MERCREDI 26 JUIN 2013

LA NOUVELLE REGLEMENTATION EN MATIERE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL:

LE PROJET DE REGLEMENT COMMUNAUTAIRE

Patrick Boiron – Karine Riahi

Matthieu Bourgeois – Cécile Fontaine

KGA Avocats

44, Avenue des Champs Elysées (Paris – 75008)

www.kga.fr - Consultez les chroniques juridiques du cabinet sur **kpratique.fr**

PARTIE 1/
RAPPEL DU DISPOSITIF EXISTANT

1. Le texte
2. Les enjeux et les risques
3. Les acteurs
4. Les formalités

1.1. Le texte : La loi informatique et libertés (6 janvier 1978)

- **Objectif = encadrer le traitement des données à caractère personnel**
  - Création d'une Autorité Administrative Indépendante = la CNIL

- **Les principes fondamentaux**

1) **Le principe de finalité : une utilisation encadrée des données**

2) **Le principe de proportionnalité**

1.2. Les enjeux et les risques

- Sanctions punitives
  - Sanctions pénales (juridictions répressives)*
    - 5 ans de prison
    - 300 000 € amende
    - Peines complémentaires :
      - Dissolution, interdiction d'exercer, fermeture de l'établissement…

  - Sanctions pécuniaires (CNIL)**
    - 150 000 € (pour 1er manquement)
    - Si récidive dans les 5 ans :
      - 5 % du CA (dans la limite de 300 000 €)

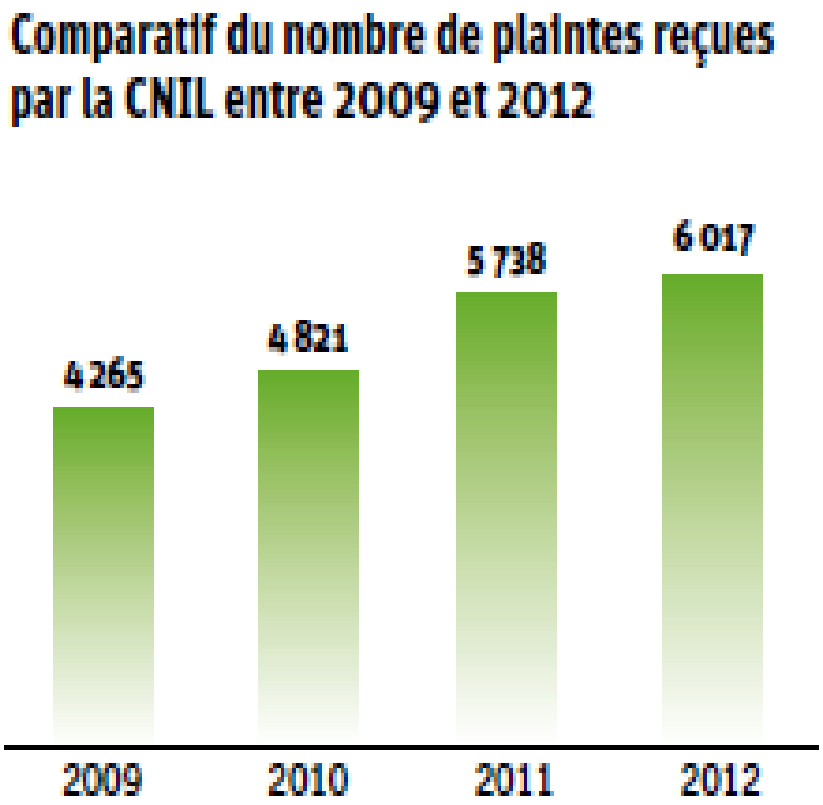
- Sanctions civiles
  - Dommages et intérêts

