Janvier 2026

Parcours PASI – Piloter animer la sécurité informatique

V.1.0

Module 1 – Fondamentaux techniques et règlementaires

Règlementation (RGPD, ISO, conformité)

Séquence 1 : Introduction au RGPD

Guillaume Carayon
Consultant senior cybersécurité

Présentation de la séquence
Objectifs et notions abordées

Comprendre les fondements juridiques de la protection des données personnelles

- Le cadre historique et institutionnel de la protection des données personnelles
- Le vocabulaire du RGPD
- Les principes associés à un traitement de données personnelles
- L'exercice du droit des personnes
- Les mesures de sécurité pour les données personnelles
- La gouvernance des organisations relatives au RGPD

Cadre historique et institutionnel de la protection des données personnelles

Cadre historique et institutionnel de la protection des données personnelles
De LIL au RGPD


• • • LE MONDE — 21 mars 1974 — Page 9

JUSTICE

Tandis que le ministère de l'intérieur développe la centralisation de ses renseignements

Une division de l'informatique est créée à la chancellerie

« Safari » ou la chasse aux Français

Révélations du journal Le Monde

Directive européenne 95/46/CE portant sur la protection des données

Règlement Général sur la Protection des Données

1973 — Projet SAFARI

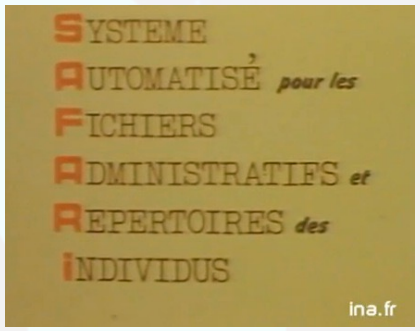
1974

1978 — Loi et Commission Nationale « Informatique et Libertés »

1995

2013 — Révélations d'Edward Snowden

2016

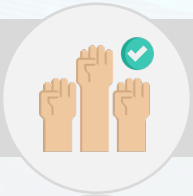


CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

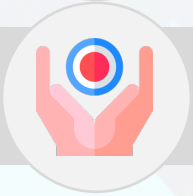
Cadre historique et institutionnel de la protection des données personnelles
De LIL au RGPD

Le Règlement Général sur la Protection des Données est un règlement européen encadrant le traitement des données à caractère personnel des personnes physiques, et à la libre circulation de ces données. Il est entré en application le 25 mai 2018.

Il a pour objectif de :



Renforcer le droit des personnes sur leurs données personnelles



Responsabiliser les acteurs qui traitent des données à caractère personnel

Crédibiliser la régulation par la coopération des autorités de protection des données

Cadre historique et institutionnel de la protection des données personnelles
De LIL au RGPD

Toute organisation, publique ou privée qui traite des données personnelles pour son compte (responsable de traitement) ou non (sous-traitant).

Dès lors qu'**elle est établie sur le territoire de l'Union européenne**, ou que son activité **cible directement des résidents européens**.

Peu importe la taille, le pays d'implantation et l'activité

Cadre historique et institutionnel de la protection des données personnelles

Le développement des institutions : la CNIL

Commission Nationale Informatique et Libertés (CNIL)

Autorité administrative indépendante chargée de réguler l'utilisation des données personnelles

- Informe et protège les droits
- Accompagne la conformité et conseille les entreprises
- Anticipe et innove les pratiques en matière de données personnelles
- Contrôle et sanctionne les manquements

Cadre historique et institutionnel de la protection des données personnelles

Le développement des institutions : le CEPD

Comité Européen de la Protection des Données (CEPD)

Coordonne l'action des CNIL européennes au moyen d'avis et de décision

- Publie des lignes directrices sur l'interprétation des concepts fondamentaux du RGPD
- Se prononce sur les litiges concernant les activités de traitement transfrontaliers
- Donne son avis sur les projets de décisions des CNIL européennes

Cadre historique et institutionnel de la protection des données personnelles

Les sanctions prévues par le RGPD

Le montant de la sanction dépendra notamment du type de manquement constaté

10M€ ou 2% C.A. monde

- Absence de **protection des données dès la conception** et de **protection des données par défaut**
- Absence de **représentant établi dans l'Union européenne**
- Absence de **registre des activités de traitement**
- Absence de **coopération** avec l'autorité de contrôle
- Absence de **notification** à l'autorité de contrôle ou à la personne concernée d'une **violation de données**
- Absence **d'analyse d'impact**

20M€ ou 4% C.A. monde

- Non-respect des **principes de bases** d'un traitement (licéité, loyauté, légitimité, adéquation et pertinence des données, consentement, données sensibles, etc.)
- Non-respect des **droits des personnes**
- Non-respect des règles relatives aux **transferts de données** à caractère personnel

Elle prend aussi en compte d'autres paramètres : bonne volonté de l'organisme à se mettre en conformité, à répondre aux attentes de la CNIL, volume de personnes concernées par les manquements, etc.

Cadre historique et institutionnel de la protection des données personnelles

Les sanctions pénales

Source : Haas-Avocats

Au-delà des sanctions administratives, il existe aussi des sanctions pénales

Infraction	Textes	Peines
Non-respect des **formalités préalables**	Art. 226-16 du Code Pénal	300.000 € d'amende 5 ans d'emprisonnement
Non-respect relatif à **l'obligation de sécurité**	Art. 226-17 et 226-17-1 du Code Pénal	
Détournement de la finalité du traitement de données personnelles	Art. 226-21 du Code Pénal	
Procéder à un **transfert de données transfrontière** contrevenant aux mesures prises par la Commission des Communautés européennes	Art. 226-22-1 du Code Pénal	
Absence d'information des personnes concernées	Art. R. 625-10 du Code Pénal	1.500 € d'amende par infraction constatée
Non-respect des **droits des personnes**	Art. R. 625-11 du Code Pénal	

Principes généraux et terminologie

Principes généraux et terminologie
La définition d'une donnée à caractère personnel

Article 4 du RGPD
Article 2 de la LIL

Définition générale

« Toute information se rapportant à une personne physique identifiée ou **identifiable** »

« identifiable »

« La personne physique peut être **identifiée, directement ou indirectement**, notamment par référence à un identifiant (...) »

- Identification directe
- Identification indirecte

L'adresse IP dynamique peut-elle être considérée comme une donnée à caractère personnel ?

