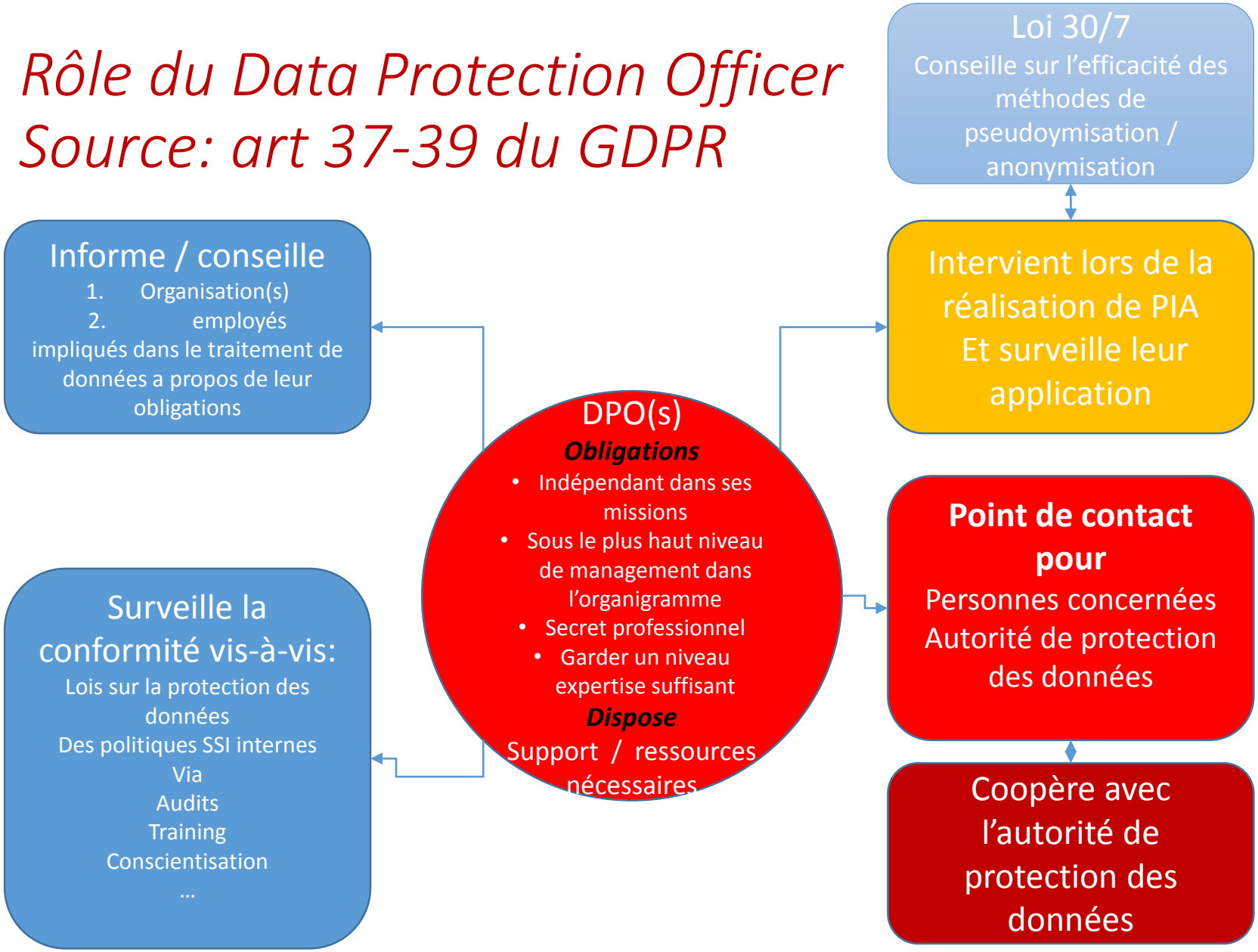