*Art. 226-16 à 226-24. C. Pén.
** Art 47 loi 1978

1.2. Les enjeux et les risques (2/)

L'activité de la CNIL en chiffres

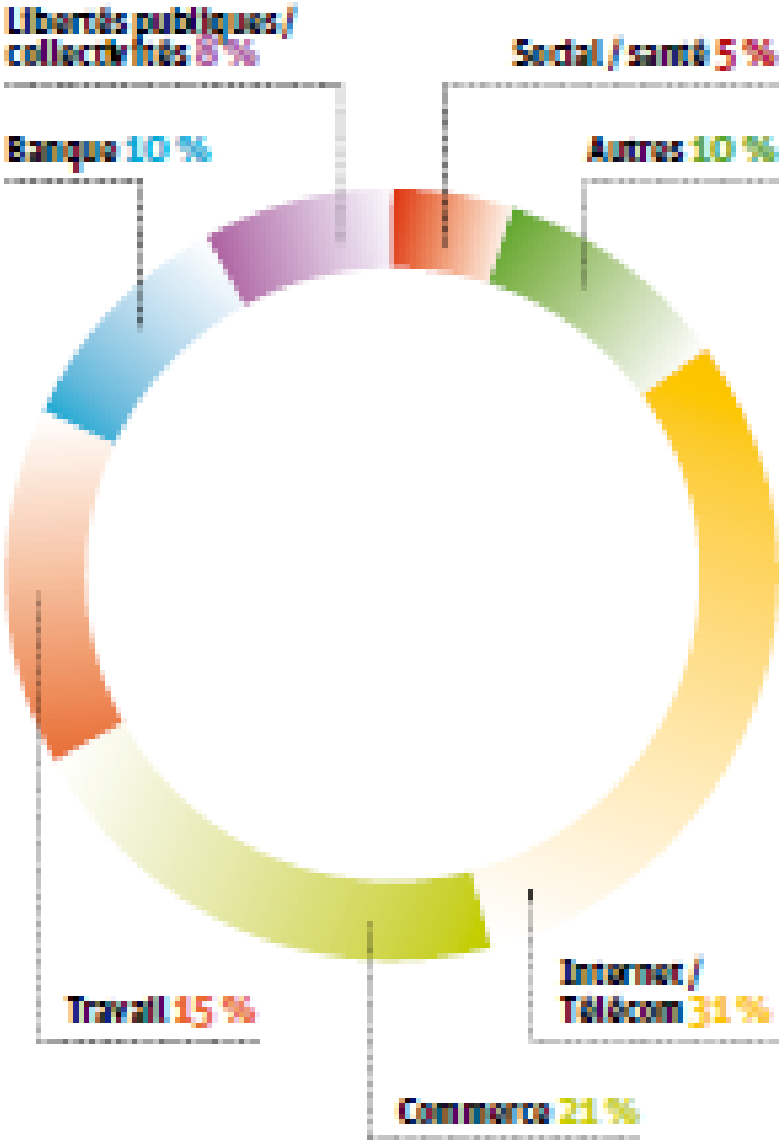
- **6 017 plaintes** (+ 4,9 % par rapport à 2011) dont 44 % reçues en ligne (cnil.fr)
- **458 contrôles** (+ 19 % par rapport à 2011)
- **43 mises en demeure** ≠ sanction
- **13 sanctions**, dont
  - 9 avertissements (pas besoin d'une mise en demeure préalable),
  - **4 sanctions financières** (besoin d'une mise en demeure préalable)



Extrait du rapport d'activité 2012 de la CNIL (page 46).

