CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

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

RGPD
Règlement Général sur la Protection des Données personnelles

AMRAE
27 juin 2018

Qu'est ce que le RGPD ?

- Des principes précisés
  - collecte loyale et transparente
  - principe de finalité (légitime, explicite et spécifique) et possible réutilisation des données pour des traitements ultérieurs sous certaines conditions
  - principe de proportionnalité des données (adéquates, pertinentes et non excessives)
  - durée de conservation limitée
  - garantie d'une sécurité appropriée des données
- Les bases légales
  - distinction entre les données à caractère personnel et les données sensibles pour lesquelles le principe d'interdiction maintenue (art 9).
  - définition des données sensibles est étendue (prise en compte des données génétiques)
  - bases légales renforcées (consentement)
  - renversement de la charge de la preuve pesant désormais sur le RT/ST

Qu'est ce que le RGPD ?

- De nouvelles définitions
  - Données génétiques, données biométriques, pseudonymisation, profilage (art 20) limitation du traitement (art 18)
  - Traitement transfrontalier, établissement principal du RT – ST, autorité de contrôle concernée, objection pertinente et motivée
  - BCR

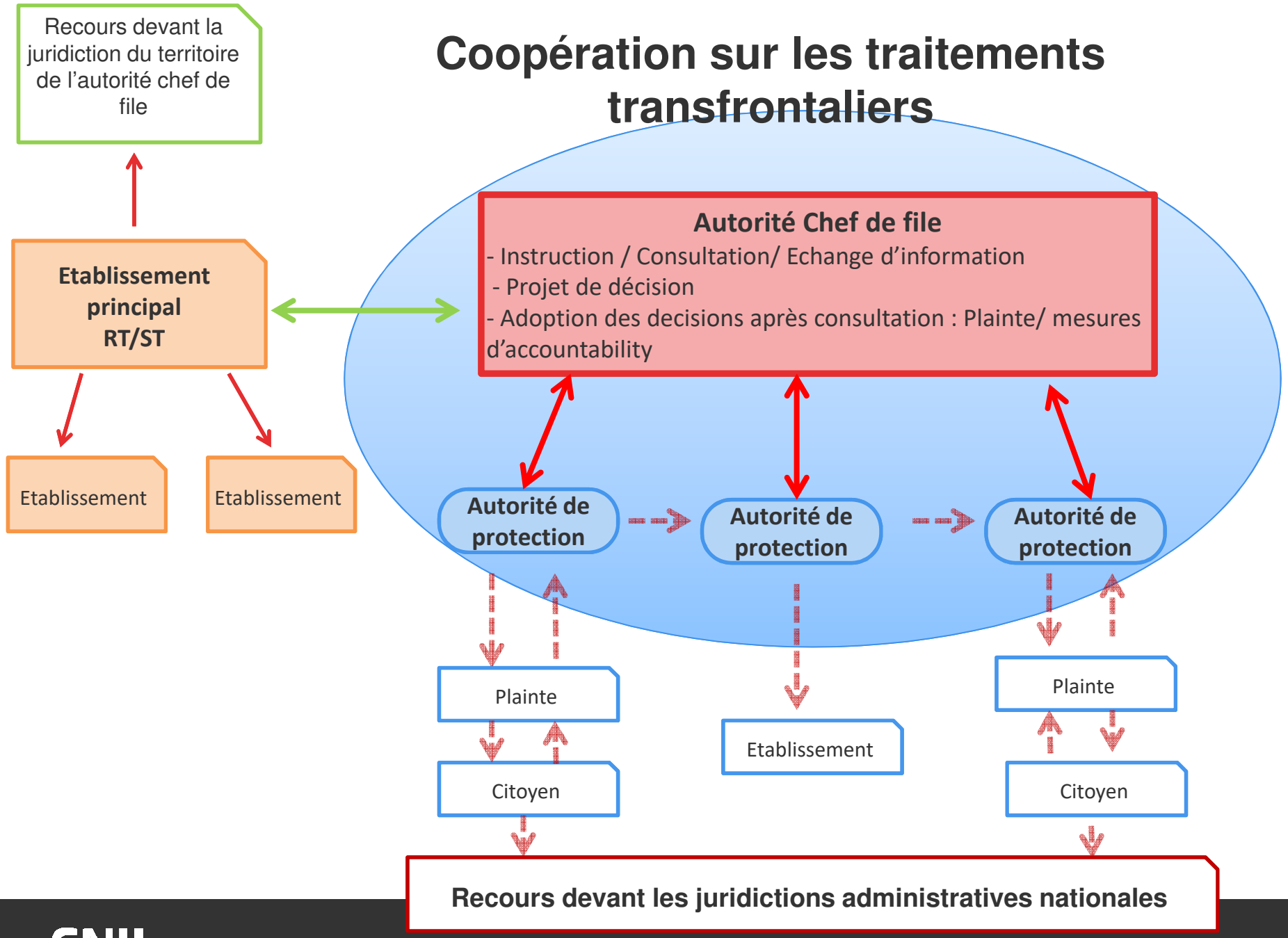
- Le renforcement des droits existants
  - obligation générale de faciliter l'exercice des droits (fourniture d'une information claire, intelligible et aisément accessible)
  - information renforcée (ex. transferts hors de l'UE)
  - droit d'accès précisé (ex. : possibilité d'introduire une réclamation devant une « CNIL »)
  - droit de rectification maintenu
  - droit à l'effacement et à l'oubli numérique confirmé (art 19)
  - clarification de l'expression du consentement (charge de la preuve incombe au RT/non ambigüe)

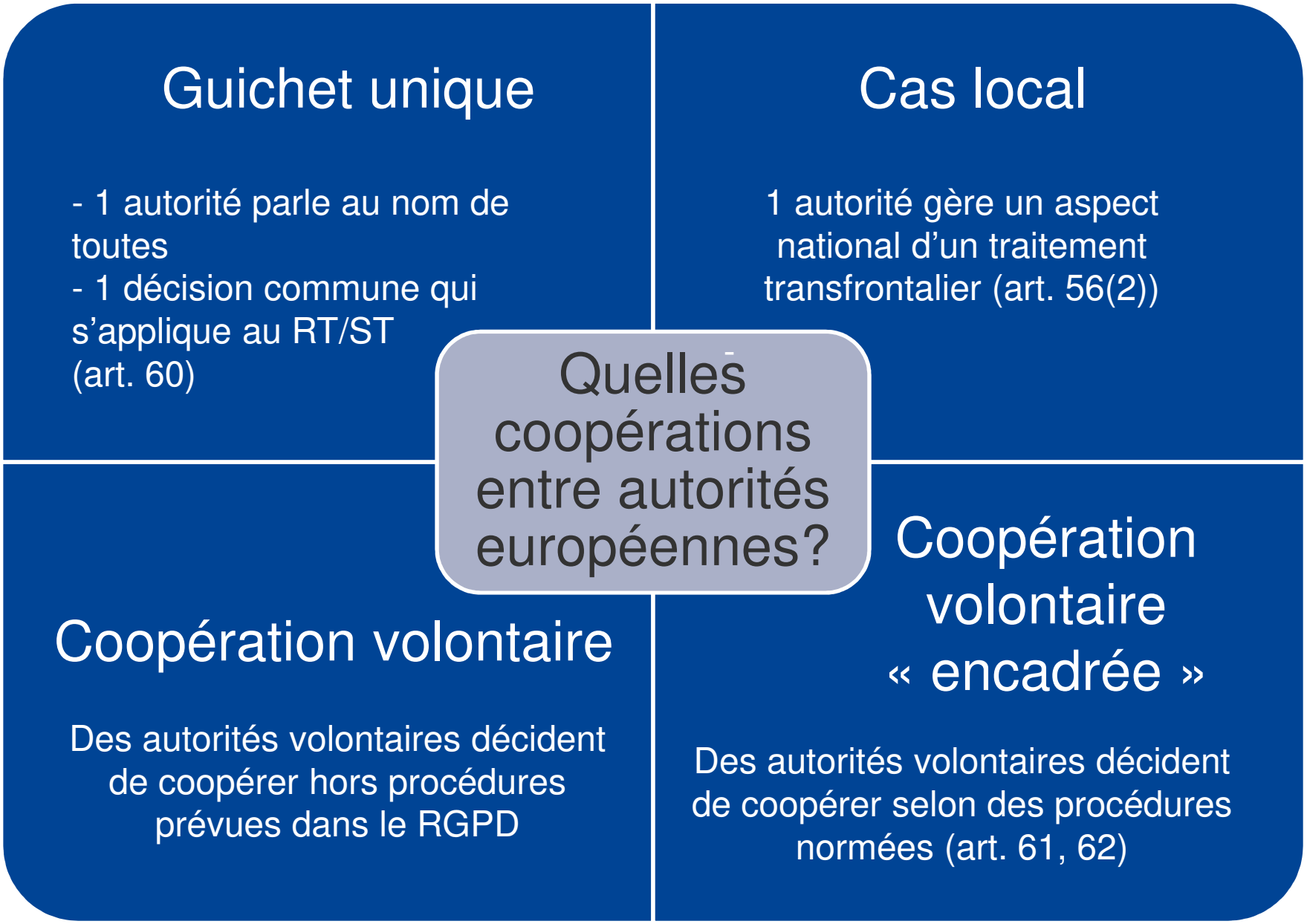
Qu'est ce que le RGPD ?

