Les contraintes du RGPD

A quoi la véritable anonymisation de données à caractère personnel permet-elle d'échapper ?

Congrès 2019

Société informatique de France

Charlotte Barraco-David, avocat

Donnée personnelle vs Donnée anonyme Le grand débat

DONNÉE PERSONNELLE

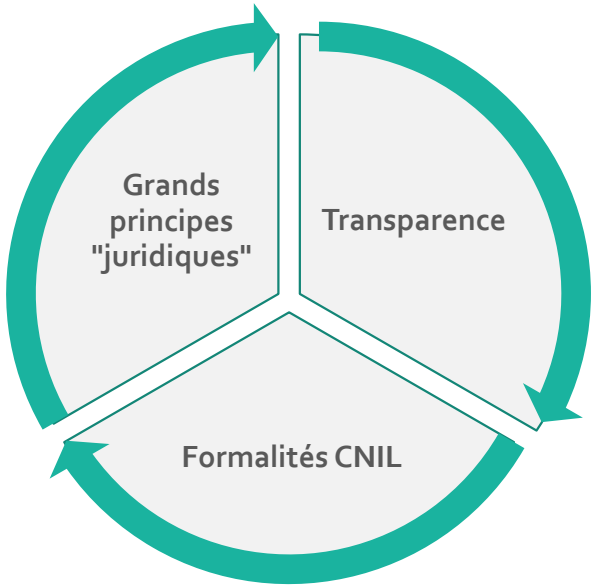
Art. 4 RGPD : «toute information se rapportant à une personne physique [...] qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale»

Considérant 26 RGPD : « il convient de prendre en considération l'ensemble des moyens **raisonnablement susceptibles d'être utilisés** par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. **Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche**. »

