HAAS AVOCATS

Fromont Briens
avocats spécialisés en droit social

Member of Littler GLOBAL

# DRH et DATA

## Cadre légal et moyens d'actions

**Me Gérard HAAS**
Avocat à la Cour

**2017**

**HAAS Société d'Avocats**

32 rue de la Boétie
75008 PARIS

Tel :01.56.43.68.80
Fax : 01.40.75.01.96

contact@haas-avocats.com

www.haas-avocats.com
www.jurilexblog.com

# 1 | Les principes du droit des données personnelles

# A | Les grands principes « Informatique et libertés »

# LA LOI INFORMATIQUE ET LIBERTES

## 1978

**LIL : 1ère version**

Une des premières législation en matière de données personnelles

L'informatique est au service du citoyen

Protection de la vie privée des personnes

## 2004

**LIL : 2ème version**

Définition des « traitements » de données

Extension du rôle de la CNIL (pouvoir d'investigation *a posteriori*)

Extension du droit d'information

Formalités : introduction du régime d'autorisation

## 2016

**LIL : 3ème version**

Renforcement du contrôle de chaque citoyen sur ses données

Renforcement de l'information sur la durée de conservation des données

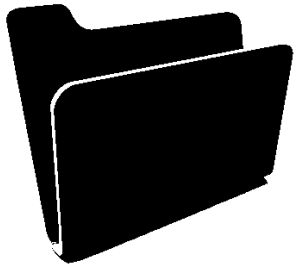
Augmentation des sanctions

HAAS AVOCATS

# LES NOTIONS FONDAMENTALES

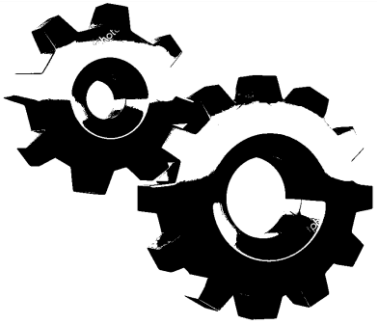
## Donnée personnelle

Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement



## Fichier de données

Tout ensemble structuré et stable de données à caractère personnel



## Traitement de données

Toute opération ou tout ensemble d'opérations, automatisés ou non, portant sur de telles données, quel que soit le procédé utilisé

HAAS AVOCATS

# LES NOTIONS FONDAMENTALES

| | |
|---|---|
| **Identification directe** | **Données d'identification**<br>*Ex. : nom, adresse mail, etc.* |
| **Identification indirecte** | **Données « identifiante »** : personne identifiable lorsqu'un fichier comporte des informations permettant indirectement son identification.<br>*Ex. : n° d'immatriculation, adresse IP (logs de connexion), n° de téléphone, etc.*<br><br>Toutes les informations dont le recoupement permet d'identifier une personne précise. (ex. : une empreinte digitale, l'ADN, une date de naissance associée à une commune de résidence …). |
| **Données anonymisées (irréversible)** | **Données qui ne peuvent plus être reliées à un individu déterminé ou déterminable**<br>Les principes la loi LIL ne s'appliquent pas aux données rendues anonymes.<br>Le passage d'une information anonyme à personnelle est apprécié par le juge (et par la CNIL). |
| **Données pseudonymisées (réversible)** | **Données d'identification remplacée par un pseudonyme** mais qui ne sont pas des données anonymes.<br>Les principes de la LIL s'appliquent à de telles données. |

HAAS AVOCATS

# LES NOTIONS FONDAMENTALES

| IDENTIFIER DES DONNÉES À CARACTÈRE PERSONNEL | IDENTIFIER DES TRAITEMENTS |
|---|---|
| • Numéro de téléphone de personnes<br>• Plaque d'immatriculation<br>• Numéro de poste d'un salarié<br>• Localisation du bureau<br>• Permis de conduire<br>• Badge d'accès aux locaux<br>• Niveau d'étude d'un candidat<br>• Age, Sexe, Activité professionnelle, Situation géographique, Célibataire / Marié | • Fiche de suivi d'un candidat au recrutement / CV<br>• Facturation<br>• Listing papier des employés d'une compagnie d'assurance<br>• Organigramme<br>• Fichier client<br>• Calendrier des congés<br>• Vidéosurveillance<br>• Cloud Computing<br>• Constitution du répertoire d'adresses de la famille |