- De nouveaux droits
  - Portabilité / article 20
  - Limitation du traitement / article 18

- Une plus grande responsabilisation des RT et ST : obligation générale de mettre en place des mesures appropriées et de démontrer leur conformité à tout moment : c'est l' accountability.
  - l'application des principes de privacy by design et privacy by default
  - la conduite d'analyses d'impact
  - la tenue d'un registre des traitements mis en œuvre
  - la notification de failles de sécurité (aux autorités et personnes concernées)
  - la désignation d'un délégué à la protection (obligatoire dans certain cas)
  - la consultation de la CNIL pour certains traitements présentant des risques élevés
  - la certification de traitements et l'adhésion à des codes de conduites

Coopération sur les traitements transfrontaliers




Guichet unique
- 1 autorité parle au nom de toutes
- 1 décision commune qui s'applique au RT/ST (art. 60)
Cas local
1 autorité gère un aspect national d'un traitement transfrontalier (art. 56(2))
Quelles coopérations entre autorités européennes?
Coopération volontaire
Des autorités volontaires décident de coopérer hors procédures prévues dans le RGPD
Coopération volontaire « encadrée »
Des autorités volontaires décident de coopérer selon des procédures normées (art. 61, 62)

La CNIL est chef de file

Cas du guichet unique « classique »

1. La CNIL **coopère** avec les autorités concernées (art. 61 & 62)
2. La CNIL communique **(i)** toutes informations utiles et **(ii)** un projet de décision
3. La CNIL adopte le **projet de décision**
4. La CNIL (i) **notifie** la décision au RT/ST et (ii) **informe** les CSA et l'EDPB

« Cas local » : réclamation dont l'objet concerne exclusivement le territoire d'un autre EM

1. La CNIL informe l'autorité concernée par le cas local
2. La CNIL décide de traiter le cas

2'. La CNIL laisse le cas à l'autorité concernée

3. La CNIL peut recevoir un projet de décision de la part de l'autorité concernée
4. La CNIL gère le cas selon la procédure classique, mais doit tenir compte du projet de décision reçu

La CNIL est concernée

Cas du guichet unique « classique »

1. La CNIL coopère avec les autorités concernées *selon* les demandes de la LSA
2. La CNIL reçoit **(i)** toutes informations utiles et **(ii)** un projet de décision
3. La CNIL formule (ou pas) d'objection pertinente et motivée
4. La CNIL (i) est informée de l'adoption de la décision et (ii) la notifie au plaignant

« Cas local » : réclamation dont l'objet concerne exclusivement le territoire français

1. La CNIL informe la LSA
2. La LSA laisse la CNIL traiter le dossier [sinon procédure d'OSS classique]
3. La CNIL traite le cas avec les procédures articles 61 & 62 [élément(s) d'extranéité]

3'. La CNIL traite seule le cas [aucun élément d'extranéité]

4. La CNIL notifie la personne du résultat

Qui est concerné par le RGPD ?

- Un champs d'application matériel 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 RGPD s'applique :
  - au RT ou au ST sur le territoire de l'Union européenne

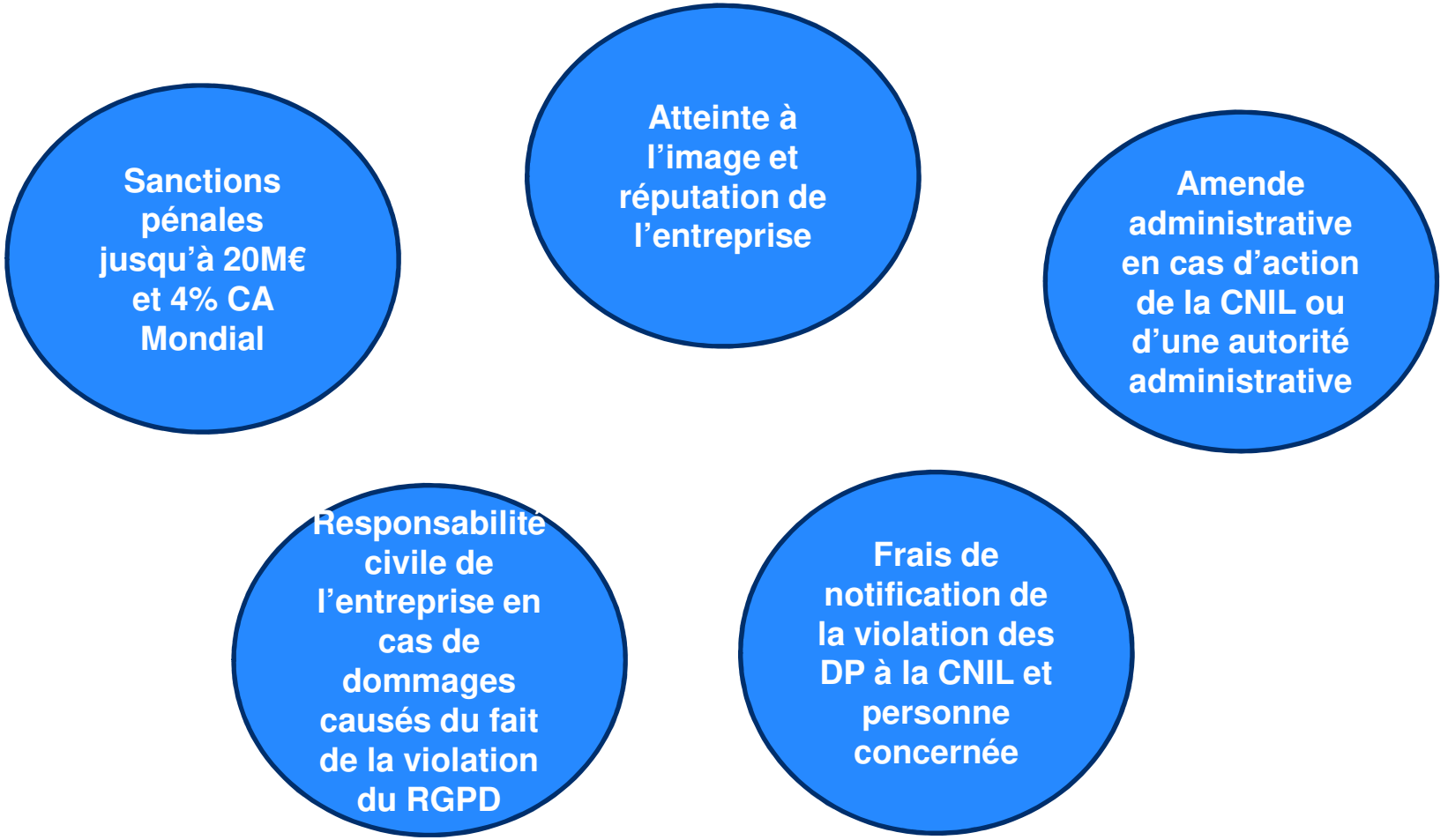
    OU
  - au RT ou ST non établi sur le territoire de l'UE, mais qui met en œuvre des traitements visant
    - à fournir des biens et des services aux résidents européens ou
    - à surveiller leurs comportements

Quelles sont vos obligations au titre du RGPD ?