Principes généraux et terminologie
La définition d'une donnée à caractère personnel

Les données à caractère personnel concernent aussi bien la vie personnelle que professionnelle, peu importe le moyen de captation

Les données des personnes morales ne sont pas des données à caractère personnel, mais les données relatives aux dirigeants et aux associés sont des données à caractère personnel

Les données à caractère personnel des personnes décédées n'entrent pas dans le champ d'application des lois concernant la protection des données personnelles

Principes généraux et terminologie
Les données sensibles

Article 9 du RGPD
Article 6 de la LIL

Les données sensibles sont des données dont le traitement peut présenter un risque pour les droits et libertés fondamentaux et bénéficient d'un régime dérogatoire (interdiction de traitement par défaut)

- Origine raciale ou ethnique
- Opinions politiques
- Convictions religieuses ou philosophiques
- Appartenance syndicale
- Données génétiques
- Données biométriques
- Données de santé
- Vie sexuelle ou orientation sexuelle

Principes généraux et terminologie

Les DCP spéciales : le NIR et les informations policières / judiciaires

Le NIR (ou numéro de sécurité sociale)

Données relatives aux infractions, condamnations pénales et mesures de sûreté connexes

Principes généraux et terminologie
Le traitement de données à caractère personnel

Est un traitement **toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à ces données** ou des ensembles de données à caractère personnel

RGPD, article 4

Type de traitement de données à caractère personnel présenté dans le RGPD

- Collecte
- Enregistrement
- Organisation
- Conservation
- Adaptation
- Modification
- Extraction
- Consultation
- Utilisation
- Communication par transmission ou diffusion
- Mise à disposition
- Rapprochement

Les principes associés à un traitement de données personnelles

Les principes associés à un traitement de données personnelles

Les conditions du traitement et les obligations des acteurs du traitement

Principes liés au traitement

- Finalités déterminées, explicites et légitimes
- Licéité qui repose sur une des six bases légales du RGPD
- Loyauté du traitement
- Transparence du traitement

Principes liés aux données

- Minimisation et proportionnalité des données
- Exactitude des données
- Conservation des données pour une durée déterminée
- Sécurité et confidentialité

Les principes associés à un traitement de données personnelles

Les finalités déterminées, explicites et légitimes

Une finalité correspond à un but bien précis, légal et légitime.

- La finalité doit être déterminée, explicite et légitime
- Elle permet d'identifier :
  - Les données personnelles traitées
  - Leurs durées de conservation
  - La liste des personnes habilitées à y accéder

Les principes associés à un traitement de données personnelles

Les fondements de la licéité d'un traitement

La finalité du traitement doit reposer sur une base légale

- La personne a **consenti** au traitement de ses données
- Le traitement est nécessaire à **l'exécution ou à la préparation d'un contrat** avec la personne concernée
- Le traitement est **imposé par des textes légaux**
- Le traitement est nécessaire à l'exécution d'une **mission d'intérêt public**
- Le traitement est nécessaire à la poursuite d'**intérêts légitimes** de l'organisme
- Le traitement est nécessaire à **la sauvegarde des intérêts vitaux** de la personne concernée ou d'un tiers

Les principes associés à un traitement de données personnelles

Les fondements de la licéité d'un traitement : le cas de l'intérêt légitime

La personne concernée peut-elle raisonnablement s'attendre à ce que ses données fassent l'objet d'un traitement à une fin spécifique ?

Intérêts poursuivis par le responsable de traitement

Droits de la personne concernée et ses propres intérêts

Les principes associés à un traitement de données personnelles
La minimisation des données

- Ce principe signifie que les données collectées doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées » (RGPD, article 5-1).

- La collecte de données personnelles doit être limitée aux seules données nécessaires. Elle doit justifier de son caractère nécessaire et proportionné.

    - Ne pas collecter des données « au cas où » ➔ la réutilisation de données pour d'autres finalités est interdite
    - Mettre en pratique le principe de minimisation ➔ par exemple, si je collecte la nationalité, je privilégierai « Français / UE / hors UE »
    - Être vigilant avec les zones de commentaires libres

Les principes associés à un traitement de données personnelles

La minimisation des données

Quel est mon objectif ?

Quelles données sont indispensables pour atteindre cet objectif ?

Ai-je le droit de collecter ces données ?

Ai-je bien distingué les données obligatoires des données facultatives ?

Les principes associés à un traitement de données personnelles
L'exactitude des données

Les données personnelles doivent être « exactes et, si nécessaire, tenues à jour »

Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder »

RGPD, article 5-1.d

Les principes associés à un traitement de données personnelles
La durée de conservation

Le cycle de vie d'une donnée : de la base active à l'archivage définitif

Base active (ou archive courante)

Commence à la création du document et dure tant que ce dernier est utilisé quasi-quotidiennement par le service qui l'a produit.

Archivage intermédiaire

Commence quand le document n'a plus d'usage fréquent mais qu'il peut être nécessaire pour faire face à des recours, à d'éventuels délais de prescription

DUA : Durée d'Utilité Administrative

Archivage définitif

Certaines archives peuvent être conservées au-delà de leur DUA. Il s'agit des documents qui présentent un intérêt historique, scientifique, statistique ou public permanent, et qui doivent être conservés indéfiniment pour la connaissance de notre société par nos descendants

Les principes associés à un traitement de données personnelles
La durée de conservation

Les données doivent être conservées pour une durée déterminée, limitée au strict minimum

Dispositions légales ou réglementaires	Certains textes imposent une durée minimale de conservation
Délibérations de la CNIL	Référentiels sectoriels de durées, « cadres de référence » de la CNIL
Références sectorielles	Les codes de conduite…
Finalités du traitement	Si aucun des éléments précédents ne permettent de définir la durée de conservation

Principes associés aux droits des personnes

Principes associés aux droits des personnes
Généralités

Quels sont les droits que les personnes peuvent exercer concernant leurs données personnelles ?

Les droits renforcés

- Le droit d'accès
- Le droit de rectification
- Le droit d'opposition
- Le droit à l'effacement

Les nouveaux droits

- Le droit à la portabilité
- Le droit à la limitation du traitement
- Le droit concernant la décision individuelle automatisée

Principes associés aux droits des personnes
Généralités

	DROIT D'ACCÈS	DROIT DE RECTIFICATION	DROIT À L'EFFACEMENT	DROIT À LA LIMITATION DU TRAITEMENT	DROIT À LA PORTABILITÉ	DROIT D'OPPOSITION
Consentement	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Retrait du consentement**
Contrat	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Non**
Intérêt légitime	**Oui**	**Oui**	**Oui**	**Oui**	**Non**	**Oui**
Obligation légale	**Oui**	**Oui**	**Non**	**Oui**	**Non**	**Non**
Intérêt public	**Oui**	**Oui**	**Non**	**Oui**	**Non**	**Oui**
Intérêts vitaux	**Oui**	**Oui**	**Oui**	**Oui**	**Non**	**Non**

Principes associés aux droits des personnes
L'information des personnes

Les informations doivent être communiquées « d'une façon **concise, transparente, compréhensible et aisément accessible**, en **termes clairs et simples**, en particulier pour toute information destinée spécifiquement à un enfant »

RGPD, article 12.1

Principes associés aux droits des personnes
L'information des personnes

Les personnes concernées doivent être informées de manière simple, claire et complète de l'ensemble des informations visées par les dispositions de l'article 13 du RGPD

Que doivent contenir les mentions d'information ?