# LES NOTIONS FONDAMENTALES

**Données sensibles**
Collecte interdite, par principe

**Opinions** politiques et syndicales

Données de **santé**

Données **biométriques**

Données **génétiques**

Orientations **sexuelles**

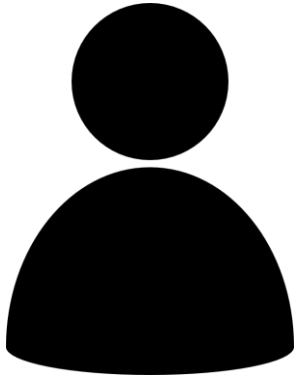
# LES ACTEURS

**Responsable de traitement**

Déterminer les finalités et les moyens du traitement

**Sous-traitant**

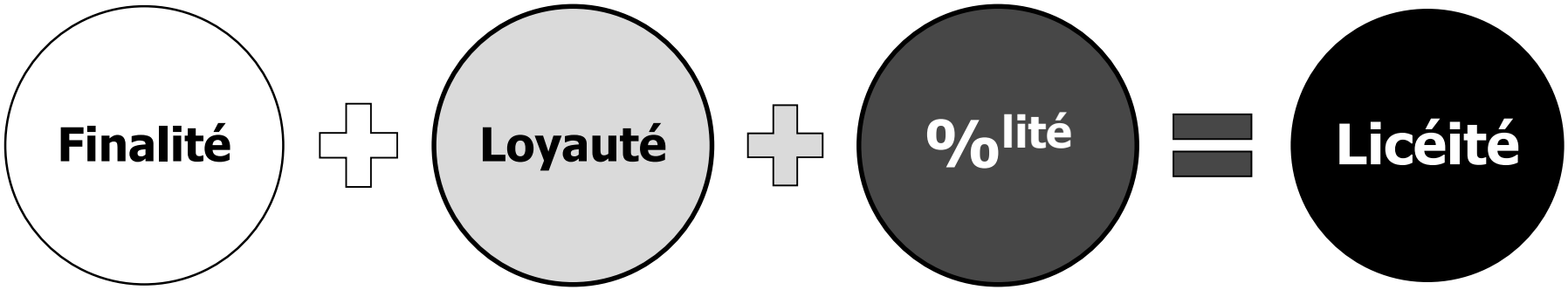
Traite des données pour le compte du responsable de traitement



**Personne concernée**

Personne dont les données personnelles sont traitées

# LES PRINCIPES DIRECTEURS : LICÉITÉ DU TRAITEMENT



# LES PRINCIPES DIRECTEURS : FINALITE

1

Recueil des données pour un **usage déterminé et légitime**

2

Au stade de la **collecte** : recueil de **données en relation avec la finalité** du traitement

3

Au stade du **traitement** : pas de **détournement** de finalité

HAAS AVOCATS

# LES PRINCIPES DIRECTEURS : LOYAUTE ET PROPORTIONNALITE

**Loyauté**

Les données doivent être collectées de manière **transparente**

**Proportionnalité**

Seules les données **nécessaires** à la finalité du traitement doivent être collectées