Mettre en place une organisation adaptée à la taille de votre entreprise et à la sensibilité des données personnelles traitées

- Mettre en place la gouvernance et la désignation d'un DPO (le cas échéant)
- Tenir une documentation permettant de démontrer sa conformité au RGPD
- Protéger les données dans la mise en œuvre de mesures techniques et organisationnelles
- Prendre en compte les enjeux liés à la protection des données dès la phase de conception du produit ou du service par défaut
- Notifier les violations de données auprès de la cnil / personne concernée en cas de risque élevé

Quels sont les risques encourus en cas de violation du RGPD ?



L'analyse d'impacts : PIA

- Qu'est-ce qu'un DPIA ?
  - Un processus permettant de :
    - évaluer la nécessité et la proportionnalité ;
    - gérer les risques sur les droits et libertés.
  - Un outil pour bâtir sa conformité et la démontrer

- Sur quoi un DPIA porte-t-il ?
  - Un traitement ou des traitements identiques mis en œuvre par plusieurs responsables de traitements (RT)
  - Traitements similaires en termes de finalités, fonctionnalités, risques, technologies, etc.

- Quels traitements font l'objet d'un DPIA ?
  - Tous les traitements rencontrant au moins 2 critères (voir slide suivante) : ceux créés après mai 2018 mais aussi ceux créés avant
  - Mise à jour dès qu'ils changent de manière significative
  - Composants des risques : données, supports des données, sources de risques, impacts potentiels, menaces
  - Bonne pratique : mise à jour régulière

Les conditions pour mener un DPIA (2 listes à produire par la CNIL)

- DPIA obligatoire ? Au moins 2 critères
  1. Évaluation/*scoring*
  2. Décision automatique avec effet légal
  3. Surveillance systématique
  4. Données sensibles
  5. Large échelle
  6. Croisement de données
  7. Personnes vulnérables
  8. Usage innovant
  9. exclusion du bénéfice d'un droit/contrat.

- DPIA pas nécessaire ? Art 35.5
  - Pas susceptible d'engendrer des risques élevés
  - DPIA existant sur un traitement similaire
  - Base légale nationale / UE et PIA déjà mené
  - Liste publiable par les DPAs, avec des conditions de mise en œuvre définies, par exemple sur la base des autorisations unitaires et/ou des formalités simplifiées

Quand mener un PIA ? Avant la mise en œuvre du traitement => principe de privicy by design

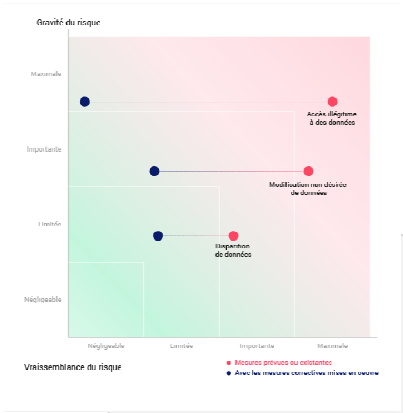
Les parties prenantes du DPIA

- Le responsable de traitement (RT)
  - Le DPIA peut être mené par autrui, mais le RT est responsable
- Le DPO, s'il est désigné
  - Conseil et vérification d'exécution, évaluation des mesures et risques résiduels, développement de bases de connaissances personnalisées
- Les personnes concernées (ou leurs représentants), le cas échéant
  - Leur avis doit être pris et documenté
- Les sous-traitants, s'il y en a
  - Assistance et fourniture d'informations (règles à contractualiser)
- Le métier, si possible
  - Proposition de mener un DPIA, participation au DPIA et à sa validation
- Le responsable de la sécurité des systèmes d'information (RSSI)
  - Évaluation des mesures, proposition de mener un DPIA, assistance
- La direction informatique, si possible
  - Assistance

Les critères d'un bon DPIA / méthode

- Description du traitement
  - Nature, périmètre, contexte et finalités
  - Données, destinataires, durées de conservation
  - Description fonctionnelle
  - Supports de données
  - Codes de conduite à prendre en compte
- Étude juridique
  - Nécessité et la proportionnalité
    - Finalité, loyauté, minimisation, durées de conservation
  - Mesures prévues pour permettre l'exercice des droits
    - Information, droit d'accès, sous-traitants, transferts, etc.
- Étude des risques
  - Sources de risques
  - Impacts potentiels sur les droits et libertés en cas de :
    - accès illégitime ;
    - modification non désirée ;
    - disparition de données.
  - Gravités et vraisemblances
  - Mesures prévues pour traiter les risques
    - Organisation, sécurité logique, sécurité physique, etc.
- Implication des parties prenantes
  - Conseil du DPO
  - Avis des personnes concernées

La démarche



Contexte

- Description fonctionnelle
- Données
- Supports des données
- Etc.

Principes fondamentaux

- Proportionnalité et nécessité
- Mesures protectrices des droits

Risques liés à la sécurité des données

- Mesures existantes ou prévues
- Appréciation des risques

Réitérations possibles (PIA non validé, mise à jour du traitement…)

Validation du PIA

- Évaluation (intégrée aux étapes précédentes)
- Plan d'action (intégré aux étapes précédentes)
- Décision

Juristes

Experts techniques

Focus sur les risques
Quelles sont les mesures de sécurité ? [art. 32]

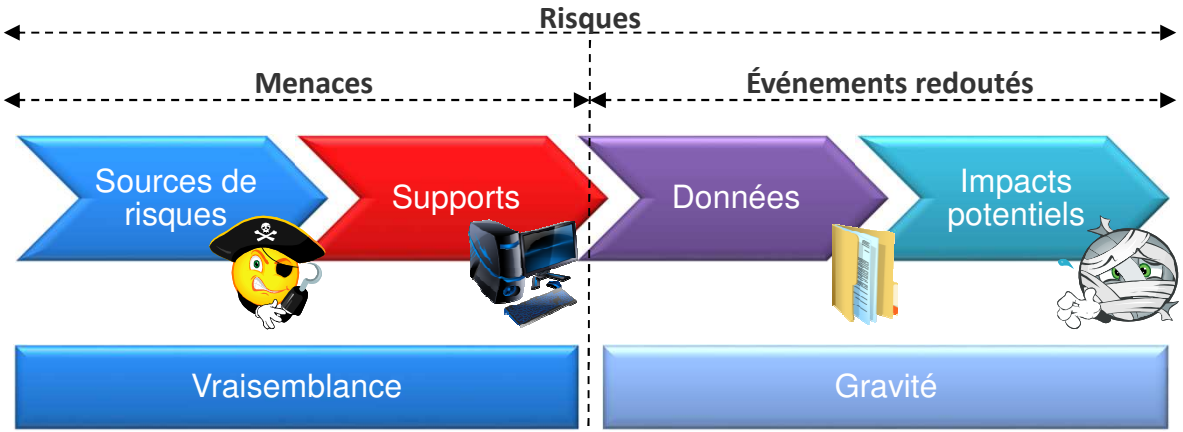
- Mesures sur les données du traitement
  - Chiffrer
  - Anonymiser
  - Cloisonner
  - Contrôler les accès logiques
  - Journaliser
  - Contrôler l'intégrité
  - Archiver
  - Sécuriser les documents papier

- Mesures générales de sécurité
  - Sécuriser l'exploitation
  - Lutter contre les logiciels malveillants
  - Gérer les postes clients
  - Sécuriser les sites web
  - Sauvegarder
  - Maintenance
  - Sécuriser les canaux informatiques
  - Tracer l'activité du système
  - Contrôler l'accès physique
  - Réduire les vulnérabilités des matériels
  - S'éloigner des sources de risques
  - Se protéger des sources de risques non humaines

- Mesures organisationnelles
  - Gérer l'organisation de la protection de la vie privée
  - Gérer la politique de protection de la vie privée
  - Gérer les risques
  - Intégrer la protection de la vie privée dans les projets
  - Gérer les incidents de sécurité et les violations de données
  - Réduire les vulnérabilités du personnel
  - Relations avec les tiers
  - Superviser le protection de la vie privée

Que peut-il arriver aux personnes concernées ?