Collecte et traitement des données personnelles : évolution règlementaire

AVANT

28 pays = 28 règlementations = 28 façons de *(mal)* appliquer une directive

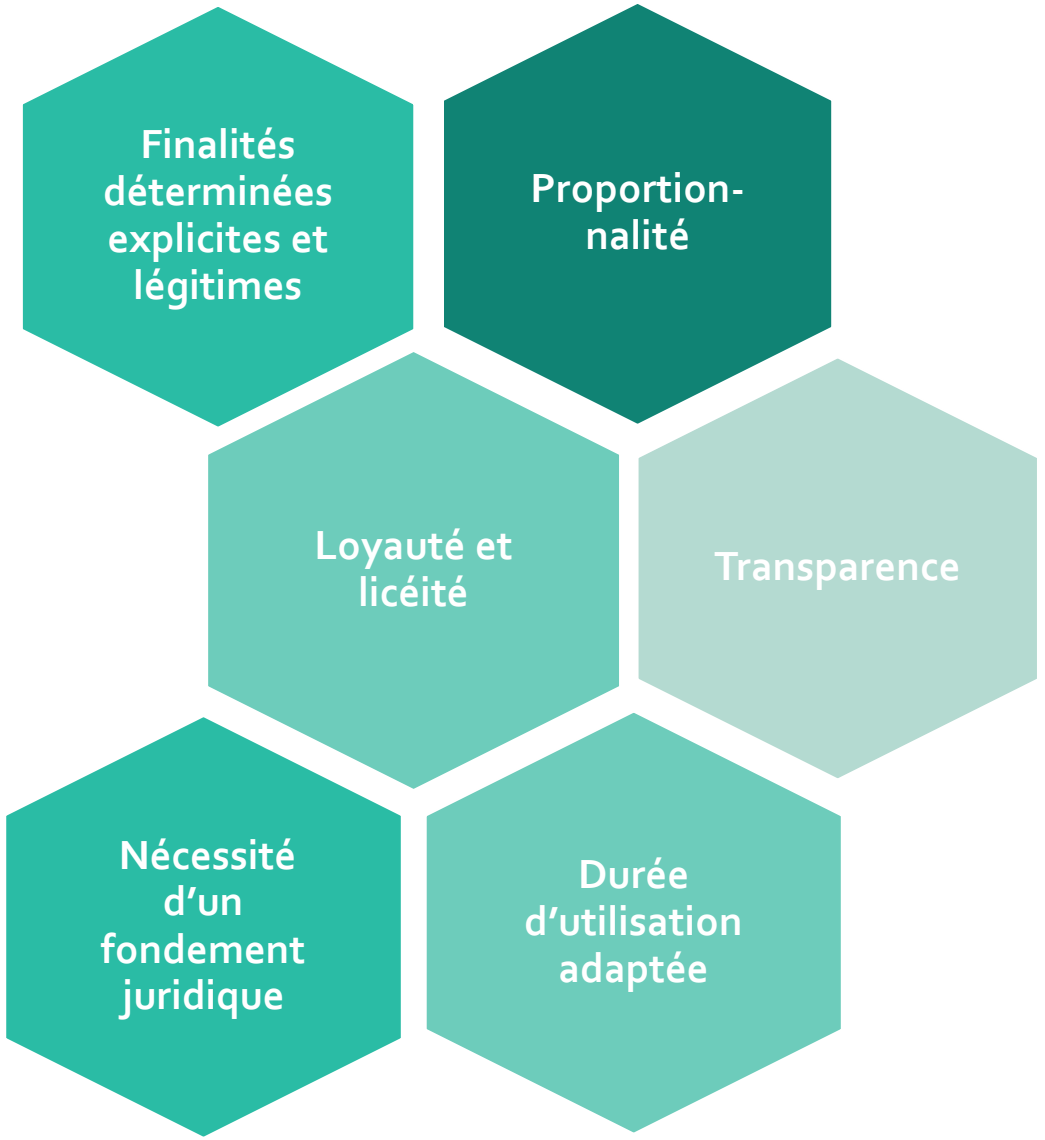


AUJOURD'HUI

Depuis le 25 mai 2018 : **1 seul texte** *(ou presque…)* **très dissuasif**

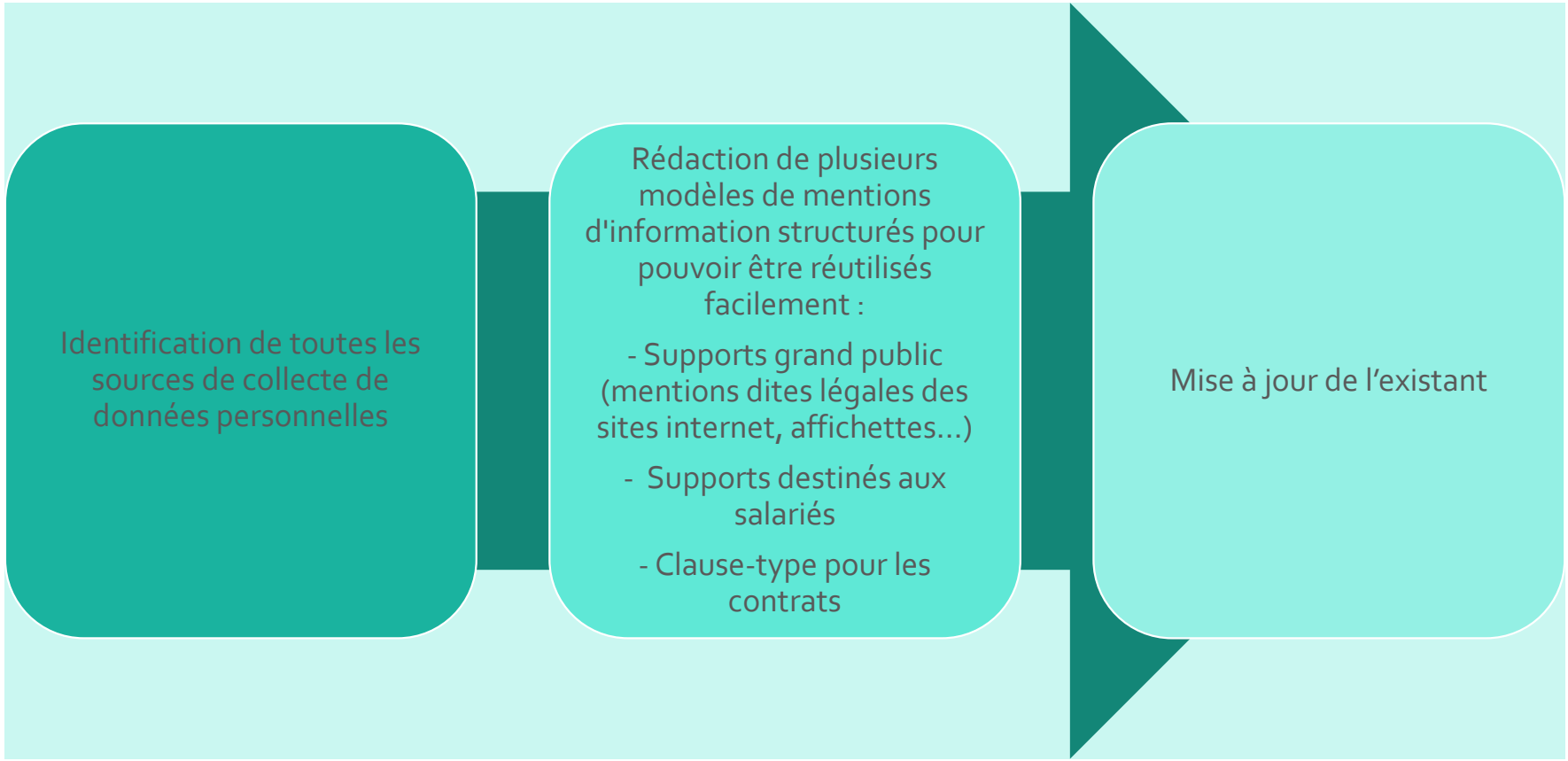
LES PILIERS DE LA RÉGLEMENTATION