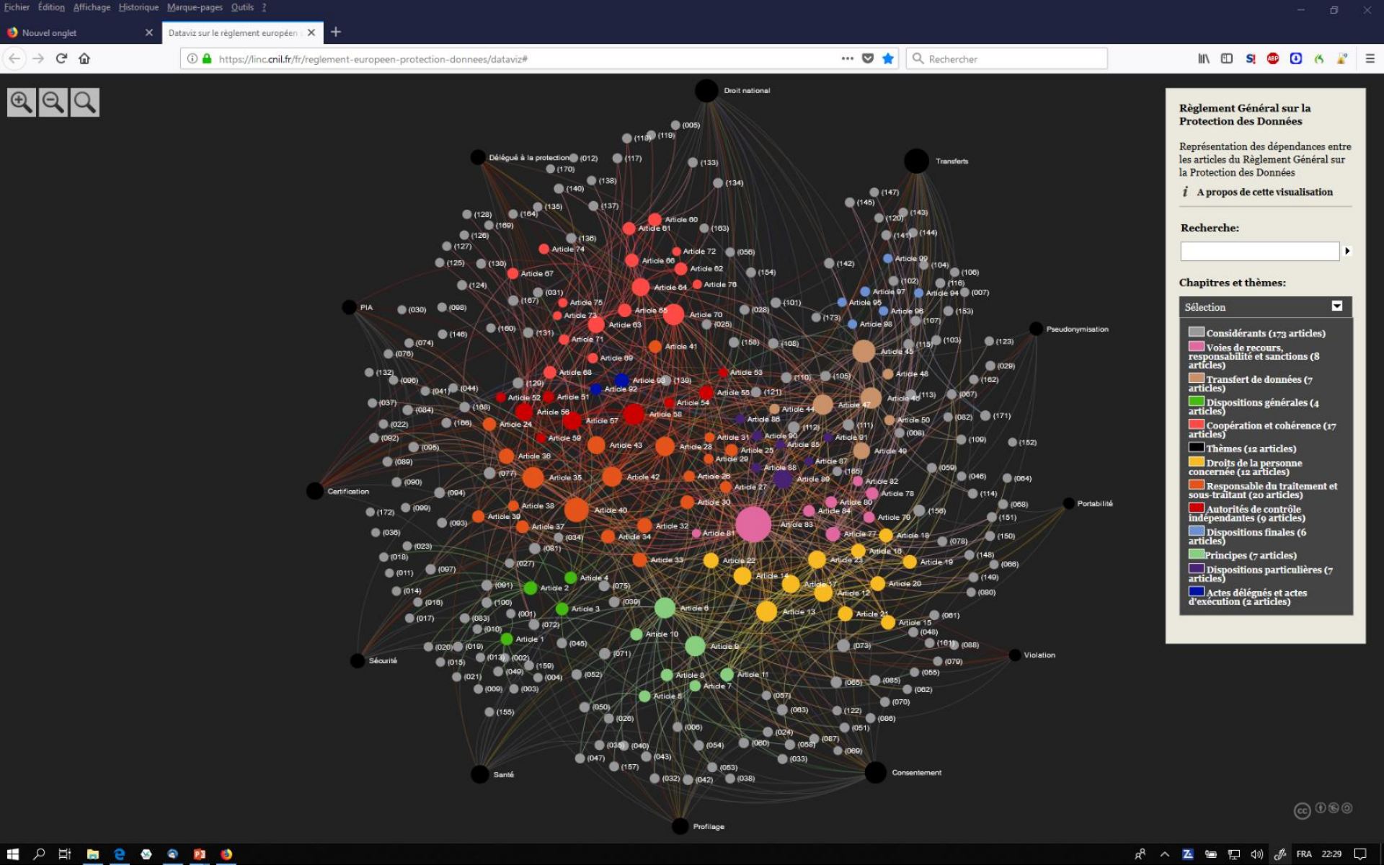
19ème RENCONTRE Eveline Markiewicz