- Un risque sur la « vie privée » est un scénario décrivant un événement redouté et toutes les menaces qui le rendent possible. Il est estimé en termes de gravité et de vraisemblance



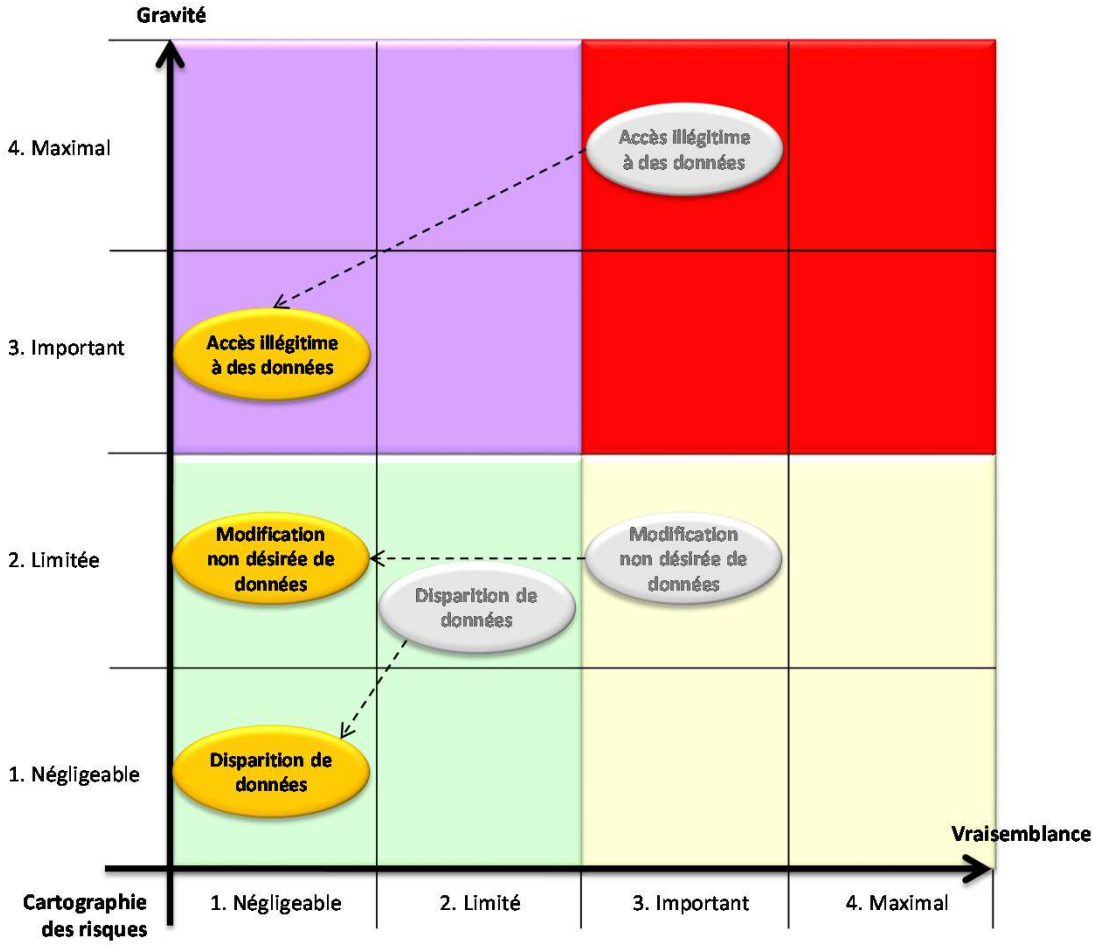
- Sources de risques
  - Personnes externes
  - Personnes internes
  - Sources non humaines
- Supports
  - Matériels
  - Logiciels
  - Réseaux
  - Personnes
  - Supports papier
  - Canaux papier
- Données
  - Données du traitement
  - Données liées aux mesures
- Impacts potentiels
  - Vie privée
  - Identité humaine
  - Droits de l'homme
  - Libertés publiques

Comment les décrire ?

	Accès illégitime à des données	Modification non désirée de données	Disparition de données
Sources de risques			
Impacts potentiels			
Menaces			
Mesures			
Gravité			
Vraisemblance			

- Notes :
  - Les impacts sont ceux sur la vie privée des personnes concernées, et non ceux sur l'organisme
  - Les menaces sont tous les moyens que les risques se concrétisent
  - Les mesures sont celles qui contribuent à traiter le risque parmi celles identifiées
  - La gravité est essentiellement estimée en fonction des impacts potentiels
  - La vraisemblance est essentiellement estimée en fonction des vulnérabilités exploitables

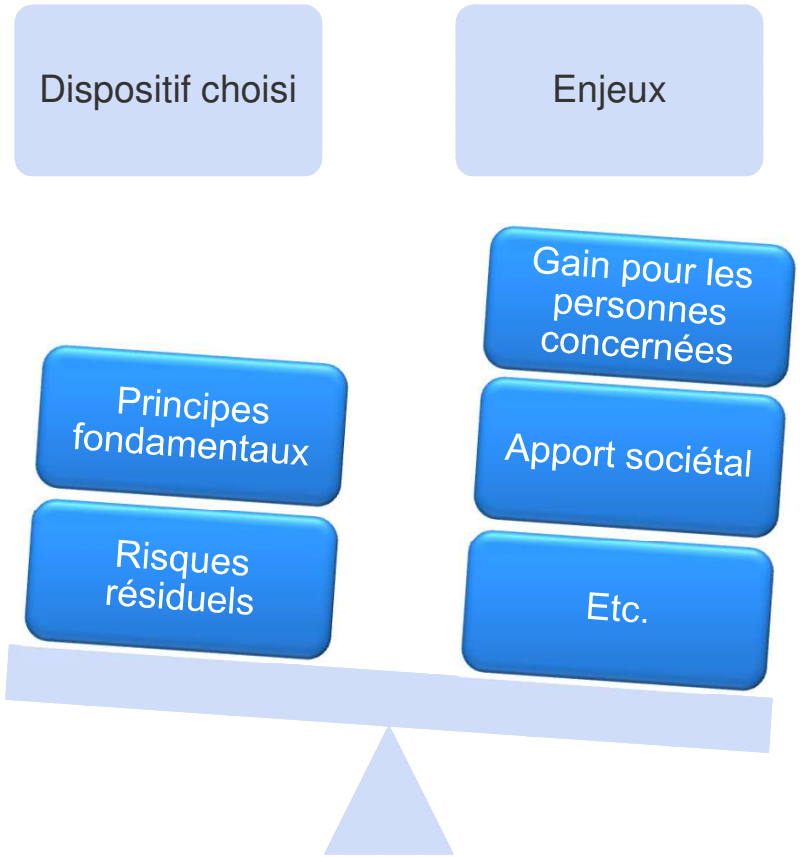
Comment les présenter ?