# LES FORMALITES PREALABLES

**Dispense**

Norme simplifiée
*ou*
Dispense

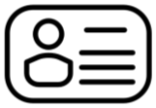
**Déclaration**

Simplifiée
*ou*
Normale

**Autorisation**

Autorisation unique
*ou*
Demande d'autorisation

# LES PRINCIPES DIRECTEURS : INFORMATION DES PERSONNES


Identité du responsable du traitement ou de son représentant

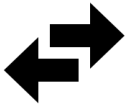

Finalités du traitement


Caractère obligatoire ou non des réponses


Conséquences d'un défaut de réponse


Destinataire(s) des données

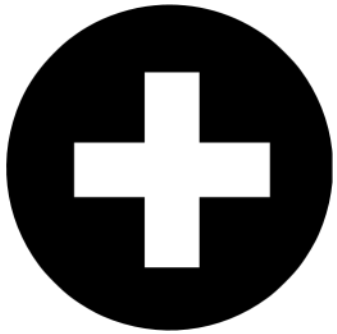

**Droits de la personne**


Transfert de données hors UE


**Durée de conservation** des données

HAAS AVOCATS

# LES PRINCIPES DIRECTEURS : CONSENTEMENT DES PERSONNES



**Exprès**

Par la réalisation d'un **acte positif**

**Eclairé**

La personne doit être **informée** des conséquences de son consentement

# LES PRINCIPES DIRECTEURS : EXCEPTIONS AU CONSENTEMENT

Respect d'une obligation légale

Sauvegarde de la vie de la personne concernée

Exécution d'une mission de service public

Exécution d’un contrat

Réalisation de l'intérêt légitime du responsable de traitement

HAAS AVOCATS

# LA DURÉE DE CONSERVATION

Durée strictement **nécessaire** aux finalités pour lesquelles les données sont collectées et traitées.

**Accès aux locaux & contrôle des horaires**

NS -042

Accès : 3 mois

Suivi du temps de travail : 5 ans

**Géolocalisation des véhicules des salariés**

Deux mois

(recommandation CNIL)

Sauf si :