Le rôle du délégué à la protection des données

Ir Etienne Stanus, PhD
Délégué à la protection des données
Institut Jules Bordet
Etienne.stanus@bordet.be

Rôle du Data Protection Officer
Source: art 37-39 du GDPR



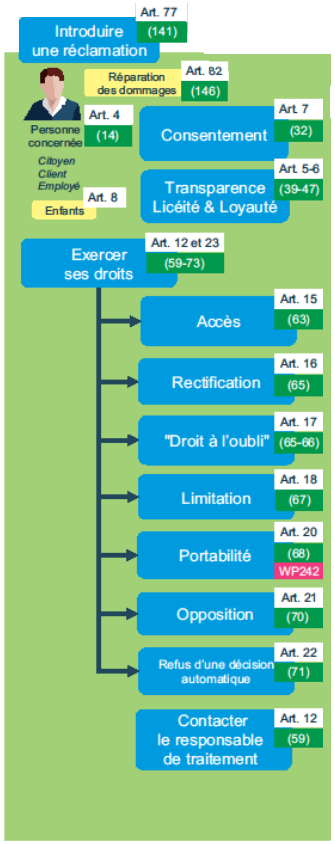


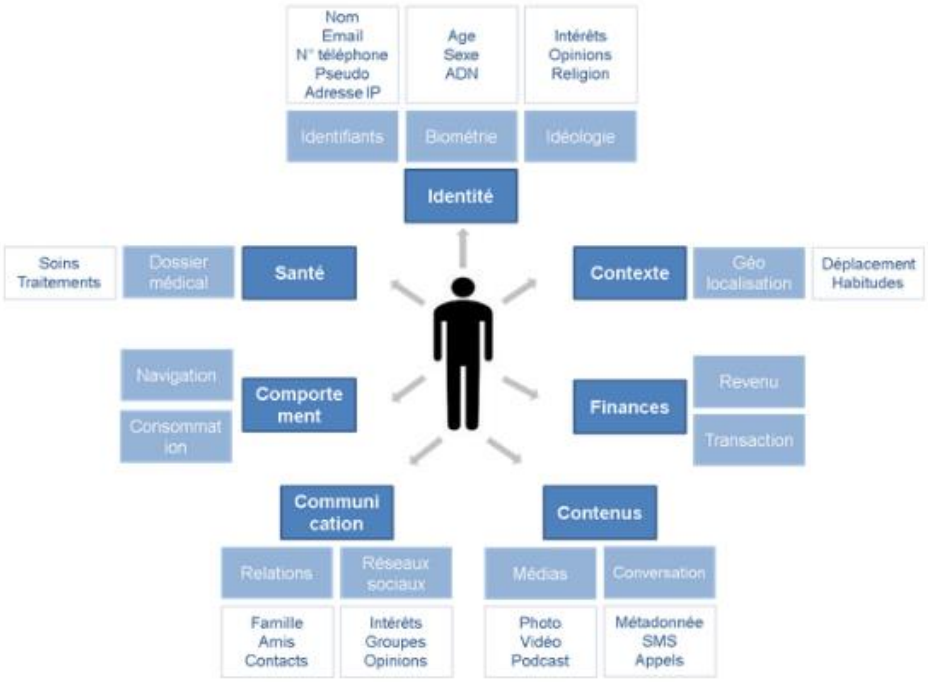
Source https://linc.cnil.fr/fr/reglement-europeen-protection-donnees/dataviz

GDPR: 88 pages, 173 considérants, 99 articles

Pour une version « manipulable » en mode texte cf: www.gdpr-expert.eu

25 mai 2018, les données à caractère personnel entrent dans l'ére du GDPR
Evolution pas une révolution ! Mais avec des conséquences importantes sur la responsabilité des personnes qui les traitent.
30 juillet 2018: la Belgique précise (entre autres choses) le cas de la recherche.





Cartographie des données personnelles

Source : serdaLAB

Définition officielle (GDPR art 4):
toute information se rapportant à une personne physique identifiée ou identifiable;
est réputée être une "personne physique identifiable" une personne physique **qui peut être identifiée, directement ou indirectement,** notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

A VISUAL GUIDE TO PRACTICAL DATA DE-IDENTIFICATION

Produced by FUTURE OF PRIVACY FORUM FPF.ORG

In collaboration with EY

What do scientists, regulators and lawyers mean when they talk about de-identification? How does anonymous data differ from pseudonymous or de-identified information? Data identifiability is not binary. Data lies on a spectrum with multiple shades of identifiability.

This is a primer on how to distinguish different categories of data.

DEGREES OF IDENTIFIABILITY

Information containing direct and indirect identifiers.

PSEUDONYMOUS DATA

Information from which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact.

DE-IDENTIFIED DATA

Direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities.