- Une cartographie des risques permet de comparer visuellement les risques les uns par rapport aux autres

- Elle permet également de faciliter la détermination des objectifs pour les traiter (par « zones »)

Les risques résiduels sont-ils acceptables ?



- Si les mesures prévues (pour respecter les principes fondamentaux et traiter les risques) sont jugées suffisantes et les risques résiduels acceptables, alors le PIA peut être validé par le responsable de traitement

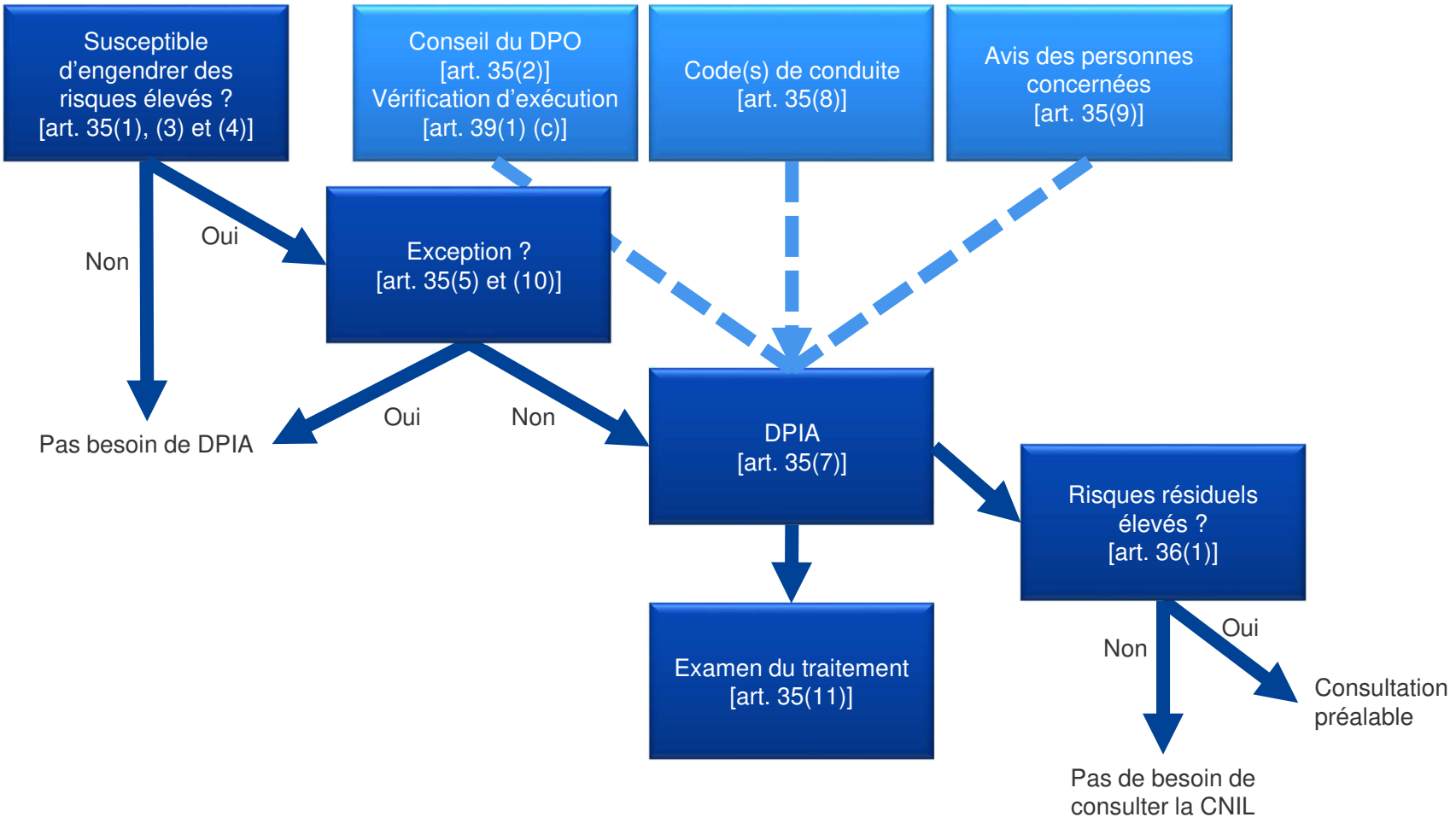
- Sinon, alors il convient d'identifier les objectifs pour y parvenir et de refaire une itération de la démarche

La consultation préalable de la CNIL

- Quand la CNIL doit-elle être consultée ?
  - « *Le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 35 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque* » [art. 36(1)]
  - Le G29 considère que la consultation est obligatoire quand les risques résiduels demeurent élevés

- Un DPIA doit-il être communiqué ?
  - À la CNIL ?
    - Communication obligatoire en cas de consultation préalable
    - Communication potentiellement requise en cas de contrôle
  - Aux personnes intéressées (public, partenaires, personnes concernées) ?
    - Publication ou communication conseillée afin d'apporter de la confiance
    - Tout ou partie du DPIA (on peut exclure des parties compromettantes : risques de sécurité, secrets industriels ou commerciaux, etc.)