1.2. Les enjeux et les risques (3/)

Répartition des plaintes par secteur



Extrait du rapport d'activité 2012 de la CNIL

1.2. Les enjeux et les risques (4/)

Les formalités en chiffres

- 10 709 organismes ont désignés un **correspondant**
  (+ 24 % par rapport à 2011)

- 8 946 déclarations relatives à des systèmes de **vidéosurveillance**
  (**+ 49,3 % par rapport à 2011**)

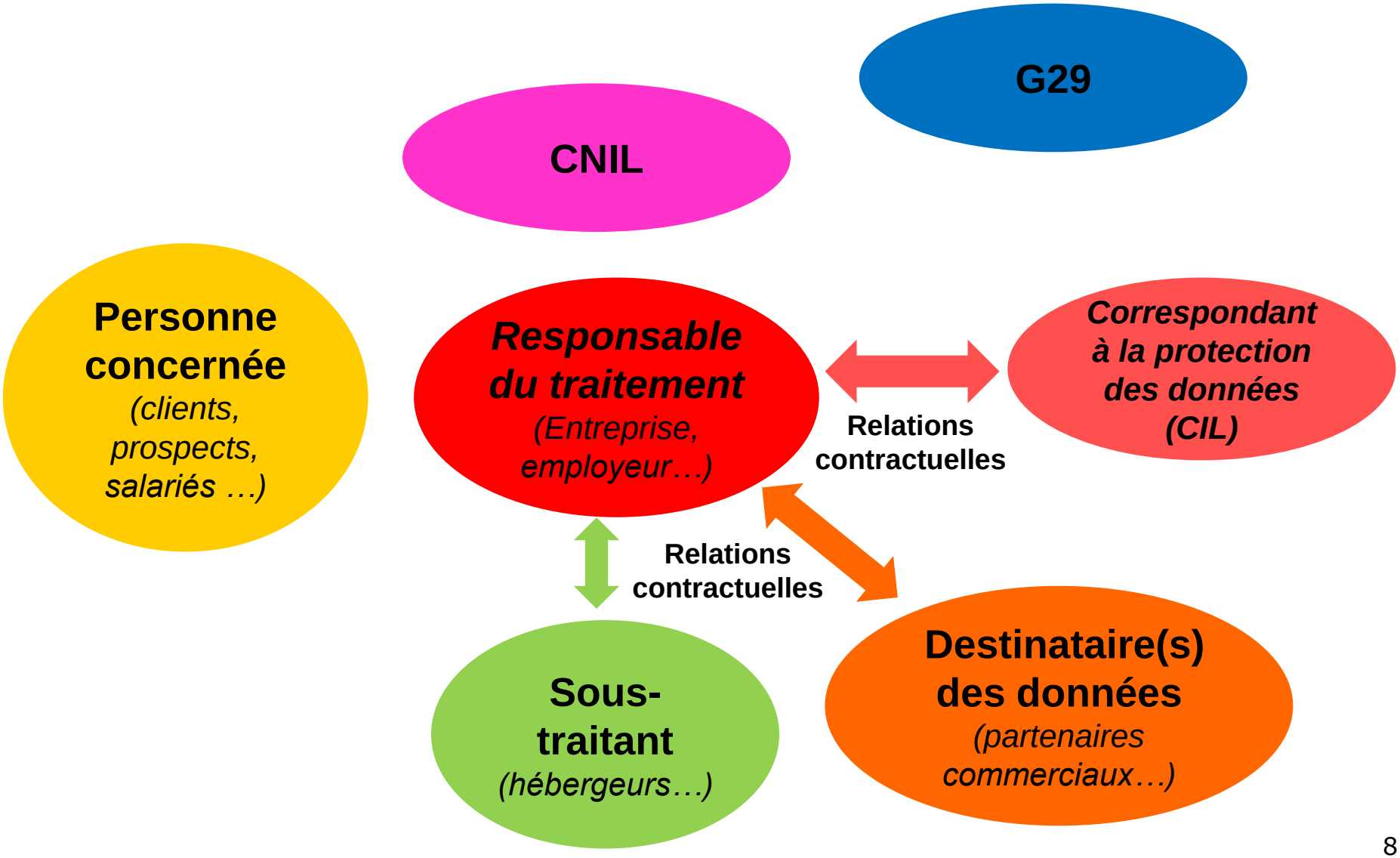
- 5 483 déclarations relatives à des dispositifs de **géolocalisation**
  (**+ 22,3 % par rapport à 2011**)