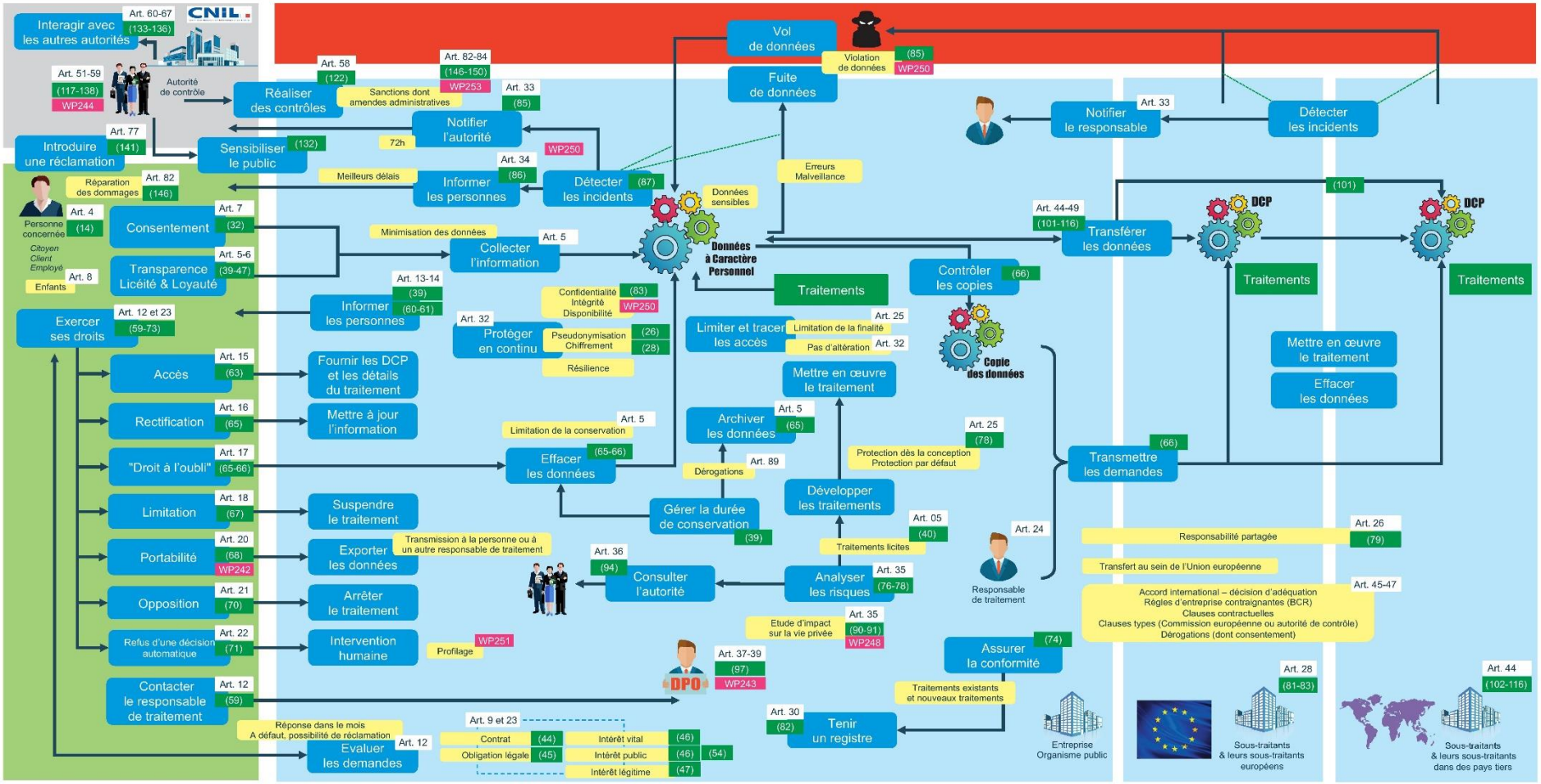
ANONYMOUS DATA

Direct and indirect identifiers have been removed or manipulated together with mathematical and technical guarantees to prevent re-identification.

	EXPLICITLY PERSONAL	POTENTIALLY IDENTIFIABLE	NOT READILY IDENTIFIABLE	KEY CODED	PSEUDONYMOUS	PROTECTED PSEUDONYMOUS	DE-IDENTIFIED	PROTECTED DE-IDENTIFIED	ANONYMOUS	AGGREGATED ANONYMOUS
DIRECT IDENTIFIERS Data that identifies a person without additional information or by linking to information in the public domain (e.g., name, SSN)	INTACT	PARTIALLY MASKED	PARTIALLY MASKED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
INDIRECT IDENTIFIERS Data that identifies an individual indirectly. Helps connect pieces of information until an individual can be singled out (e.g., DOB, gender)	INTACT	INTACT	INTACT	INTACT	INTACT	INTACT	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
SAFEGUARDS and CONTROLS Technical, organizational and legal controls preventing employees, researchers or other third parties from re-identifying individuals	NOT RELEVANT due to nature of data	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	NOT RELEVANT due to nature of data	NOT RELEVANT due to high degree of data aggregation
SELECTED EXAMPLES	Name, address, phone number, SSN, government-issued ID (e.g., Jane Smith, 123 Main Street, 555-555-5555)	Unique device ID, license plate, medical record number, cookie, IP address (e.g., MAC address 68:A8:6D:35:65:03)	Same as Potentially Identifiable except data are also protected by safeguards and controls (e.g., hashed MAC addresses & legal representations)	Clinical or research datasets where only curator retains key (e.g., Jane Smith, diabetes, HgB 15.1 g/dl = Csrk123)	Unique, artificial pseudonyms replace direct identifiers (e.g., HIPAA Limited Datasets, John Doe = SL7T LX619Z) (unique sequence not used anywhere else)	Same as Pseudonymous, except data are also protected by safeguards and controls	Data are suppressed, generalized, perturbed, swapped, etc. (e.g., GPA: 3.2 = 3.0-3.5, gender: female = gender: male)	Same as De-Identified, except data are also protected by safeguards and controls	For example, noise is calibrated to a data set to hide whether an individual is present or not (differential privacy)	Very highly aggregated data (e.g., statistical data, census data, or population data that 52.6% of Washington, DC residents are women)