- L'identité et les coordonnées de l'organisme collecteur responsable du traitement de données
- Les coordonnées du délégué à la protection des données désigné
- Les finalités du traitement et la base juridique associé. Dans le cas d'un traitement reposant sur l'intérêt légitime, précisez lesquels
- Les destinataires des données personnelles
- La durée de conservation
- Les droits des personnes concernées et la possibilité de référer à la CNIL en cas de problème

Principes associés aux droits des personnes

L'information des personnes

La forme de l'information est importante pour s'assurer de respecter les exigences du RGPD

Compréhensible

Format lisible

Accessible

Global

L'information doit être claire, précise et simple :

- Utiliser un vocabulaire simple, faire des phrases courtes et employer un style direct
- Adapter l'information au public visé

Principes associés aux droits des personnes
L'information des personnes

La forme de l'information est importante pour s'assurer de respecter les exigences du RGPD

Compréhensible

Format lisible

Accessible

Global

- Être concis
- Prioriser les éléments d'information
- Adapter la fourniture d'informations aux situations et aux supports

Principes associés aux droits des personnes
L'information des personnes

La forme de l'information est importante pour s'assurer de respecter les exigences du RGPD

Compréhensible

Format lisible

Accessible

Global

Les personnes ne doivent pas avoir à chercher l'information

Principes associés aux droits des personnes

L'information des personnes

La forme de l'information est importante pour s'assurer de respecter les exigences du RGPD

- Compréhensible
- Format lisible
- Accessible
- **Global**

Centraliser les informations si plusieurs modalités d'information sont utilisées par l'organisme

Principes associés aux droits des personnes
Le consentement (art. 4-11 du RGPD)

Lors du recueil du consentement, la demande doit être présentée sous une forme compréhensible et aisément accessible, formulées en des termes simples et clairs. Le consentement doit respecter 4 critères

Libre | **Spécifique** | **Eclairé** | **Univoque**

Il est important de distinguer le consentement comme base légale, du consentement comme exception pour recueillir des données sensibles.

Le choix du consentement comme base légal ne semble pas approprié pour les traitement du milieu médico-social en raison de la potentielle vulnérabilité des personnes concernées.

Principes associés aux droits des personnes
Le consentement (art. 4-11 du RGPD)

Le consentement des mineurs

Le RGPD prévoit des conditions particulières de consentement pour les mineurs dans le cadre des services de la société de l'information

« Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel » *(considérant 38 du RGPD)*

15 ans ou plus

- Les enfants de 15 ans ou plus peuvent consentir eux-mêmes au traitement de leurs données fondés sur le consentement

Moins de 15 ans

- La loi « Informatique et Libertés » impose le recueil du consentement conjoint de l'enfant et du titulaire de l'autorité parentale

Le consentement du titulaire de la responsabilité parentale n'est pas nécessaire dans le cadre de services de prévention ou de conseil proposés directement à un enfant.

Principes associés aux droits des personnes
Le consentement (art. 4-11 du RGPD)

La preuve du consentement

Les responsables de traitement doivent documenter les conditions de recueil du consentement

« Dans les cas ou le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.»
(article 7.1 du RGPD)

La documentation doit permettre de démontrer :

- La mise en place de mécanismes de consentement non contraints ou non liés à la réalisation d'une autre finalité d'un contrat
- La séparation claire et intelligible des différentes finalités de traitement
- La bonne information des personnes
- Le caractère positif de l'expression du choix de la personne

Pour conserver ces preuves, le responsable de traitement peut tenir un registre des consentements

Mesures de sécurité pour les données personnelles

Mesures de sécurité pour les données personnelles

Les principes généraux concernant la sécurité des données personnelles

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, **le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque**, y compris entre autres, selon les besoins:

a) la pseudonymisation et le chiffrement des données à caractère personnel;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

RGPD, article 32-1

Mesures de sécurité pour les données personnelles

Les principes généraux concernant la sécurité des données personnelles

Les risques et les sources de risques sont multiples pour les organismes et varient en fonction des contextes

Nature	Origine	Dimension
• Erreur humaine • Intentionnelle • Catastrophe • Sinistre	• Externe • Interne	• Masse • Ciblée

Risques	Accès non autorisés	Modifications injustifiées	Inaccessibilité des données