- 795 autorisations de **systèmes biométriques**
  (**+ 8 % par rapport à 2011**)

- En 2012, la CNIL a traité 88 990 dossiers de formalités (comprenant notamment **48 833 déclarations simplifiées**)

- **93 % des formalités ont été effectuées en ligne en 2012**

1.3. Les acteurs



1.3. Les acteurs (2/)

Obligations à la charge du Responsable du Traitement

- **Recueillir le consentement** de la personne physique concernée (art 7), laquelle doit avoir été préalablement informée de certains éléments

- **Procéder aux formalités** déclaratives (art 22) auprès de la CNIL

1.4. Les formalités

Dispense

Déclaration simplifiée

DÉCLARATION NORMALE

Autorisation

Interdiction

Norme simplifiée 46 =) fichiers RH (courant)

Norme simplifiée 48 =) fichiers clients/prospects

Vidéo-surveillance (couplée d'un système de reconnaissance automatisé (faciale par ex)

PARTIE 2/
PROJET DE REGLEMENT COMMUNAUTAIRE

2.1. CONTEXTE

- **25 janvier 2012 : un texte à l'initiative de la Commission**
  - Proposition de Règlement déposée par la Commission Européenne
  - Faisant suite à plusieurs consultations publiques lancées auprès d'entreprises et d'organismes concernés, ainsi qu'à 2 avis du G29 (mars et octobre 2012)

- **Le choix du Règlement, comme instrument juridique**
  - Le règlement ne nécessite pas de transposition par les Etats-membres (article 288, al. 2 TFUE)
  - Il sera appliqué directement dans toute l'UE, et sans possibilité d'intervention des Etats.
  - Pas de risque de fragmentation juridique
    - Favorise le marché commun

Objectifs

Moderniser le cadre européen de la protection des données personnelles issu de la directive n°95/46/CE du 24 octobre 1995