LES DONNÉES À CARACTÈRE PERSONNEL SONT ENTRÉES DANS L'ÈRE DU RGPD

Cette infographie est issue d'un groupe de travail du CLUSIF (www.clusif.fr). Elle résume le Règlement Général sur la Protection des Données.
Elle ne peut pas être exhaustive mais elle offre une grille de lecture graphique et synthétique pour découvrir la portée de la règlementation, puis s'y référer ultérieurement.



Le CLUSIF (Club de la Sécurité de l'Information Français) est le 1er club de professionnels de la sécurité de l'information français, réunissant plus de 300 entreprises et collectivités issues de tous les secteurs de l'économie. L'objectif principal du CLUSIF est de favoriser les échanges d'idées et de retours d'expériences à travers des groupes et espaces de travail, comme Espace RSSI, des publications de référence et des conférences thématiques organisées tout au long de l'année. Quelques exemples de sujets abordés dans les groupes de travail : applications mobiles, cyberassurance, étude MIPS (menaces informatiques et pratiques de la sécurité), internet des objets, panorama de la cybersécurité, RGPD, sécurité numérique au quotidien, signature électronique, systèmes industriels, tableaux de bords de sécurité…

Pour toute information complémentaire, vous pouvez contacter : Luména Duluc, déléguée générale : 01 53 25 08 80 (clusif@clusif.fr)

Légende

- Art. 51 — Article du Règlement européen
- (141) — Considérant du Règlement européen
- WP244 — Ligne directrice du G29

Qu'est-ce qu'une EIVP /PIA, analyse d'impact relative à la protection des données

- **Une description détaillée** du traitement de données mis en œuvre, comprenant tant les aspects techniques qu'opérationnels
- **L'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux** (finalité, données et durées de conservation, information et droits des personnes, *etc*.) non négociables, qui sont fixés par la loi et doivent être respectés, quels que soient les risques ;
- **L'étude, de nature plus technique, des risques sur la sécurité des données** (confidentialité, intégrité et disponibilité) **ainsi que leurs impacts potentiels sur la vie privée**, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données.

Source: CNIL www.cnil.fr

Quand est-ce qu'une analyse d'impact est obligatoire ?

GDPR : quand le traitement est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées* ».

G29 : le traitement remplit au moins deux des neuf critères issus des lignes directrices du

- évaluation/scoring (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles données à caractère personnel ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat.

- Etats : imposition par la réglementation
  - Belgique: loi du 30 juillet
  - France: liste imposée par la CNIL

Extrait de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise

https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-avec-aipd-requise.pdf

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise

Types d'opérations de traitement	Critères issus des lignes directrices du CEPD qu'ils remplissent	Exemples
Traitements de données de santé mis en œuvre par les établissements de santé ou les établissements médico-sociaux pour la prise en charge des personnes.	- collecte de données sensibles - personnes dites « vulnérables »	- traitements « de santé » mis en œuvre par les établissements de santé (hôpital, CHU, cliniques, etc.) : • dossier « patients » ; • algorithmes de prise de décision médicale ; • dispositifs de vigilances sanitaires et de gestion du risque ; • dispositifs de télémédecine ; • gestion du laboratoire de biologie médicale et de la pharmacie à usage intérieur, etc. - traitement portant sur les dossiers des résidents pris en charge par un centre communal d'action sociale (CCAS) ou par un établissement d'hébergement pour personnes âgées dépendantes (EPHAD).
Traitements portant sur des données génétiques de personnes dites « vulnérables » (patients, employés, enfants, etc.).	- collecte de données sensibles - personnes dites « vulnérables »	- mise en œuvre d'une recherche médicale portant sur des patients et incluant le traitement de leurs données génétiques ; - traitement utilisé pour la gestion d'une consultation de génétique dans un établissement de santé.
Traitements des données de santé nécessaires à la constitution d'un entrepôt de données ou d'un registre	- collecte de données sensibles - personnes dites « vulnérables »	- entrepôt de données de santé mis en œuvre par un établissement de santé ou une personne privée, pour servir des finalités de recherche.