Mesures de sécurité pour les données personnelles

Les principes généraux concernant la sécurité des données personnelles

Deux méthodes préconisées par le RGPD

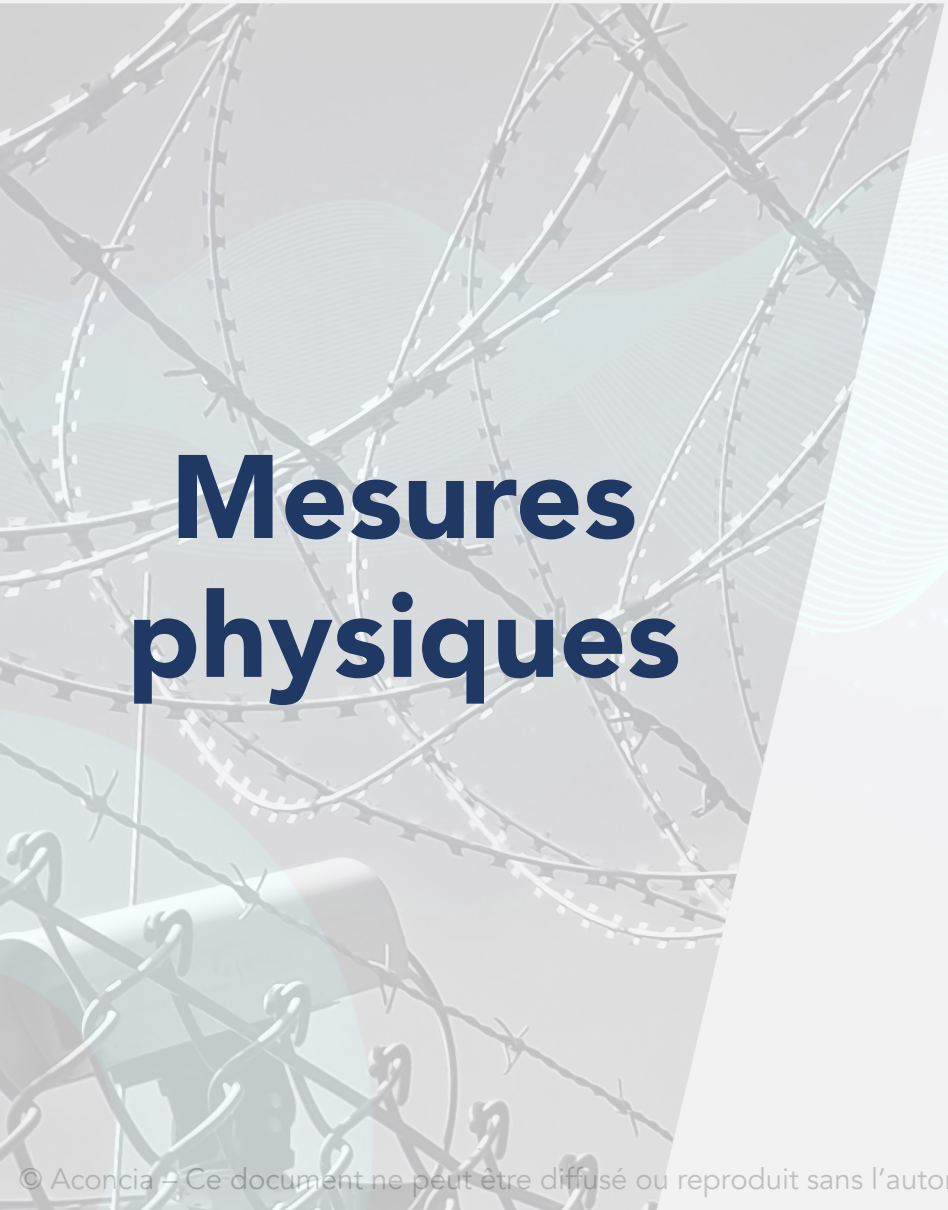
Chiffrement

Pseudonymisation

Ces méthodes ne sont pas imposées et ne sont pas exhaustives et ne sont pas imposées par défaut. L'organisme doit apprécier les mesures à mettre en œuvre d'un point de vue physique, logique ou organisationnel

Mesures de sécurité pour les données personnelles

Quelques exemples de mesures de sécurité



Mesures physiques

Sécuriser l'accès physique aux locaux et notamment aux salles hébergeant les serveurs informatiques et les éléments du réseau

- Installer des alarmes anti-intrusion et les vérifier régulièrement
- Distinguer les zones des bâtiments selon les risques
- Protéger le matériel informatique par des moyens spécifiques
- Installer des systèmes de contrôle d'accès dans les bureaux

Mesures de sécurité pour les données personnelles

Quelques exemples de mesures de sécurité

Mesures logiques

- Adopter une politique d'accès logique et de mot de passe rigoureuse
- Sécuriser les postes de travail en renforçant leurs configurations (verrouillage automatique, contrôle des ports USB)
- Mettre en place des moyens de traçabilité des actions réalisés sur les postes et serveurs informatiques
- Installer et configurer des antivirus et des pare-feu
- Utiliser des canaux sécurisés de communication
- Limiter les accès aux interfaces et aux outils d'administration
- Réaliser régulièrement des sauvegardes des données
- Chiffrer les données stockées sur les postes de travail

Mesures de sécurité pour les données personnelles

Quelques exemples de mesures de sécurité

Mesures organisationnelles

- Formaliser une politique de contrôle d'accès aux données et aux systèmes (procédures en fonction du mouvement du personnel, revue des comptes)
- Mettre en place des mesures de sensibilisation de l'ensemble du personnel aux risques cyber
- Définir une politique de gestion des incidents de sécurité
- Réaliser des audits réguliers des traitements de données mis en œuvre

Mesures de sécurité pour les données personnelles

Guide de la CNIL sur la sécurité des données personnelles

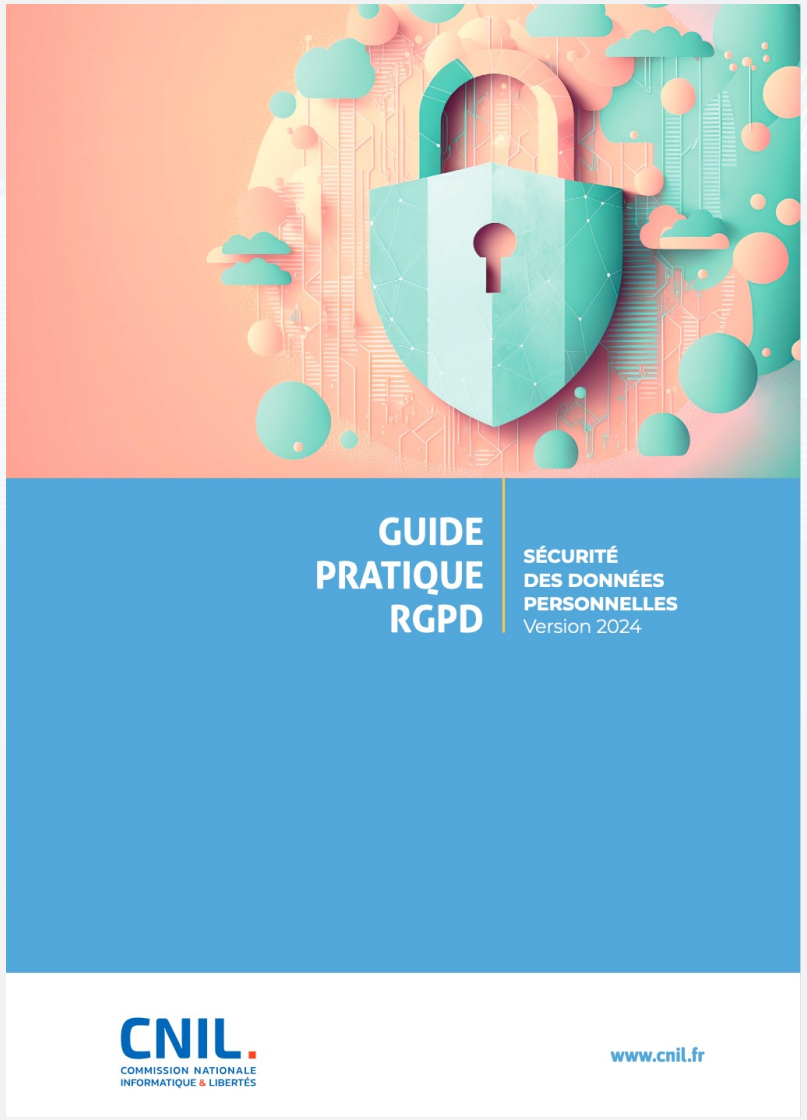


TABLE DES MATIÈRES

Gouvernance des organisations relative au RGPD

Gouvernance des organisations relative au RGPD

Les rôles et responsabilités dans le cadre du RGPD

Responsable de traitement (RT)