Collecte et traitement de données personnelles : les grands principes à respecter



RENFORCEMENT DE LA TRANSPARENCE (ou quand trop d'information tue l'information)

Collecte et traitement de données personnelles : l'obligation d'information



LA (QUASI) DISPARITION DES FORMALITÉS CNIL : une fausse bonne nouvelle

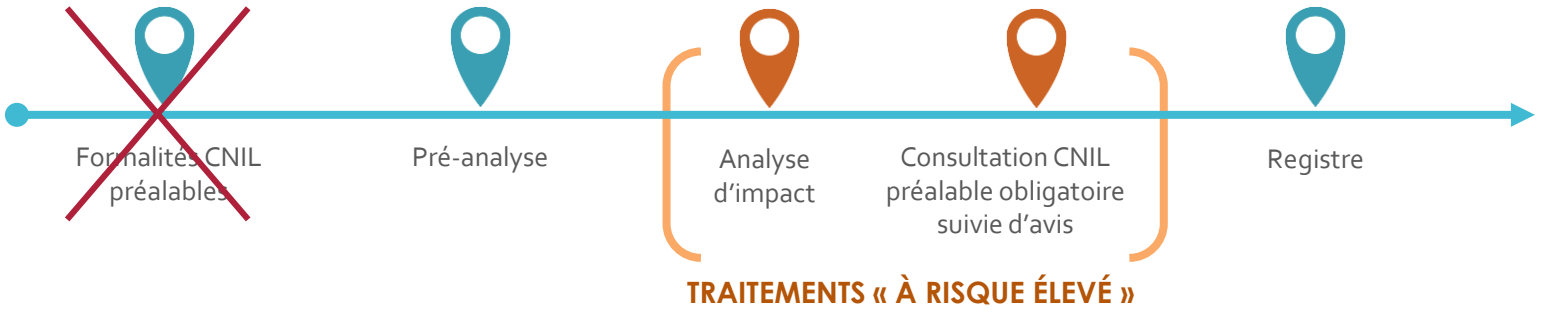
Les obligations de documentation des traitements de données personnelles