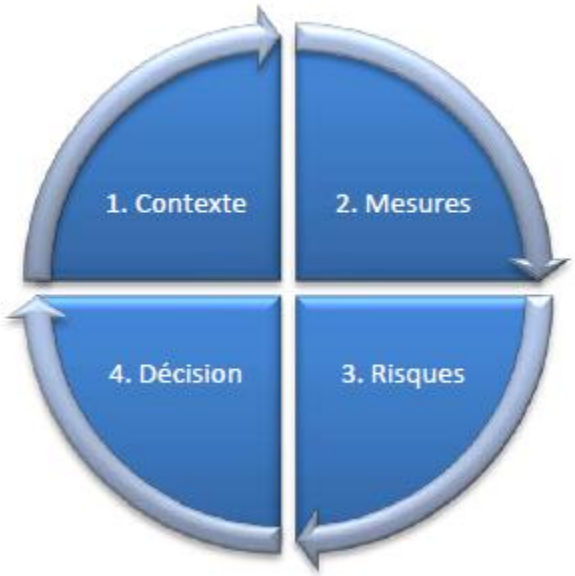
En pratique
Quand est-ce qu'une analyse d'impact n'est pas obligatoire ?

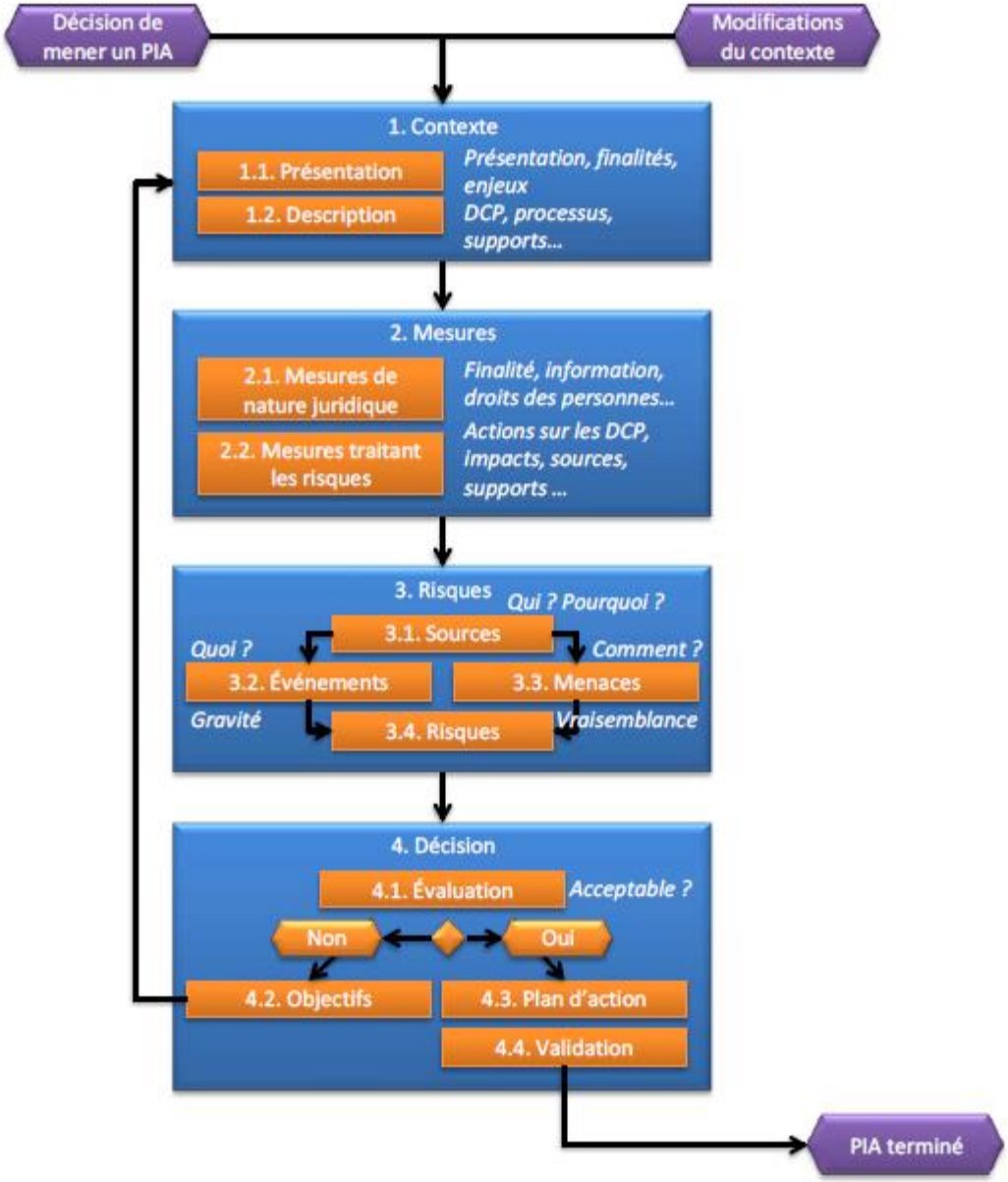
- quand le traitement ne présente pas de risque élevé pour les droits et libertés des personnes concernées ;
- quand le traitement répond à une obligation légale ou est nécessaire à l'exercice d'une mission de service public (art 6.1.c 6.1.e), sous réserve que les conditions suivantes soient remplies :
  - qu'il ait une base juridique dans le droit de l'UE ou le droit de l'État membre ;
  - que ce droit règlemente cette opération de traitement ;
  - et qu'une AIPD ait déjà été menée lors de l'adoption de cette base juridique ;
- lorsque la nature, la portée, le contexte et les finalités du traitement envisagé sont très similaires à un traitement pour lequel une AIPD a déjà été menée