Harmoniser les règles de protection des données personnelles au sein de l'UE

Améliorer la protection des données des citoyens

Réduire les formalités administratives

Etapes de la procédure d'adoption du projet

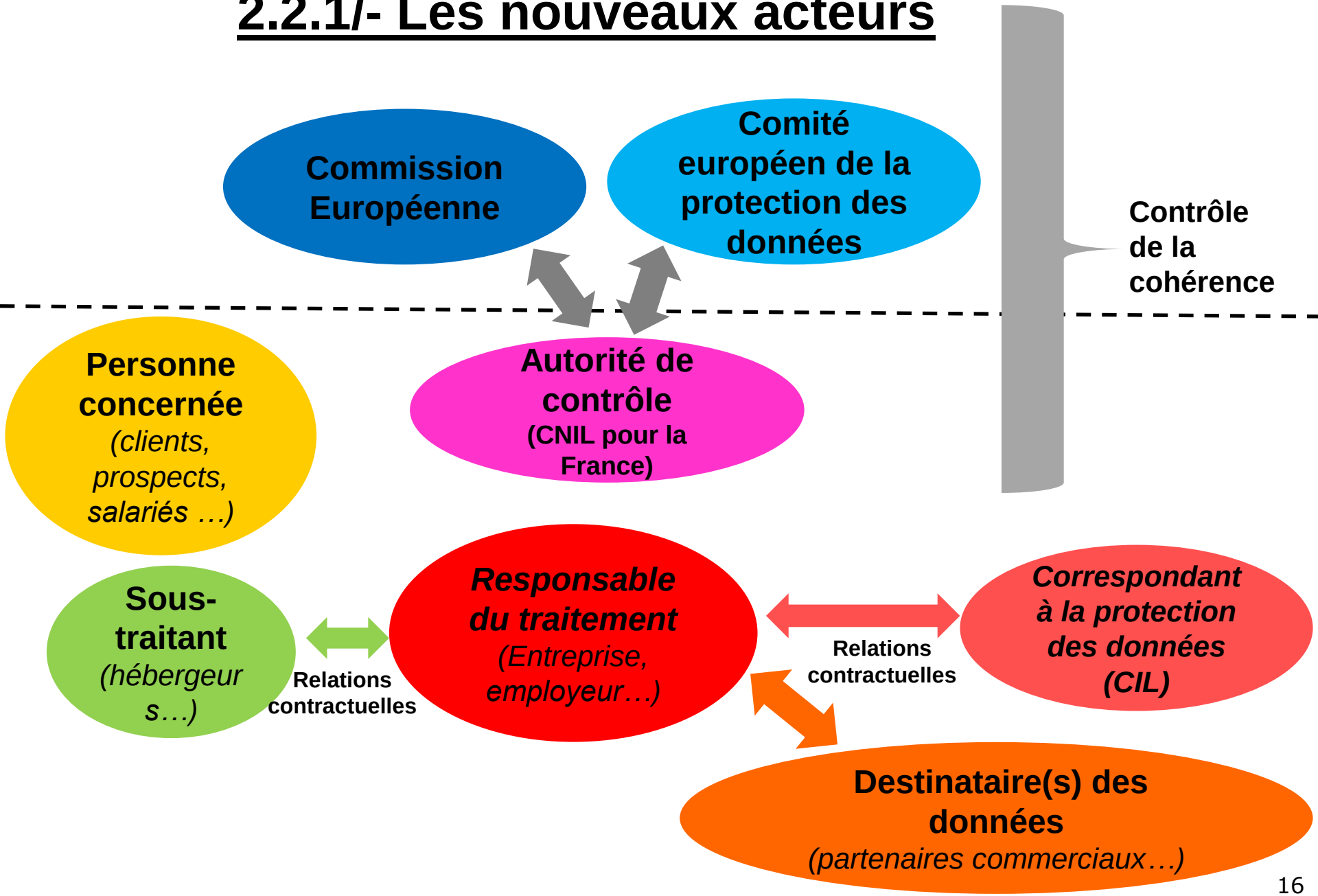
- Proposition de règlement européen élaboré par la Commission Européenne du **25 janvier 2012** (issue d'un large travail de consultation)
- Avis du Groupe de l'Article 29 (groupe des CNIL européennes): **mars et octobre 2012**
- Examen du projet par la commission DAPIX du Conseil de l'UE: rapport rendu **le 31 mai 2013**
- Examen par la Commission LIBE du Parlement Européen pour élaborer une position commune (vote annoncé pour **septembre-octobre 2013**)
- Début du trilogue (Parlement, Conseil de l'UE, Commission) :
  - **Automne 2013**
  - **Vote en 2014?**

2.2. Les principales nouveautés

2.2.1/- LES NOUVEAUX ACTEURS

2.2.2/- LES PRINCIPALES NOUVEAUTÉS DE FOND

2.2.1/- Les nouveaux acteurs



2.2.2/- les principales nouveautés de fond

i. La responsabilité conjointe du traitement et la responsabilité directe du sous-traitant

ii. Une application territoriale plus large

iii. L'instauration d'un « guichet unique »

iv. La simplification des formalités

2.2.2/- les principales nouveautés de fond (2)

v. Les obligations en matière de documentation, de procédure et d'audit

vi. La conformité dès la conception (« privacy by design »)

vii. Le droit à l'oubli numérique

viii. Des sanctions renforcées

i. La responsabilité conjointe du traitement et la responsabilité directe du sous-traitant

- Responsabilité conjointe :
  - Admise par le Règlement (≠ loi informatique et libertés
  - Dans ce cas:
    - un contrat doit définir les obligations de chaque responsable du traitement (art. 24)
    - principe de responsabilité solidaire (art. 77)