Traitement de données personnelles

Sous-traitant (ST)

Co-responsable de traitement (CoRT)

Délégué à la protection des données (DPO)

Gouvernance des organisations relative au RGPD

Les rôles et responsabilités dans le cadre du RGPD

Le RT est une personne morale ou physique qui définit les finalités et les moyens d'un traitement. Généralement, il s'agit du responsable légal de la structure

Le responsable de traitement est soumis au principe d'accountability

Il doit documenter toutes les démarches entreprises pour la mise en conformité de sa structure

- Etablir le registre des traitements
- Désigner le DPO
- Mettre en œuvre les mesures pour garantir la sécurité des données
- Assurer l'effectivité de l'information fournie aux usagers
- Mettre en place les procédures adaptées face aux violation de données
- Réaliser l'AIPD du traitement

En cas de non-conformité, c'est sa responsabilité qui est engagée

Gouvernance des organisations relative au RGPD

Les rôles et responsabilités dans le cadre du RGPD

Le délégué à la protection des données (DPD ou DPO en anglais) a la charge de la mise en œuvre de la conformité au RGPD des traitements réalisés au sein d'une structure.

Sa désignation

- Obligatoire lorsque l'organisme est public, ou qu'elle met en œuvre un suivi régulier et systématique des personnes à grandes échelles, ou des traitements à grande échelle de données sensibles ou relatives à des condamnations pénales et infractions
- Le DPO peut être interne ou externe à la structure
- Il doit avoir les compétences, les moyens et pouvoir garder son indépendance

Ses missions

- Information du responsable de traitement, des sous-traitants et des employés sur les exigences RGPD
- Conseil et accompagnement dans la réalisation d'analyse d'impact
- Contrôle du respect du règlement par la structure
- Coopération avec l'autorité de contrôle (la CNIL)

Le DPO n'est pas responsable en cas de non-respect du règlement

Gouvernance des organisations relative au RGPD

Les obligations des sous-traitants

Un sous-traitant est une personne physique ou morale qui traite des données personnelles pour le compte d'un organisme responsable de traitement, dans le cadre d'un service ou d'une prestation

Le contrat entre le RT et le ST doit inclure les éléments suivants exigés selon l'article 28 du RGPD	Ne traiter les données à caractère personnel que sur instruction documentée du responsable de traitement
	Veiller à ce que les personnes autorisées à traiter les données personnelles s'engagent à respecter la confidentialité
	Mettre en œuvre les mesures de sécurité techniques et organisationnelles appropriés concernant le traitement des données personnelles et notifie le responsable en cas de violation
	Ne recruter un autre sous-traitant uniquement sur autorisation du responsable de traitement
	Assister le responsable de traitement dans la réponse à l'exercice du droit des personnes
	Mettre à disposition du responsable de traitement toutes les informations nécessaires pour montrer le respect des obligations prévues

Gouvernance des organisations relative au RGPD
Le registre des traitements

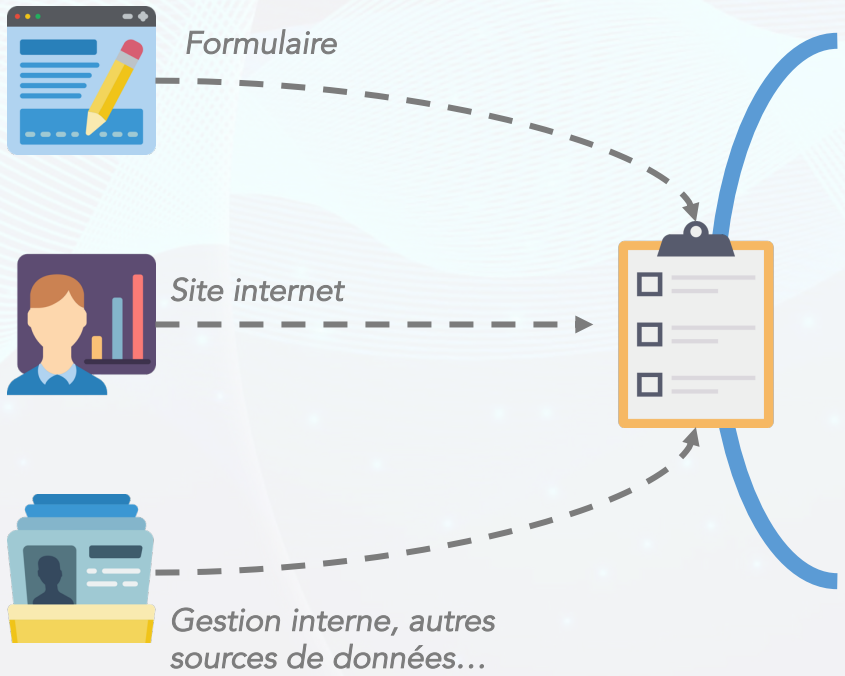
Le registre est une cartographie légale des traitements de données à caractère personnel.

Registre du responsable de traitement

Recense l'ensemble des traitements mis en œuvre par l'organisme

Registre du sous-traitant

Recense l'ensemble des catégories d'activités de traitement effectuées pour le compte des clients



Le registre des traitements contient :

- Les parties prenantes
- L'objectif poursuivi
- Les catégories de données utilisées
- Les destinataires des données
- La durée de conservation
- Les mesures de sécurité

Le registre est un document écrit (format libre), sous la responsabilité du dirigeant légal de l'organisme et présentable à la CNIL lors d'un contrôle

Gouvernance des organisations relative au RGPD
La notification de violations de données personnelles

Une violation de données concerne une perte de disponibilité, d'intégrité ou de confidentialité de données personnelles, de manière accidentelle ou illicite

1 Documentation de la violation en interne

2 Notification à la CNIL (via le site) dans les 72h

3 Notification auprès des personnes concernées

Gouvernance des organisations relative au RGPD

L'analyse d'impacts relative à la protection des données

Certains traitements de données nécessitent la réalisation d'une analyse d'impact relative à la protection des données (AIPD).

Il s'agit d'une analyse des risques pour la vie privée des personnes concernées par un traitement, notamment lorsque le risque est élevé.