Utilisées pour optimiser les tournées / à fins de preuve : 1 an

Utilisées pour suivi du temps de travail : 5 ans

**Ecoute et enregistrement des appels**

6 mois maximum

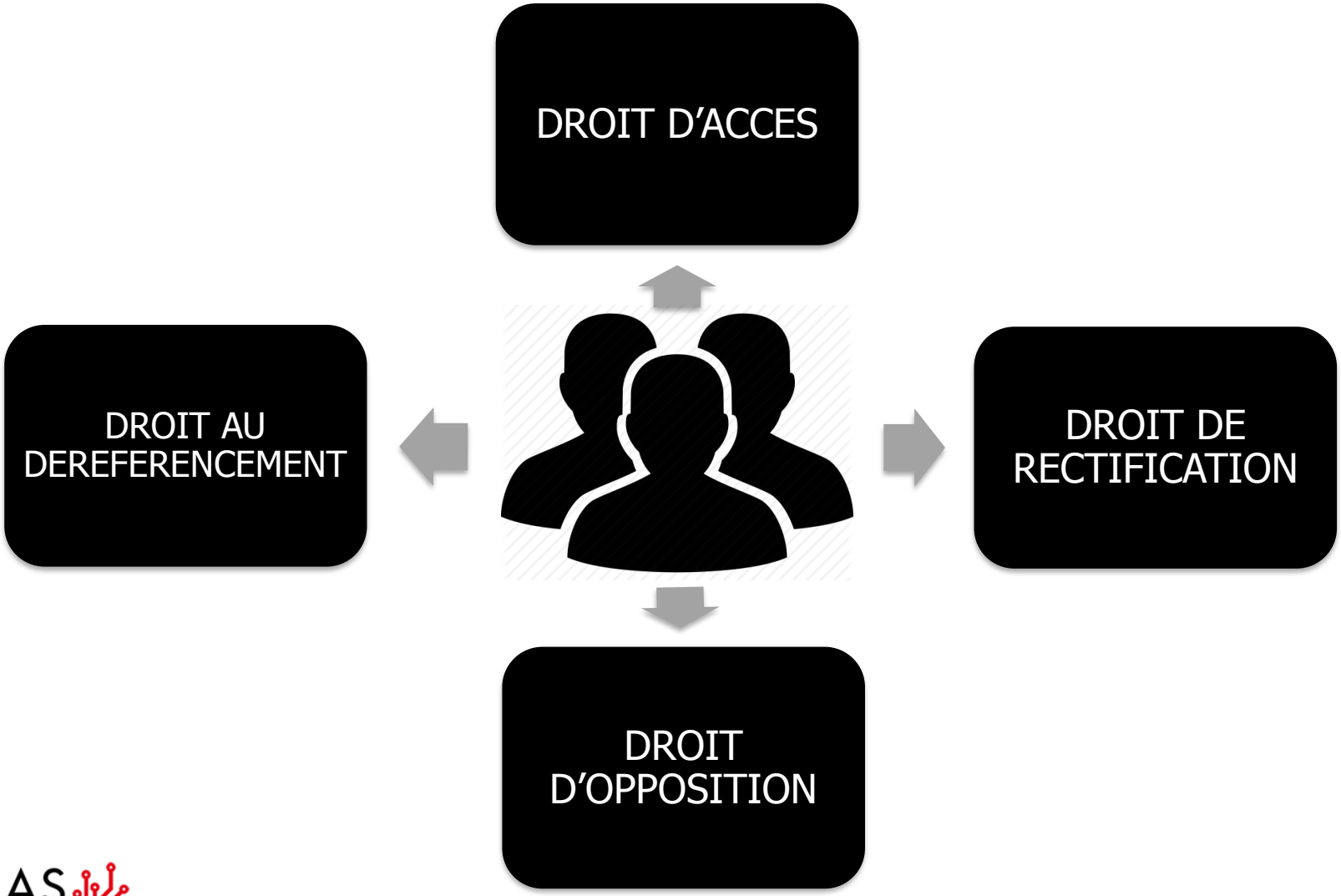
lorsque autorisé

(recommandation CNIL)

1 an pour les documents d'analyse

HAAS AVOCATS

# LES DROITS DES PERSONNES



# QUIZZ

1. Est-ce que le fait de stocker les noms et prénoms, la date de naissance, les coordonnées, le numéro de sécurité sociale, le numéro d'immatriculation de la voiture de la personne est considéré comme un « traitement » de données personnelles ?

2. Peut-on collecter les données sur l'appartenance syndicale des personnes ?

3. Quand la réglementation sur les données personnelles trouve-t-elle à s'appliquer ?

4. Qu'est-ce que le principe de finalité du traitement ? Qu'est-ce que le principe de proportionnalité dans la collecte des données ?

