accréditation des organismes de certification

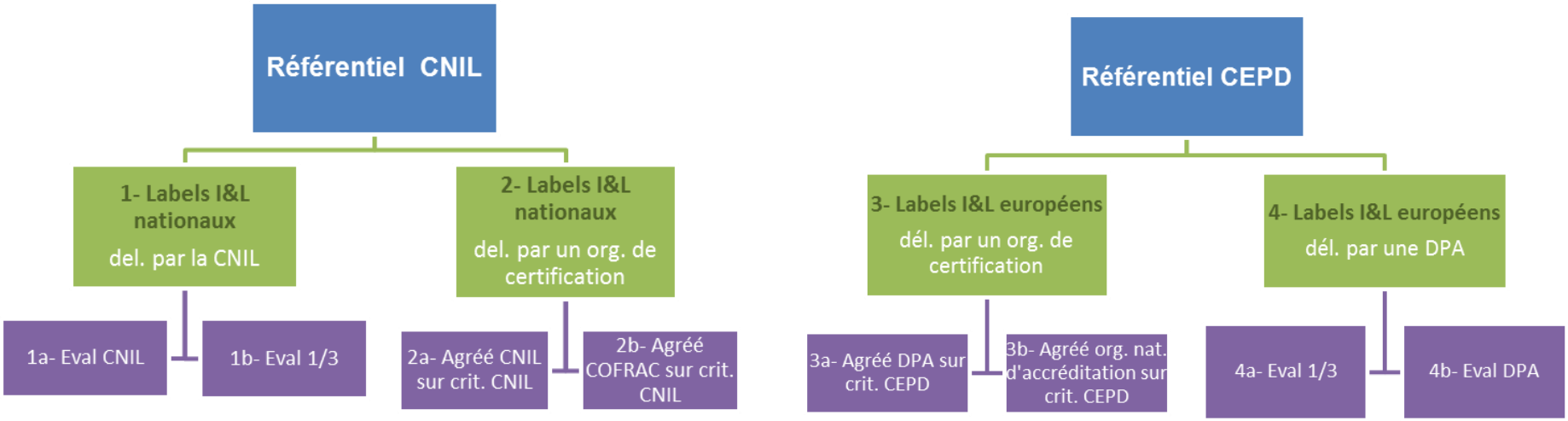
B - Les acteurs, obligations et outils de la conformité

5. Codes de conduite

Champ d'application	Contenu	Procédure	Autorité
✓Association représentant des catégories de RT/ST ✓Les RT/ST non soumis au RGPD afin d'encadrer leurs transferts et de fournir des garanties appropriées dans ce cadre	Précise les modalités d'application des dispositions du RGPD. Ex: ✓Intérêt légitime ✓Pseudonymisation ✓Exercice des droits des personnes ✓Notification des violations ✓Transferts…..	**Organisme :** ✓Accrédité par les autorités ✓Surveille le respect du code ✓Prise de mesures en cas de violation au code (ex: exclusion du code d'un des membres)	✓Analyse ✓Approuve ✓Publie ✓Accrédite l'organisme ✓Elabore les critères d'accréditation de l'organisme ✓Révoque l'accréditation

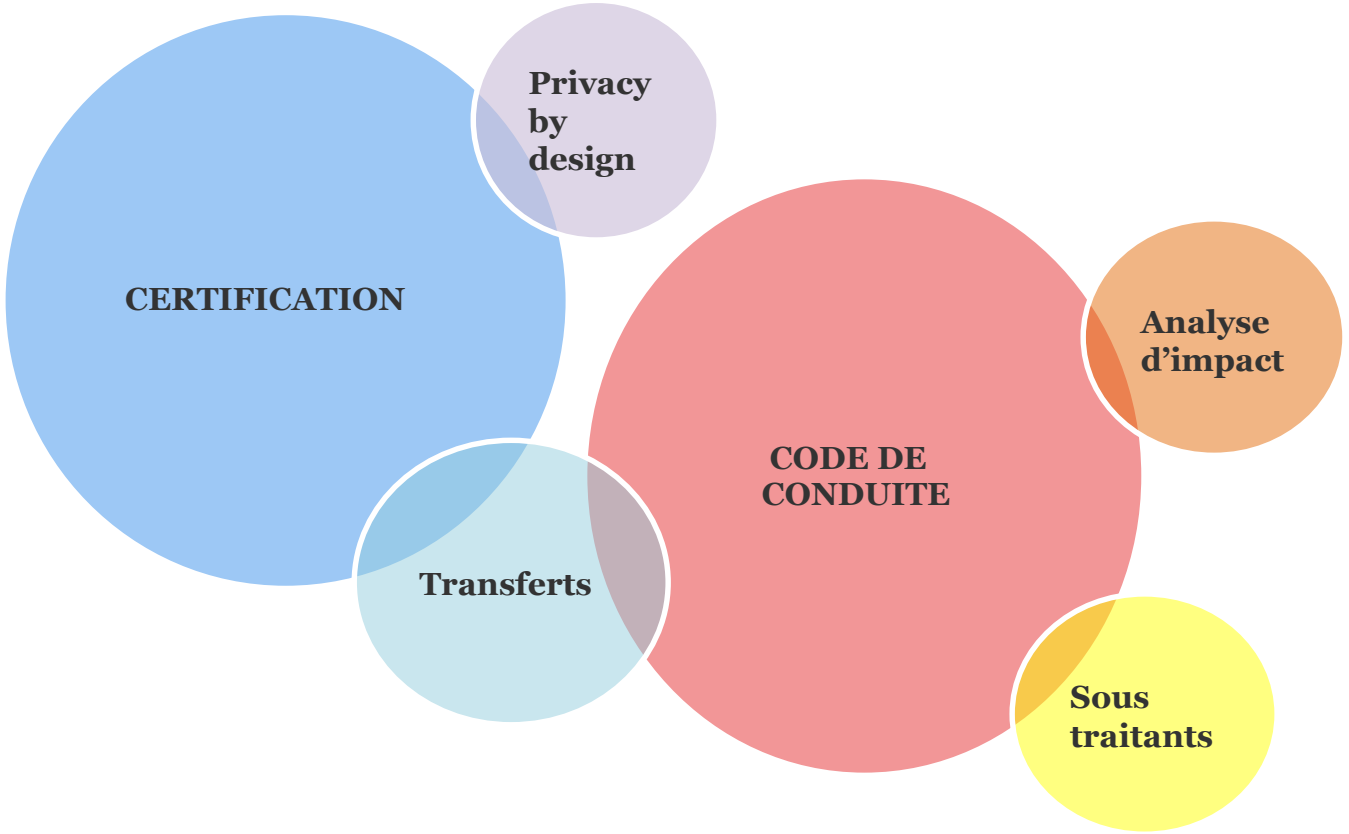
B - Les acteurs, obligations et outils de la conformité

5. Certification et codes de conduite



B - Les acteurs, obligations et outils de la conformité

5. Certification et codes de conduite



IV. COMMENT SE PRÉPARER ?

Comment se préparer ?

Se préparer en 6 étapes

Merci de votre attention !

Pour toute question :

correspondants@cnil.fr