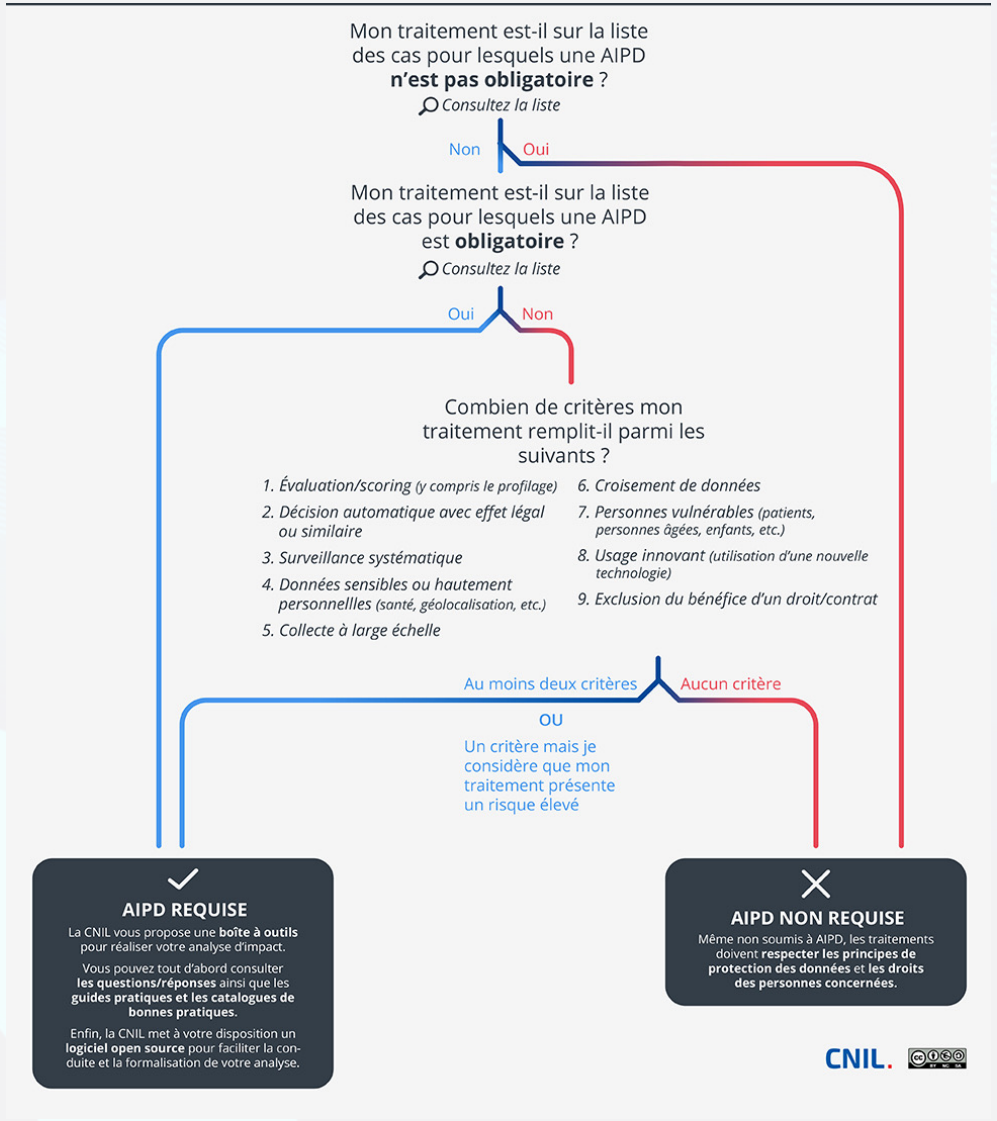
Une AIPD contient :

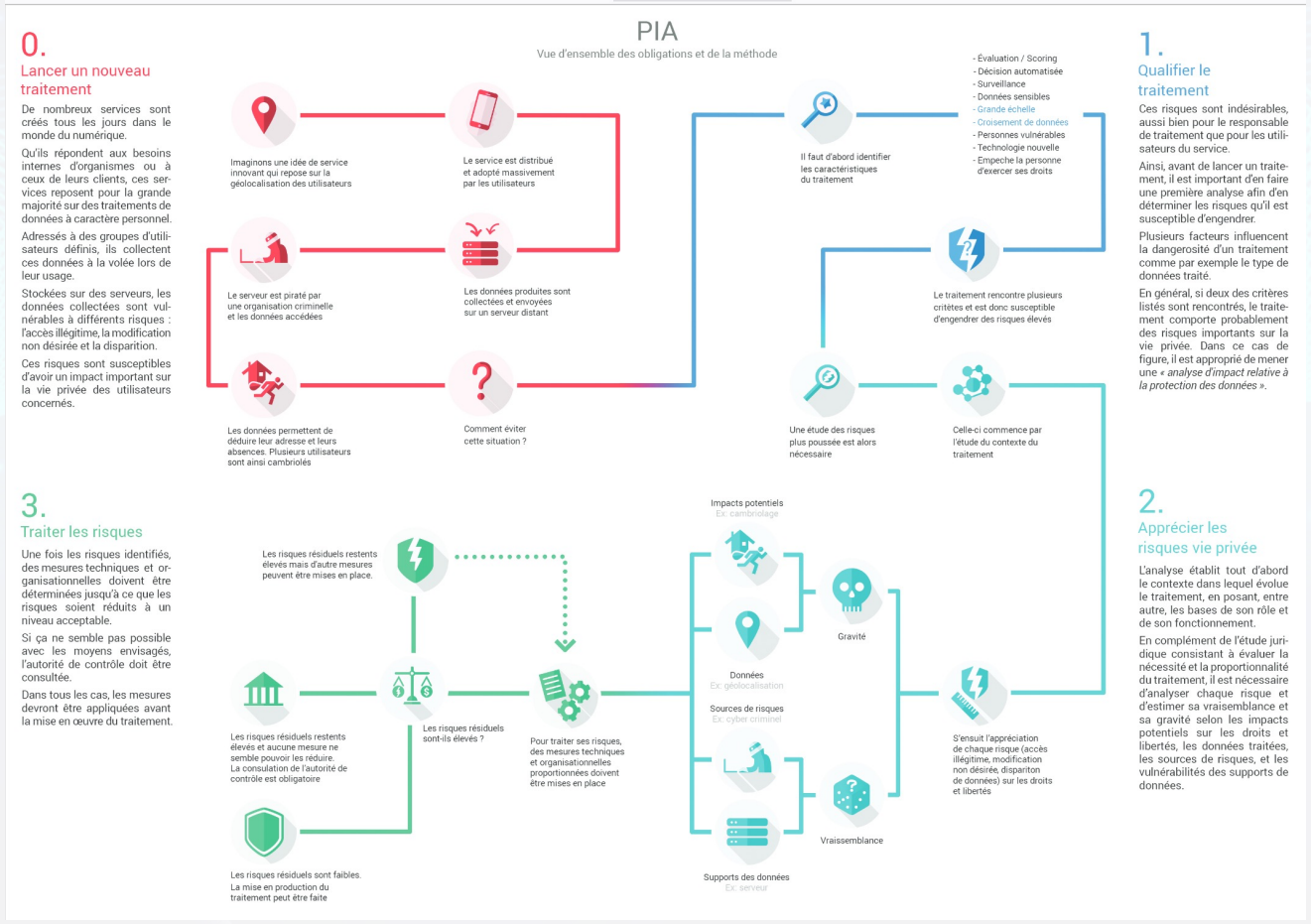
- **Une description détaillée du traitement**
- **Une évaluation des principes juridiques**
- **Une évaluation technique et organisationnelle des risques sur la confidentialité, l'intégrité et la disponibilité des données, et leurs impacts sur la vie privée**