=> intérêt de définir des cadres types:

- **méthodologies de référence (CNIL) ou code de conduites approuvés (∄ encore)**
- **à adapter au cadre légal Belge**
- **conditions techniques et organisationnelles prédéfinies**
- **engagement de conformité au cadre ainsi créé**

Synoptique de la méthode





RGPD – Droits pouvant être exercés par les personnes concernées en fonction de la base légale

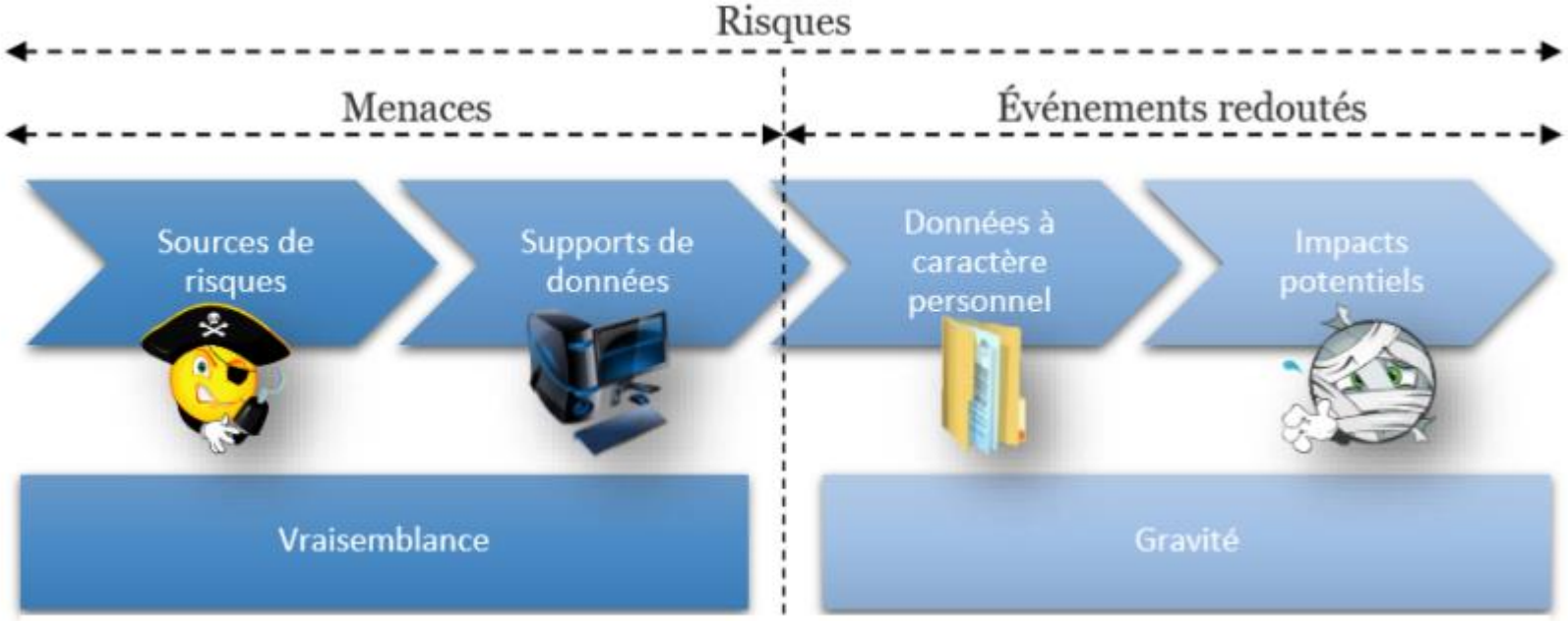
Source: Virginie Grégoire ULB

	Droit d'accès	Droit de rectification	Droit à l'effacement	Droit à la limitation	Droit à la portabilité	Droit d'opposition
Consentement	X	X	X	X	X	droit de retirer le consentement
Contrat	X	X	X	X	X	
Obligation légale	X	X		X		
Intérêts vitaux	X	X	X	X		
Mission d'intérêt public / exercice de l'autorité publique	X	X		X		X
Intérêt légitime	X	X	X	X		X
						Toujours droit d'opposition contre une décision individuelle automatisée (profilage)