5. Quelle est la différence entre l'information et le consentement de la personne ?

# B | Les nouveautés du RGPD

# LE RÈGLEMENT GÉNÉRAL POUR LA PROTECTION DES DONNÉES

**RGPD : Nouvelle réglementation européenne**

25 mai 2018

Un texte unique pour l'UE

**Objectifs**

Protéger les consommateurs

Assurer la confiance

Responsabiliser les acteurs

HAAS AVOCATS

# RGPD : LES NOUVEAUX PRINCIPES

## Minimisation des données

Proportionnalité

Pseudonymisation

## Autodétermination informationnelle

Renforcement du **consentement** et de l'obligation d'**information**

Nouveaux droits :
**Oubli**
**Portabilité**
**Profilage**

## Privacy by design/default

Mesures techniques et organisationnelles

Protection de la vie privée dès la conception et par défaut

## Accountability

Pouvoir justifier, à tout moment, de sa compliance

HAAS AVOCATS

# DISPARITION DU SYSTÈME DE FORMALITES PREALABLES

**Suppression de l'obligation générale de déclaration préalable**

Mais maintien du régime d'autorisation et de consultation préalables

**Obligation générale de tenue de registre des activités de traitement**

# RGPD : TRANSFERT HORS UE

**Clauses contractuelles types**

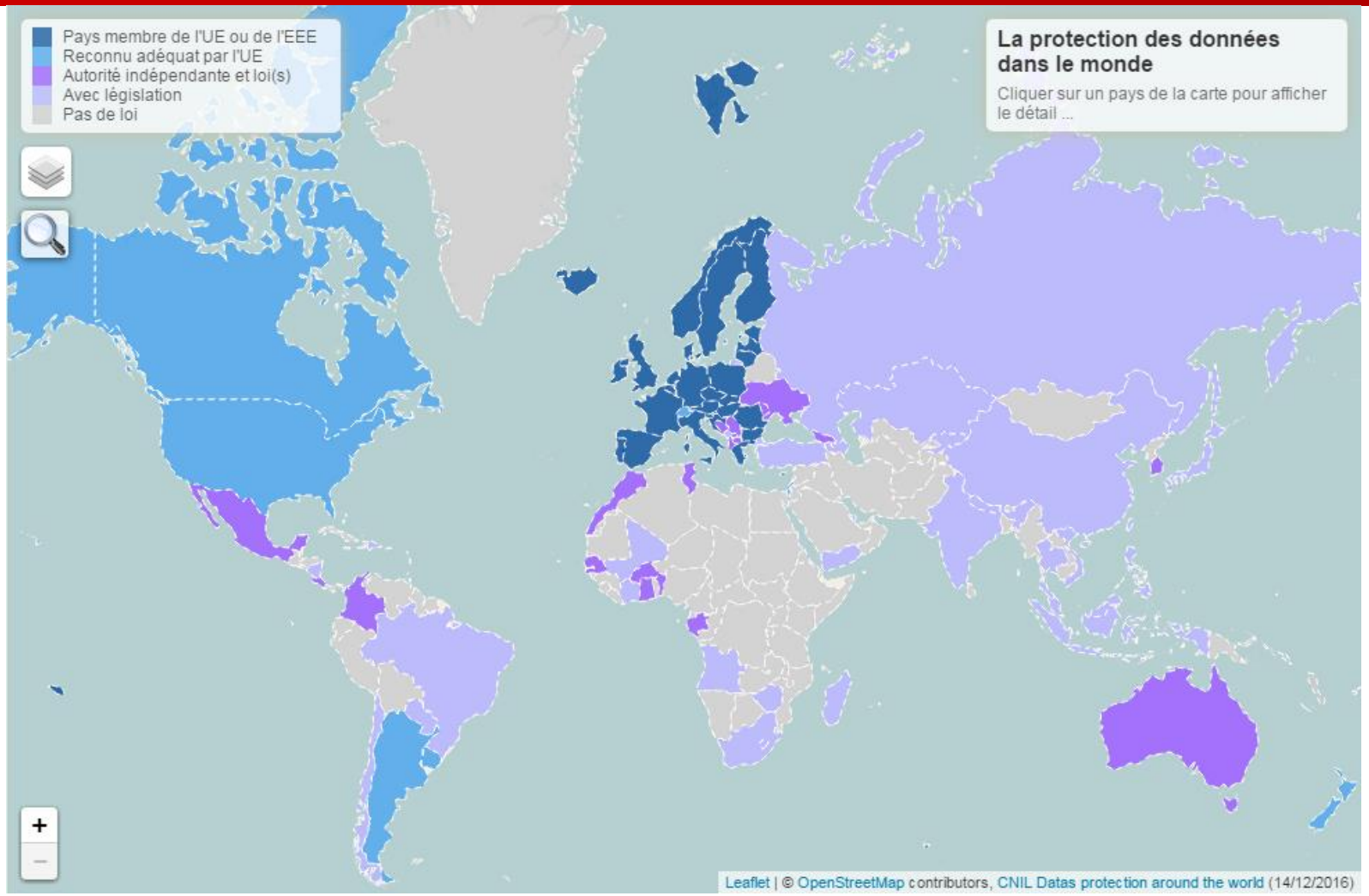
**Règles d'entrepr. contraignantes**

**Code de conduite Certifications**

**Décision d'adéquation de la Commission UE**

Privacy Shield

# FLUX TRANSFRONTIÈRES ET PROTECTION ADÉQUATE

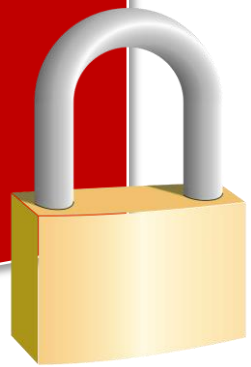


# C | La sécurité

# LA SÉCURITÉ À L'ÈRE DU RGPD : PRIVACY BY DESIGN

Mesures **techniques et organisationnelles**

Assurer d'un **niveau approprié de sécurité des données**

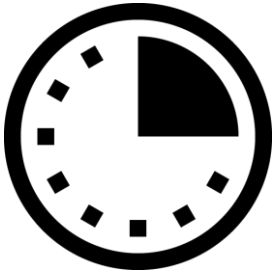


**Protection de la vie privée par défaut et dès la conception du traitement**

# LA SÉCURITÉ À L'ÈRE DU RGPD : EXEMPLES DE MESURES

Pseudonymisation et chiffrement des données

Garantir la confidentialité, l'intégrité, la disponibilité et la résilience des SI