Traitements ayant pour finalité l'accompagnement social ou médico-social des personnes	- collecte de données sensibles - évaluation ou notation - personnes dites « vulnérables »	- traitement mis en œuvre par un établissement ou une association dans le cadre de la prise en charge de personnes en insertion ou réinsertion sociale et professionnelle ; - traitement mis en œuvre par les maisons départementales des personnes handicapées dans le cadre de l'accueil, l'hébergement, l'accompagnement et le suivi de ces personnes ; - traitement mis en œuvre par un centre communal d'action sociale dans le cadre du suivi de personnes atteintes de pathologies chroniques invalidantes en situation de fragilité sociale.

Gouvernance des organisations relative au RGPD

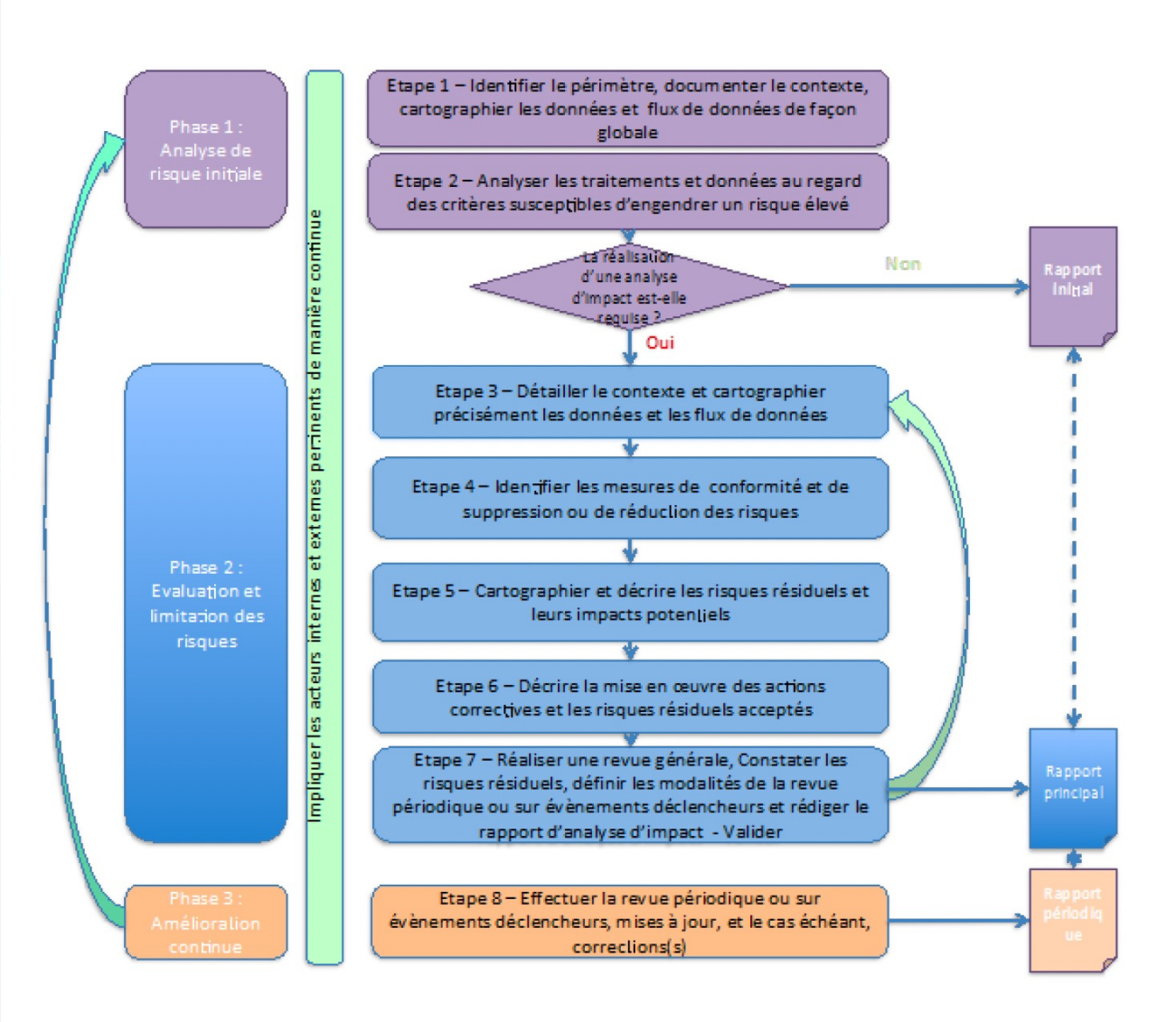
L'analyse d'impacts relative à la protection des données