La logique générale

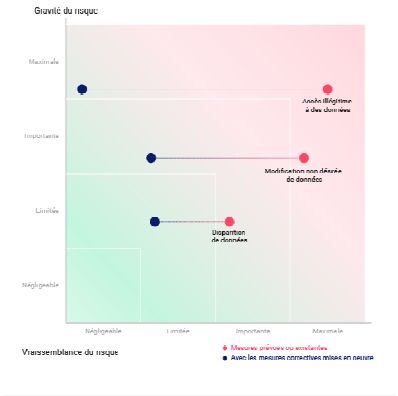


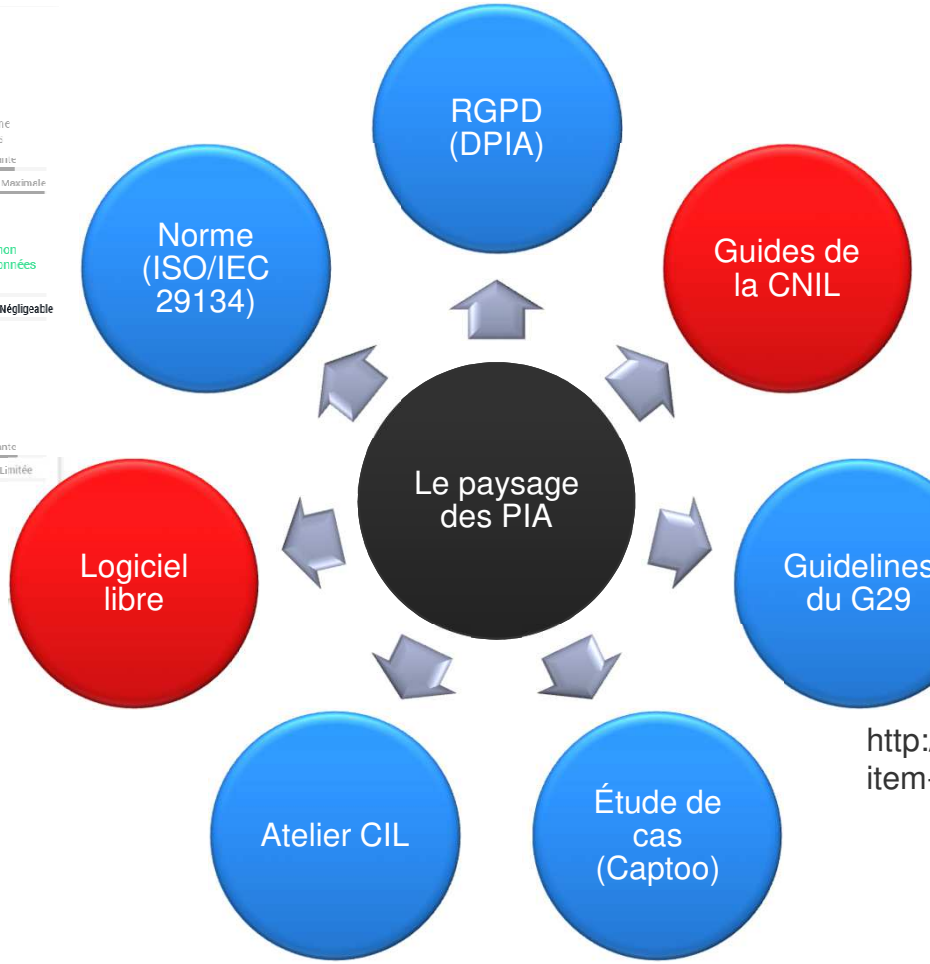
Les sanctions

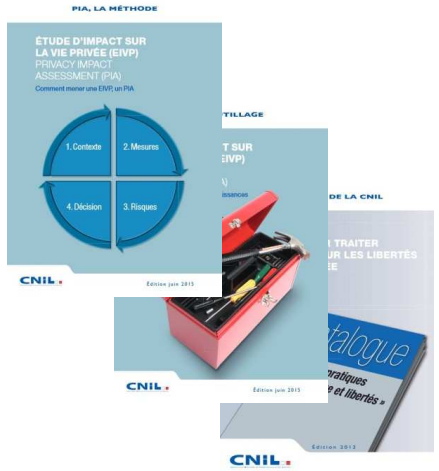
- Que risque-t-on ?
  - « *Amendes administratives pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu* » [art. 83(4)(a)]

- Dans quels cas ?
  - Quand un DPIA n'a pas été mené alors qu'il aurait dû l'être
  - Quand un DPIA n'a pas été correctement mené et documenté
  - Quand la CNIL n'a pas été consultée alors qu'elle aurait dû l'être

Point de situation







http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Les violations de données

Définition au point 12 de l'article 4 du RGPD:

« Une violation de la sécurité entraînant,

- *de manière accidentelle ou illicite,*
- ***la destruction,***
- ***la perte,***
- ***l'altération,***
- ***la divulgation non autorisée***
- *de données à caractère personnel transmises, conservées ou traitées d'une autre manière,*
- *ou* ***l'accès non autorisé*** *à de telles données ».*

Concrètement, quelques exemples

Une violation de sécurité peut être consécutive à :

- une faille ou vulnérabilité de sécurité ;
- un accident (incendie, panne matérielle, séisme, etc.) ;
- une erreur (de saisie, de manipulation, dans la conception de systèmes, etc.) ;
- une malveillance (*phishing*, vol de matériel, fraude externe ou interne, accès frauduleux, manipulation de données, bombe logique, logiciels malveillants, défiguration de sites, etc.).

C'est la concrétisation d'un risque, voire l'illustration du non respect des obligations de sécurité des données (article 32 RGPD).

Exemples : Violations de sécurité rencontrées par le parti socialiste, la société Ricard ou engendrées par le logiciel malveillant *WannaCry* (indisponibilité - *ransomware*).

Les notifications, une continuité pour la CNIL

Avant le RGPD

- Article 34 bis de la loi 78-17 du 6 janvier 1978 modifiée :

Obligation de notification des violations de données personnelles des fournisseurs de service de communications électronique au public, sans condition de risque.

- Préexistence dans d'autres pays (Etats-Unis : 47 Etats dont Californie depuis 2003, Pays-Bas …).

Avec le RGPD (articles 33 et 34)

Obligation pour tous les responsables de traitements, modulée par niveaux de risque.

Objectif

Responsabiliser les acteurs

Protéger les individus des risques qui pèsent sur eux suite à une violation en imposant des mesures

Les acteurs concernés

Le sous traitant

notifie au RT toute violation de données dans les meilleurs délais après en avoir pris connaissance afin de lui permettre de respecter son obligation de notifier, si possible, dans les 72 h

Le responsable du traitement

- documente toute violation de données
- notifie à l'autorité de contrôle la violation

dans les meilleurs délais, et si possible dans les 72 h de la connaissance de la violation

si la violation est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques

- informe les personnes concernées en cas de risque élevé

La personne concernée

reçoit communication de la violation en cas de risque élevé pour ses droits et libertés.

L'autorité de contrôle

- reçoit la notification
- examine les éléments liés à la violation
- conseille le RT sur les mesures à prendre
- peut ordonner au RT de communiquer à la personne concernée la violation de données

Quand faut il notifier à l'autorité de contrôle ?

- Lorsque le RT prend connaissance de la violation,

Cela implique des mesures de détection (mises en œuvre par les RT et ST)

La période d'investigations éventuellement nécessaire pour atteindre un degré de certitude raisonnable doit débuter le plus tôt possible

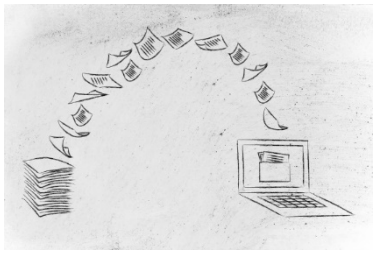
Ex. perte d'une clé USB contenant des données personnelles : le RT est reconnu informé dès lors qu'il réalise la perte

- Sans délai et, dans la mesure du possible, au plus tard dans les 72 heures suivant la découverte de la violation

- Lorsque le RT évalue que la violation est susceptible de créer un risque pour les droits et libertés des personnes au regard de :
  - le type de violation (confidentialité ou disponibilité, par exemple) ;
  - la nature, sensibilité et le volume des données personnelles concernées ;
  - la facilité d'identifier les personnes et des conséquences pour les personnes ;
  - du volume et des caractéristiques de personnes concernées (enfants, personnes vulnérables, etc.) ;
  - les caractéristiques du RT (nature, rôle, activités),

Que faut-il notifier à l'autorité de contrôle ?

Via un téléservice dédié



a minima :

- la nature de la violation ;
- les catégories et le nombre approximatif des personnes concernées ;
- les catégories et le nombre approximatif de fichiers concernés ;
- les coordonnées de la personne à contacter (DPO ou autre) ;
- les conséquences probables de la violation ;
- les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation,

Les informations peuvent être communiquées de manière échelonnée en justification des raisons qui y conduisent

Quand faut-il informer les personnes concernées ?

Dans les meilleurs délais,

Lorsque la violation est susceptible de créer un **risque élevé** pour les droits et libertés des personnes concernées, sauf dans 3 cas:

- le RT a mis en place, préalablement à la violation, des mesures techniques de protection appropriées (par exemple, mesures ayant rendu les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès, de type chiffrement) ; ou
- le RT a mis en place des mesures subséquentes à la violation, permettant d'assurer que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser ; ou
- une telle notification impliquerait un effort disproportionné. Dans ce cas, une information générale sera suffisante.

Que faut-il communiquer aux personnes concernées ?