Moyens permettant de rétablir rapidement la disponibilité des données en cas d'incident

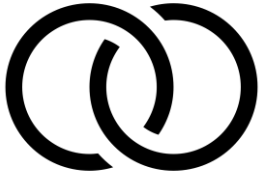
Procédure visant à tester, à analyser et à évaluer

# LA SÉCURITÉ ET LE RECOURS A LA SOUS-TRAITANCE

Action sur **instructions** du responsable

Présenter des **garanties suffisantes** pour la sécurité et la confidentialité

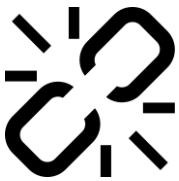
**Contractualisation** des obligations du sous traitant (sécurité et de confidentialité)



**Coresponsabilité** notamment en matière de sécurité des données

HAAS AVOCATS

# LA SÉCURITÉ À L'ÈRE DU RGPD : NOTIFICATION D'UNE FAILLE



**Violation de données**

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

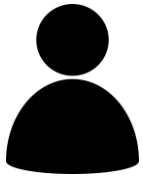
**Notification à la CNIL**
72 heures

Descriptions de la **nature** de la violation

**Coordonnées** du DPO

**Conséquences** probables

**Mesures** prises ou envisagées



**Communication à la personne concernée**
Meilleurs délais

En cas de **risques élevés** pour les droits et libertés

En des **termes clairs et simples**

HAAS AVOCATS

# LA SÉCURITÉ : EXEMPLES

**DROPBOX**

**13 octobre 2014**

Publication de 7 millions de mots de passe

Mise en cause de services annexes

**CDISCOUNT**

**20 septembre 2016**

Conservation en clair 5000 numéros de cartes bancaires

Avertissement CNIL

**YAHOO**

**23 septembre 2016**

Piratage de 500 millions de comptes

Données en clair : noms, adresses, n° de téléphone, etc.

# D | La compliance

# COMMENT ÊTRE « COMPLIANT » ?

**Réaliser une PIA**

Tester

Anticiper

Prouver

**Nommer un DPO**

Compétence & indépendance

Chef d'orchestre de votre compliance


**Programme de compliance**

Registre à jour

Plan de formation
Mesures techniques et organisationnelles

Plan de crise (sécurité)

# LA SÉCURITÉ À L'ÈRE DU RGPD : TECHNIQUEMENT

Sécurité des postes de travail

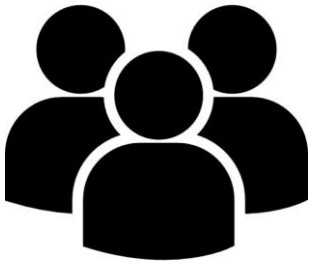
Authentification des utilisateurs

Sauvegarde, continuité et maintenance

Sécurité des locaux et des serveurs

Archivage, anonymisation, chiffrement

# LA SÉCURITÉ : ASSURER UNE GOUVERNANCE EN INTERNE

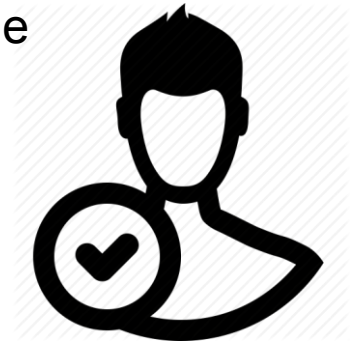


Charte « Utilisateur des Systèmes d'Information »

Politique de durée de conservation des données et d'archivage

Politique de gestion des incidents liés au SI

Charte « Administrateur des SI »



Politique d'habilitation

# ÊTRE « COMPLIANT » : QUELS BÉNÉFICES ?

## Susciter la confiance et l'adhésion

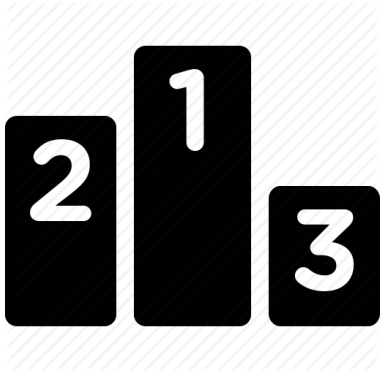
Confiance des clients et des partenaires