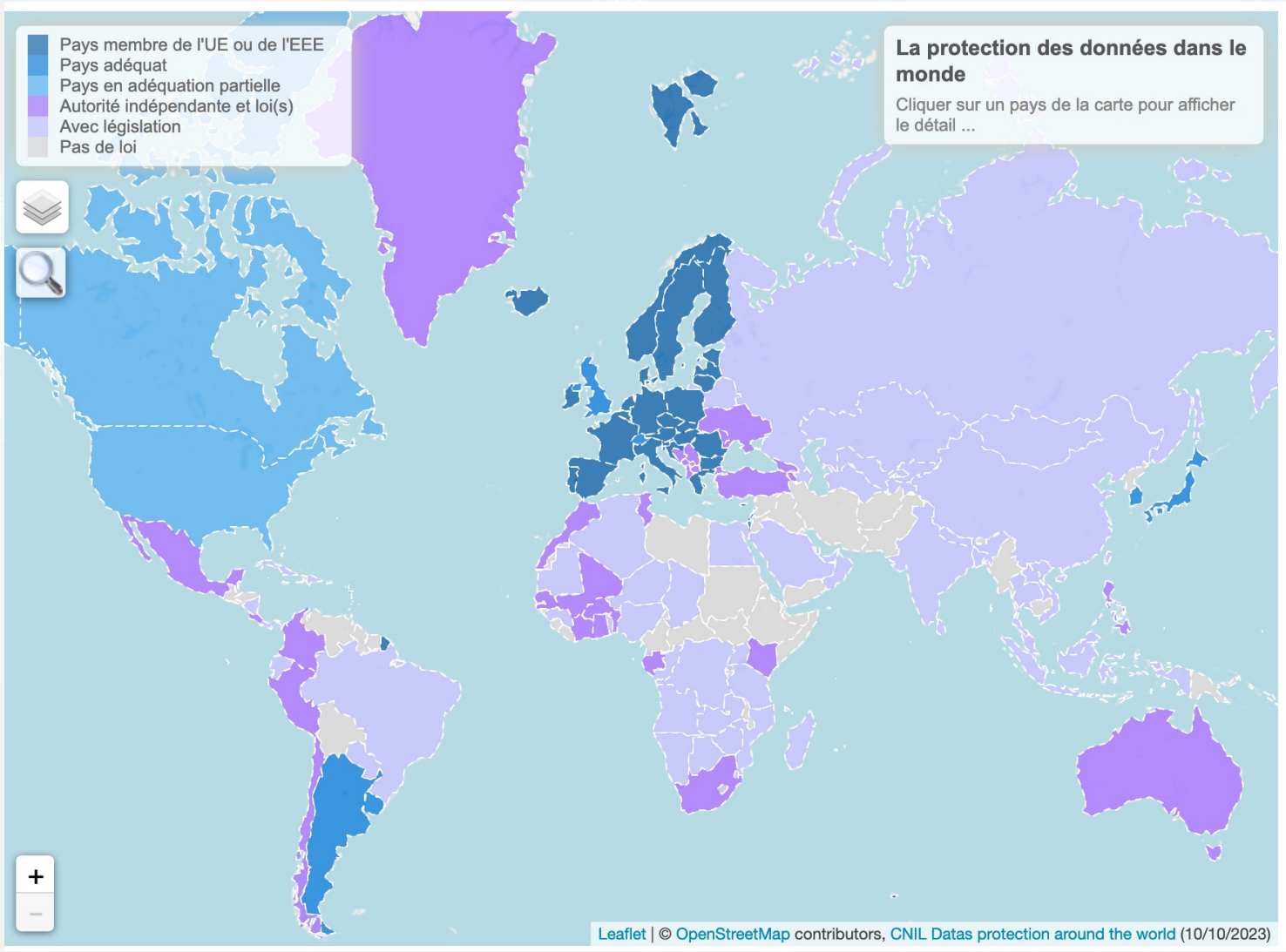
Gouvernance des organisations relative au RGPD

L'analyse d'impacts relative à la protection des données

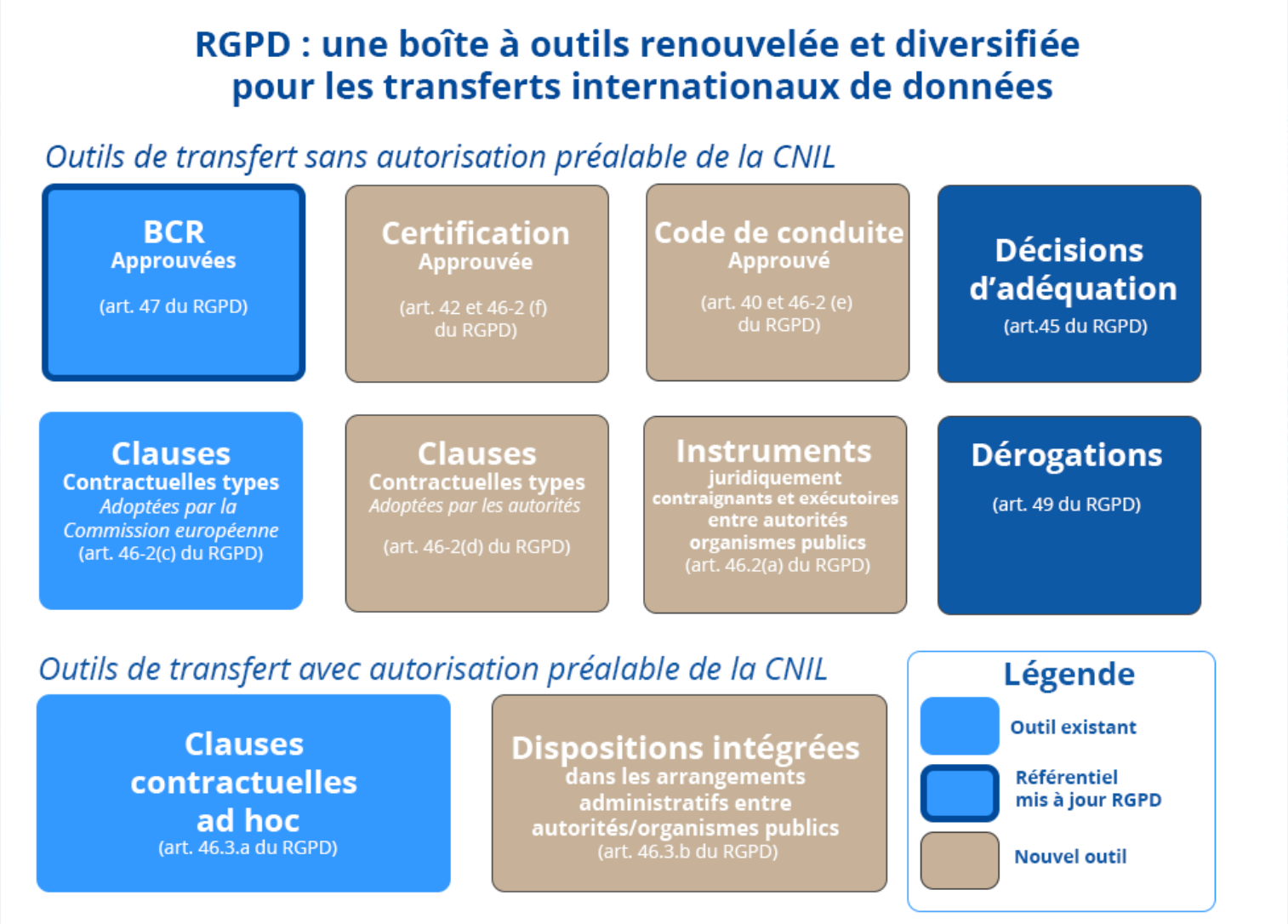


Gouvernance des organisations relative au RGPD

Les transferts de données hors UE



Gouvernance des organisations relative au RGPD
Les transferts de données hors UE



Conclusion

En conclusion : les étapes vers la conformité

1. Etablir le registre des traitements
2. Mettre en œuvre l'exercice du droit des personnes
3. Formaliser et mettre en œuvre les durées de conservation
4. Mettre en œuvre les mesures de sécurité des données
5. Réaliser une analyse d'impact
6. Veiller à la légalité des flux transfrontaliers