Les formalités préalables sont remplacées par :

REGISTRE DES TRAITEMENTS

ANALYSE D'IMPACT (TRAITEMENTS A RISQUE ELEVE)

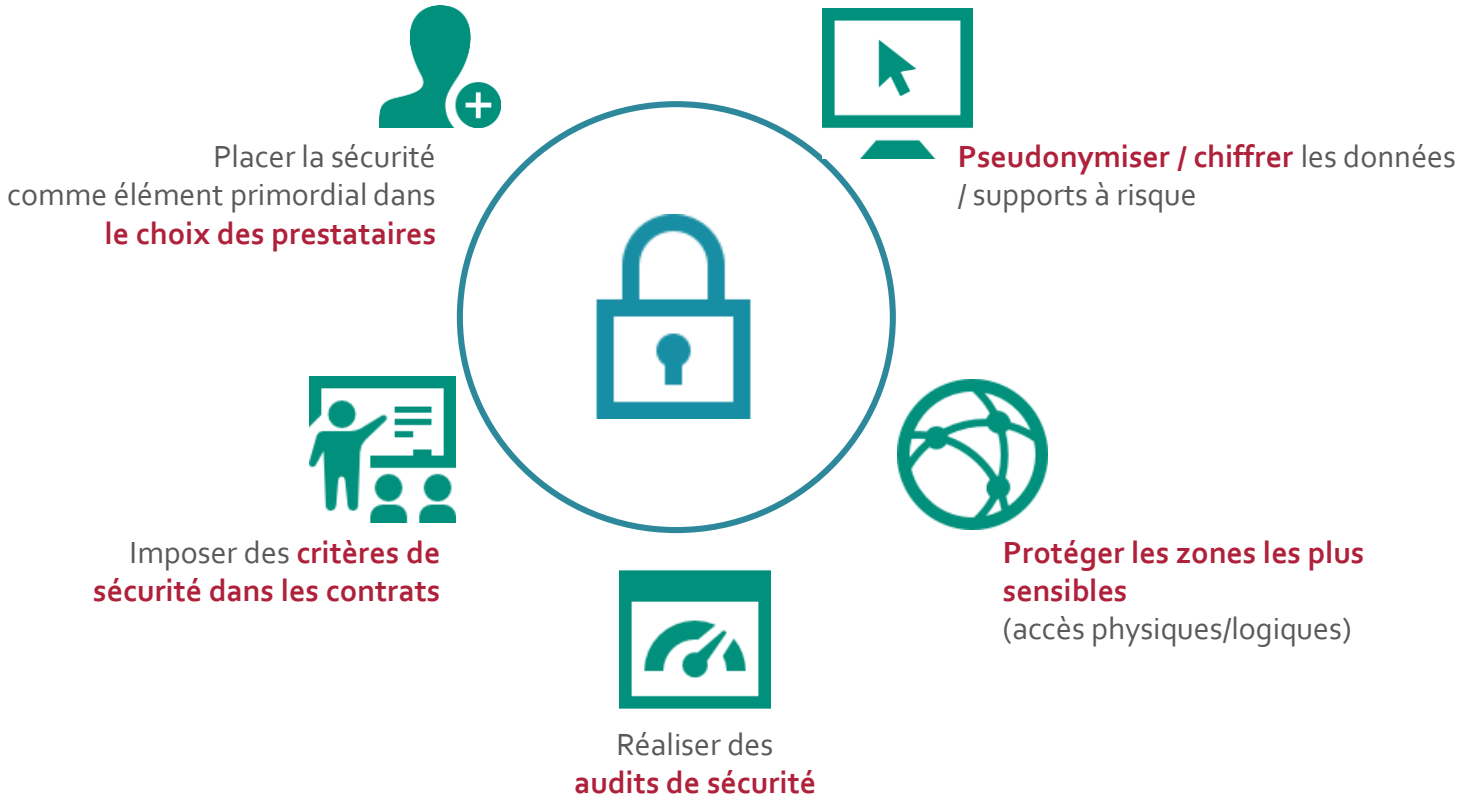
CONSULTATION DE LA CNIL (TRAITEMENTS A RISQUES ELEVES RESIDUELS)