- Responsabilité du sous-traitant :
  - Le sous-traitant est personnellement soumis aux obligations du Règlement, notamment en matière de :
    - Étude d'impact (art. 33)
    - Formalité préalable (demande d'autorisation – art. 34)
    - Mise en œuvre de mesures de sécurité (art. 30)

ii. Un champ d'application territoriale plus large

- **La loi informatique et libertés s'applique si**
  - Le responsable du traitement est ***« établi sur le territoire français »***

  ou

  - Le responsable du traitement, est établi hors UE mais ***« recourt à des moyens de traitement situés sur le territoire français »***

    [à l'exclusion des traitement qui ne sont utilisés « *qu'à des fins de simple transit* »]

- **Le Règlement s'applique si**
  - ***« L'établissement »*** du responsable du traitement **<u>ou</u> du sous-traitant**, ayant pour activité le traitement des données concernées, est situé **« *sur le territoire de l'Union* »**.

  ou

  - Le responsable du traitement est établi hors UE, mais ses **activités de traitement sont liées**
    - « ***à l'offre de biens ou de services à ces personnes concernées dans l'Union »*** *ou*
    - ***« à l'observation de leur comportement*** ».

iii. Le dispositif de « guichet unique »

- Une seule autorité de contrôle compétente déterminée sur le fondement du critère de « *l'établissement principal* »

- Etablissement principal : lieu où sont prises les principales décisions quant aux finalités, aux conditions et aux moyens du traitement (art. 4.13).

- Proposition de guichet unique critiquée:
  - Risque d'éloignement entre les citoyens et leur autorité de régulation nationale
  - Risque de forum-shopping

iv. La simplification des formalités

- **Suppression de l'obligation de déclaration préalable auprès de la CNIL**

- **Maintien de la demande d'autorisation pour les traitements suivants** (art.33 et 34) :

  - **Les traitements de données sensibles**
    - Traitements ayant été soumis à une analyse d'impact **qui** a révélé « *un degré élevé de risques particuliers* »
    - Traitements identifiés par la CNIL comme comportant des risques (« ***liste libre*** »)

  - **Les transferts hors UE**

iv. La simplification des formalités (2/)

Sont également soumis à autorisation préalable :

- Les transferts de données hors UE vers des pays n'offrant pas un niveau de protection adéquat ET en l'absence de « *clauses contractuelles types* » ou de « *règles d'entreprises contraignantes* » (BCR) conformes à celle de la Commission Européenne.

- La liste des pays n'offrant pas un niveau de protection adéquat sera établie et mise à jour par la Commission Européenne.

v. Les obligations en matière de documentation, procédure et audit (« *accountability* ») (1/)

- **A la charge du responsable du traitement ET du sous-traitant**

1)- Rédaction d'une documentation (liste) sur l'ensemble des traitements (art. 28)

2)- Formalisation d'un contrat de sous-traitance (avec clauses obligatoires - art. 26, 2)

v. Les obligations en matière de documentation, procédure et audit (« *accountability* ») (2/)

- **A la charge du responsable du traitement :**

1)- Rédaction des procédures à appliquer concernant (art. 12) :

- Les procédures d'information des personnes;
- Les procédures d'information des destinataires des données, des demandes de rectification et d'effacement ;
- Les modalités d'exercice des droits d'accès, de rectification, d'effacement et d'opposition ;

v. Les obligations en matière de documentation, procédure et audit (« *accountability* ») (3/)

2)- Rédaction de <u>règles internes</u> destinées à garantir et démontrer le respect du règlement sur (art. 22):

- Les mesures garantissant la sécurité (physique et logique) des données (art. 22.2.b) ;
- La réalisation d'analyses d'impacts (si requises – art. 22.2 c) ;
- L'accomplissement des formalités préalables (si requises – art.22.2.d)
- La désignation d'un délégué à la protection des données (si requises – art.22.2.e)

v. Les obligations en matière de documentation, procédure et audit (« *accountability* ») (4/)