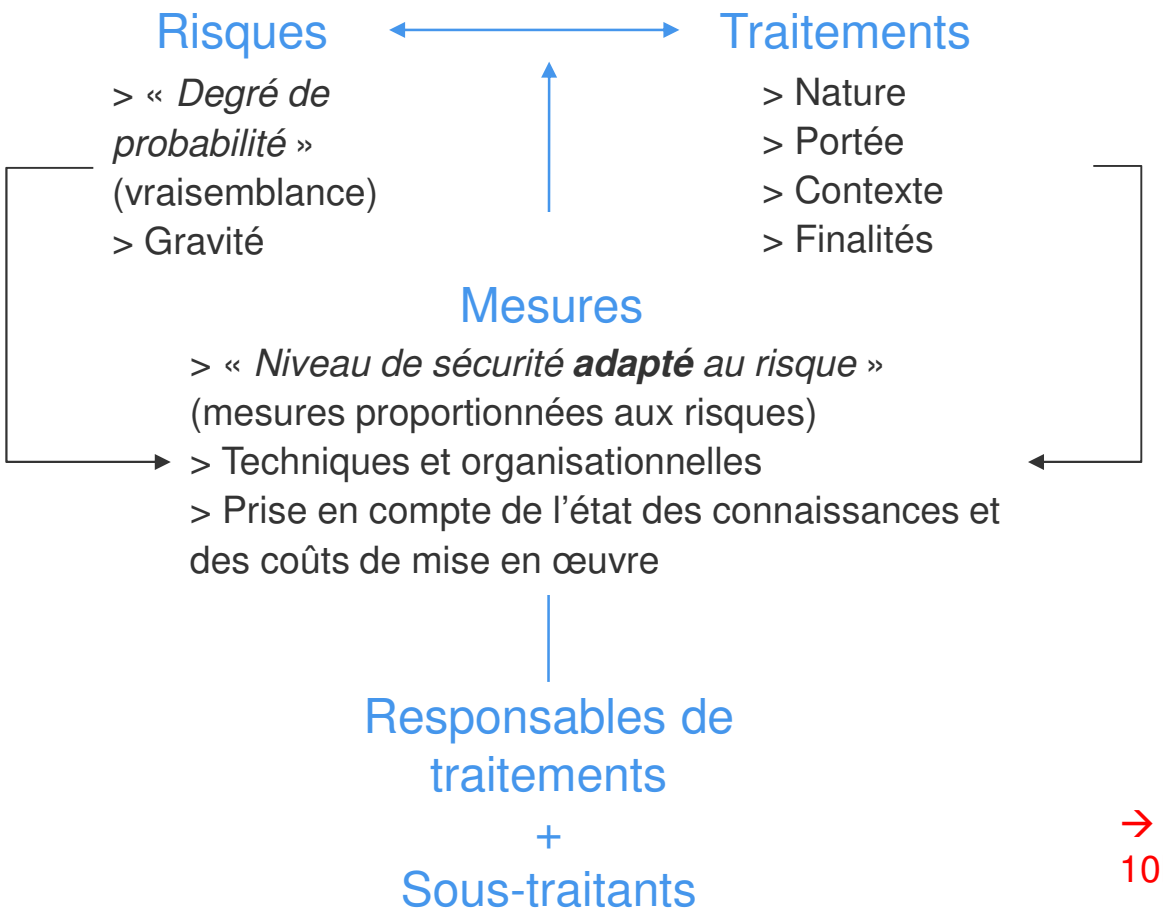
<u>Objectif</u>: informer les personnes pour qu'elles prennent les mesures visant à les protéger (ex. changer de mot de passe)

a minima et en des termes clairs et précis :

- la nature de la violation ;
- les coordonnées de la personne à contacter ;
- les conséquences potentielles de la violation, et
- les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation

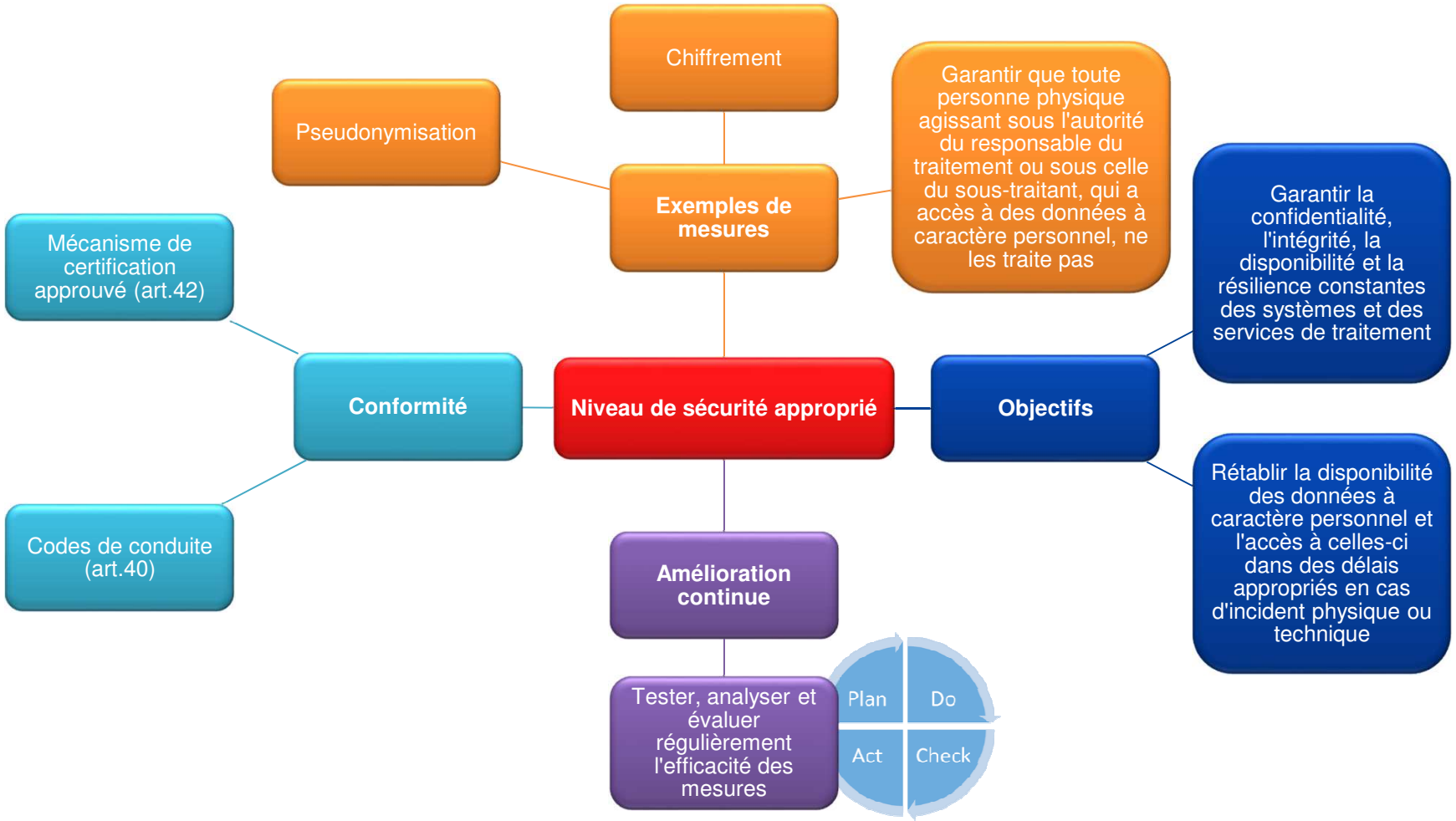
→ La CNIL pourra exiger du RT qu'il informe les personnes concernées ou prenne d'autres mesures protectrices le cas échéant