LA SÉCURITÉ : UN PRINCIPE ANCIEN, DÉPOUSSIÉRÉ

Une approche par les risques - Une protection multifactorielle

Collecte et traitement des données personnelles : assurer la sécurité



SE PRÉPARER À NOTIFIER LES COMPROMISSIONS DE DONNÉES :

72 heures pour (ré)agir

Collecte et traitement des données personnelles : notifier les compromissions

Existence d'un risque

Notification CNIL

Existence d'un risque élevé

Information des personnes

Définition d'une méthodologie d'évaluation des risques conditionnant le déclenchement d'une notification

Rédaction d'une procédure de notification

Constitution d'une cellule de gestion de crise activable à tout moment

RESPECT DU DROIT DES PERSONNES

Collecte et traitement des données personnelles : respecter les droits des personnes

Sur justification de son identité, sauf cas particulier (Cf. obligation de sécurité) :

- DROIT D'OPPOSITION
- DROIT D'ACCÈS
- DROIT DE LIMITATION DU TRAITEMENT
- DROIT DE RECTIFICATION
- DROIT DE DEFINIR DES DIRECTIVES POST-MORTEM
- DRIOT A LA SUPPRESSION (le mal nommé droit à l'oubli)
- DROIT À LA PORTABILITE

Les contraintes liées aux transferts internationaux de données personnelles

PAYS **DISPOSANT** D'UN NIVEAU DE PROTECTION SUFFISANT: **TRANSFERTS LIBRES**

UNION EUROPÉENNE

- **Transferts libres dans l'UE (+ Espace économique européen)**

HORS UNION EUROPÉENNE

- **Transferts libres vers des pays hors UE mais disposant d'un niveau de protection adéquat selon la Commission européenne**

PAYS **NE DISPOSANT PAS** D'UN NIVEAU DE PROTECTION SUFFISANT: **DÉROGATIONS**

HORS UNION EUROPÉENNE

- **Dérogation avec des « garanties appropriées » :** ex clauses contractuelles types, certification approuvée
- **Dérogation pour les groupes disposant de règles d'entreprise contraignantes** (*Binding Corporate Rules – BCR*)
- **Dérogation spécifiques** (consentement, nécessité de la réalisation de certaines finalités spécifiques, telles que la sauvegarde de la vie de la personne concernée, l'exécution d'un contrat)
- **Dérogation pour les transferts ponctuels et non massifs** (intérêts légitimes impérieux)

Des risques de sanction non négligeables

AVANT LE RGPD

Sanctions administratives
PEU DISSUASIVES ET DISPARATES
au sein de l'Europe :

- jusqu'à 3.000.000€ en France (il y a peu, jusqu'à 150.000€)
- jusqu'à 300.000€ par manquement (Espagne)
- jusqu'à £ 500.000 (Royaume Uni)

AUJOURD'HUI

Sanctions administratives
TRÈS DISSUASIVES ET UNIFIEES au sein de l'Europe :

- jusqu'à **20.000.000€ ou 4% du CA annuel monde**

Ex : 21/01/2019 condamnation par la CNIL de Google à 50,000,000€

Merci de votre attention

Charlotte Barraco-David

Avocat | Of Counsel

c.barraco-david@latournerie-wolfrom.com

latournerie wolfrom avocats

PARIS | LYON | BORDEAUX

164, rue du Faubourg Saint-Honoré
75008 Paris
Tél : 01 56 59 74 74
www.latournerie-wolfrom.com