3)- Mise en œuvre de mesures d'audit (art. 22, 3)

4)- La désignation d'un Délégué à la protection des données

Obligatoire pour les entreprises :

- Soit employant ≥ 250 salariés
- Soit dont l'activité de base « *exige un suivi régulier et systématique des personnes* » (art. 35).

vi. La conformité dès la conception (« privacy by design »)

- Obligation de prise en compte des contraintes réglementaires dans l'élaboration des mesures et procédures techniques et organisationnelles entraînant un traitement de données à caractère personnel.
  - Par exemple en :
    - Limitant le traitement aux données strictement nécessaires à la finalité (minimisation)
    - Limitant leur durée de conservation
    - Empêchant leur accès à un nombre indéterminé de personnes
- Contenu encore flou de cette notion :
  - La Commission édictera des normes plus précises ultérieurement (art. 23)

vii. Droit à l'oubli numérique et à l'effacement des données (1/)

- Principe =) droit à l'oubli pour :
  - Données diffusées lorsque la personne était enfant
  - Données non nécessaires au regard de ses finalités
  - Retrait du consentement ou (si traitement non fondé sur consentement) si le délai de conservation légal est expiré et en l'absence d'autre motif légal justifiant le traitement
  - Données pour lesquelles un droit d'opposition valable a été exprimé
  - Données résultant d'un traitement non conforme au Règlement

vii. Droit à l'oubli numérique et à l'effacement des données (2/)

- Modalités :
  - Effacement :
    - Le responsable du traitement prend « toutes les mesures raisonnables » pour :
      - Effacer lui-même
      - Informer les tiers qui traitent ces données
    - Responsabilité solidaire du responsable du traitement avec les tiers à qui il a autorisé la publication des données
  - Simple limitation :
    - Pendant la période nécessaire à la vérification d'exactitude (si demande d'effacement fondée sur inexactitude)
    - Si nécessité de conserver ces données à des fins probatoires
    - À la demande de la personne (qui refuserait l'effacement et demanderait la simple limitation)
    - En cas d'exercice, par la personne, de son droit à la portabilité de ses données

vii. Droit à l'oubli numérique et à l'effacement des données (3/)

- Exceptions =) pas d'effacement si la conservation des données est nécessaire :
  - À l'exercice de la liberté d'expression (journalisme, expression artistique…)
  - Pour des motifs d'intérêt général dans le domaine de la santé publique (médecine préventive…)
  - À des fins de recherche historique, statistique, scientifique
  - Pour satisfaire à une obligation légale de conservation

viii. Des sanctions renforcées

- Sanction pécuniaire de 250 000 € ou (pour les entreprises) 0,5 % du CA annuel mondial :
  - Absence ou non-conformité des mécanisme permettant l'exercice des droits des personnes (accès, rectification…) (art. 79, 4, a)

- Sanction pécuniaire 500 000 € ou (pour les entreprises) 1 % du CA annuel mondial :
  - Non respect du droit à l'oubli numérique,
  - Absence/insuffisance de l'obligation de documentation (art. 79, 5, c et f);

- Sanction pécuniaire de 1 000 000 € ou (pour les entreprises) 2 % du CA annuel mondial :
  - Absence de mise en place de règles internes (art. 79, 6, e)
  - Omission de désigner un Délégué à la protection des données (si requis) ((art. 79, 6, j):
  - Non respect du droit d'opposition (art. 79, 6, c)

Merci

- Retrouvez l'ensemble des chroniques juridiques de KGA sur Kpratique : www.kpratique.fr et sur votre Iphone grâce à l'application KGA Avocats.
- Suivez l'activité du cabinet en direct sur Twitter et Facebook.
- Contacts :
  - Tél : 01 44 95 20 00

www.kga.fr

www.kpratique.fr