Attention: consentir à qq chose d'illégal ne rend pas le traitement de données légal !

Risque

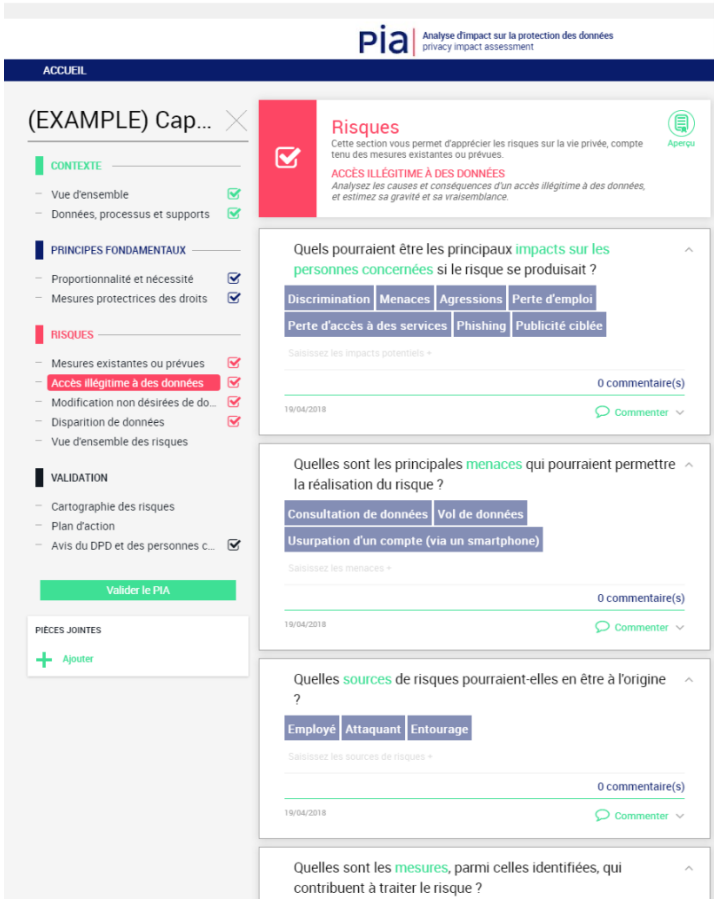
- *ISO 31000:2009 – Management du risque — Principes et lignes directrices:*
  « Le risque est l'effet de l'incertitude sur l'atteinte des objectifs »
- ISO/CEI Guide 73:2002 X50-251: Management du risque –Vocabulaire
  « Le risque est la combinaison de probabilité d'évènement et de sa conséquence »



Source cnil-pia-1-fr-methode.pdf sur www.cnil.fr

Etude d'impact sur la vie privée

Sources: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-captoo-fr.pdf
https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil



Pour en revenir au rôle de DPO, ce n'est donc pas

Source: https://www.lenetexpert.fr/rgpd-le-data-protection-officer-est-un-gardien-pour-les-donnees-personnelles/?print=print

Mais plutôt:

Source: http://www.gilles-rapaport.com/strategies-la-mise-en-conformite-rgpd-les-dpo/