La sécurité du traitement : article 32

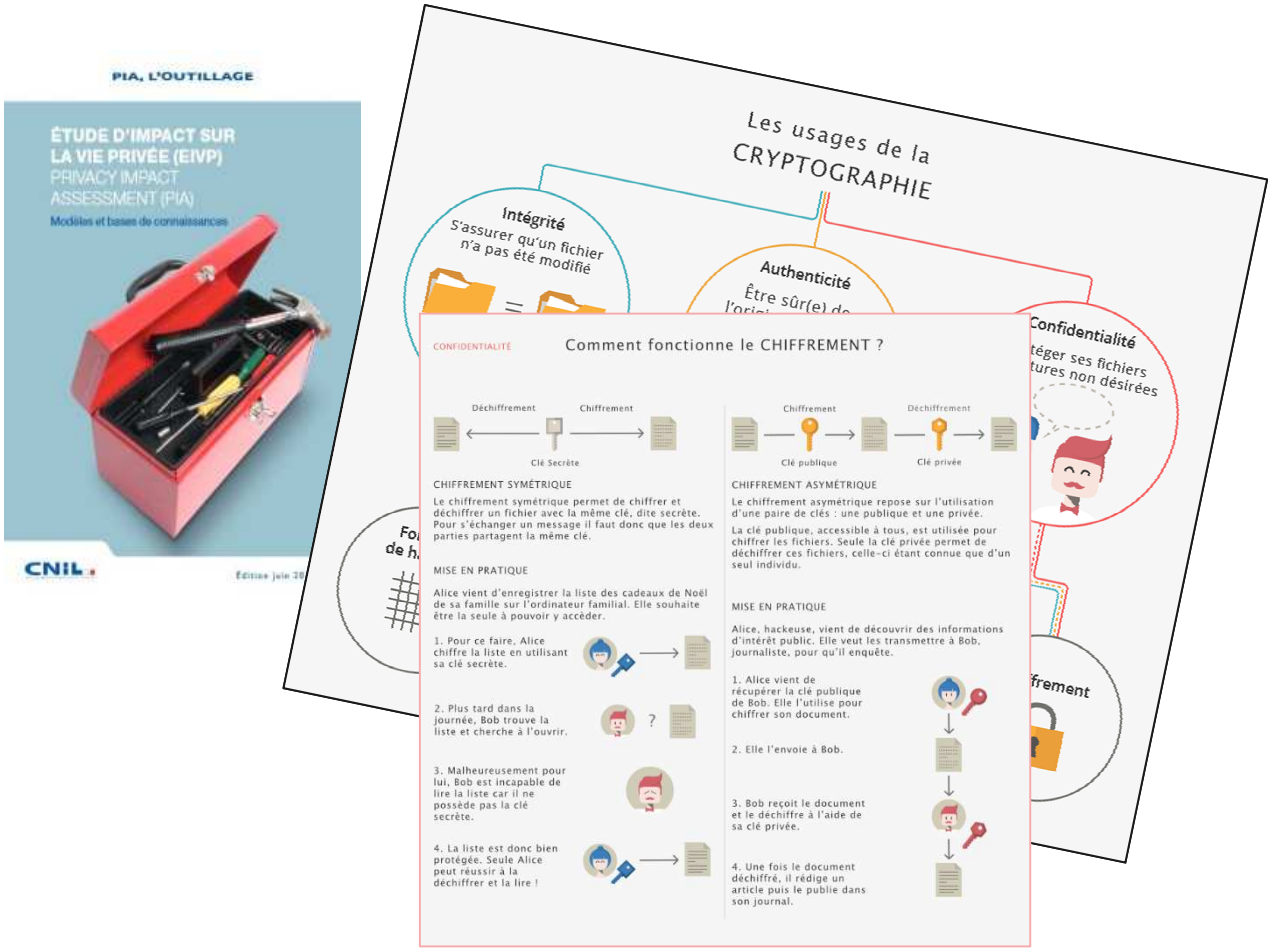


→ Sanction :
10M€ ou 2€ du CA

Niveau de sécurité approprié : principes directeurs



Pour vous aider : des guides, des communications et des recommandations de la CNIL



- Mot de passe seul (ex : *webmail*)
  - Au moins 12 caractères
  - Majuscules, minuscules, chiffres et caractères spéciaux
- Mot de passe et blocage (ex : site de e-commerce)
  - Au moins 8 caractères
  - 3 catégories parmi majuscules, minuscules, chiffres et caractères spéciaux
  - Restriction (temporisation, captcha, blocage) au bout de 10 tentatives échouées

Les nouvelles responsabilités
Logique de responsabilisation de tous les acteurs

- Axe central du RGPD
  - Rééquilibrage des situations juridiques des RT et ST
  - Obligations « égalisées » et responsabilité susceptible d'être conjointement engagée

- Obligations partagées de mise en conformité dynamique (« accountability »)
  - Application des principes de protection des données dès la conception et par défaut
  - 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, tenue d'un registre des activités de traitement, réalisation d'analyses d'impact, etc.

Les nouvelles responsabilités

Responsabilité conjointe des RT / Responsabilité spécifique des ST

- **Pas d'évolution dans la définition du RT mais (ré)introduction de la notion de « responsables conjoints du traitement »**
  - lorsque plusieurs organismes déterminent ensemble les finalités et moyens d'un seul et même traitement
  - 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
  - les personnes concernées pourront exercer leurs droits à l'égard et à l'encontre de chacun d'entre eux
- **Définition du cadre contractuel régissant les relations RT/ST et élargissement du champ de ses obligations**
  - Obligation de s'en tenir aux instructions *documentées* du RT et de prendre toutes les mesures de sécurité requises
  - Respect de conditions pour la « sous-sous-traitance »
  - Soutien du RT dans le respect de ses diverses obligations et devoir d'alerte
  - Obligation de désigner un délégué dans certains cas et de tenir un registre des catégories de traitements effectués pour le compte du RT
- **Introduction d'une responsabilité propre au ST**

Le délégué à la protection des données (DPD)

Désignation obligatoire pour les RT/ST :

1. Pour toute **autorité publique** ou tout **organisme public** (collectivités territoriales, Etat, établissements publics, etc.), quel que soit la nature du traitement

2. Si les **activités de base** de l'organisme consistent en des traitements qui exigent un **suivi régulier et systématique à grande échelle des personnes concernées**

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

Désignation volontaire encouragée par le G29

Mutualisation et externalisation

- **Mutualisation possible : flexibilité laissée aux organismes**
  - Dans le secteur privé : 1 même délégué pour un groupe d'entreprises 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* »

- **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

Le délégué à la protection des données (DPD)

Qui peut être délégué ?

- **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* »

- **Absence de conflit d'intérêts**
  - Le délégué ne peut occuper une fonction au sein de l'organisme qui le conduit à déterminer finalités et moyens d'un traitement
  - Appréciation au cas par cas

Les missions du délégué

- **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,…)
- Dispense des **conseils** en ce qui concerne **l'analyse d'impact** relative à la protection des donnée et **vérifie son exécution**
- **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
- S'assure de la **bonne tenue de la documentation** relative aux traitements

Le délégué à la protection des données (DPD) et le registre des activités de traitement

Les moyens du délégué

Des moyens et ressources à obtenir 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
- Doit disposer des ressources nécessaires à l'exécution de ses missions (notamment accès aux données et aux traitements) et au maintien de ses connaissances
- Fait directement rapport au niveau le plus élevé de l'organisme
- Indépendance dans l'accomplissement de ses missions
- Pas de sanction du fait de l'accomplissement de ses missions

Art 30 : le registre des activités de traitement (à partir de 250 employés)

Une obligation qui s'étend à tous les RT (avec ou sans DPO) et aux ST . Le contenu du registre :

- nom et les coordonnées du RT, DPO, ST
- finalités du traitement ou catégories de traitements effectués pour le compte du RT
- catégories personnes concernées et les catégories de données
- catégories de destinataires
- dans la mesure du possible, les délais prévus pour l'effacement
- 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

Pour chaque traitement de données personnelles, posez-vous les questions suivantes :

QUI ?
- Identifiez les responsables des services opérationnels traitant des données
- Etablissez la liste des ST

QUOI ?
- Identifiez les catégories de données traitées
- Identifiiez les données susceptibles de soulever des risques ou en raison de leur sensibilité

POURQUOI ?
Indiquez la ou les finalités pour lesquelles vous collectez ces données

OU ?
- Déterminez les lieux où sont stockées les données
- Indiquez le pays vers lesquels les données sont éventuellement transférées

COMBIEN DE TEMPS ?
Indiquez la durée de conservation des données

COMMENT ?
Précisez les mesures de sécurité mises en œuvre pour minimiser les risques

CNIL.

Des questions ?

Merci de votre attention

Isabelle SANSOT
Juriste au Service des Affaires Economiques

isansot@cnil.fr