Développement du projet

## Sécurité juridique

Renforcer juridiquement son projet

Valoriser ses données




## Avantage concurrentiel

Se démarquer positivement

Faire partie d'un label / Obtenir une certification

HAAS AVOCATS

# NON-RESPECT DE LA RÉGLEMENTATION DONNÉES PERSO.

**Risques économiques et opérationnels**

Fichier non déclaré
= sans valeur

Suspension de l'activité

**Sanctions importantes**

Administratives (CNIL)

Pénales
5 ans & 300 000 €

Civiles

**Risques « réputationnels »**

Perte de confiance des clients et des partenaires

Mauvaise image

HAAS AVOCATS

# AUGMENTATION DES SANCTIONS ADMINISTRATIVES


**150 000 €**

**3 000 000 €**

**10 000 000 € ou 2% CA**

Manquement à : Privacy by design, PIA, etc.

**20 000 000 € ou 4% CA**

Manquement aux droits des personnes

# SANCTIONS : EXEMPLES


15 décembre 2016

**20 000 €**

*Collecte illégale de données sensibles (défaut de consentement exprès)*


27 avril 2016

**150 000 €**

*Combinaison massive de données non consentie (pour ciblage publicitaire)*

*Défaut d'information et de recueil du consentement (données sensibles)*

*Conservation illimité de l'adresse IP*


10 mars 2016

**100 000 €**

*Manquement aux droits d'opposition des personnes et de suppression des données (déréférencement)*

12 mai 2017

**Ordonnance de référé**

*Déréférencement sous 15 jours*

HAAS AVOCATS

# QUIZZ

1. Qu'est-ce que le droit à l'oubli ? Qu'est-ce que le droit à la portabilité ?

2. Que signifie « CIL » ? Que signifie « DPO » ?

3. Quelles sont les missions du DPO ?

4. Quel outil permet de procéder à un flux transfrontières en direction des Etats-Unis d'Amérique ?

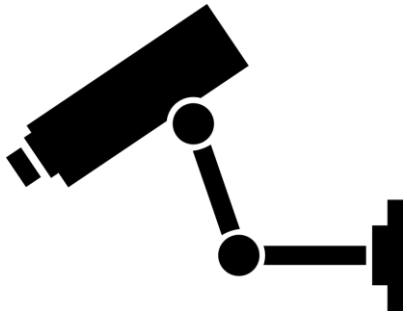
5. Quels sont les deux principaux pouvoirs de la CNIL ?

HAAS AVOCATS

# 2 | Les traitements RH

# TYPOLOGIES DE TRAITEMENTS RH

**Gestion du personnel**



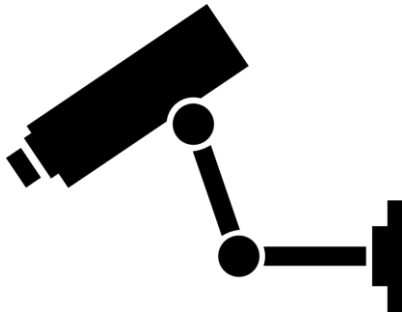
**Contrôle d'accès aux locaux**

# TRAITEMENTS DE GESTION DU PERSONNEL

- Gestion administrative du personnel et du dossier professionnel
- Gestion des carrières, de la mobilité, et des formation des personnels
- Gestion des opérations de recrutement
- Gestion des administrateurs réseau
- Gestion de la téléphonie
- Gestion des paies et accessoires

- Gestion des retraites, mutuelles et prévoyances obligatoires
- Gestion des élections professionnelles et des relations avec les instances de représentation du personnel

# TRAITEMENTS DE CONTRÔLE



- Dispositifs de géolocalisation
- Accès aux locaux et contrôle des horaires (badges, biométrie)
- Utilisation d'internet et de la messagerie
- Vidéosurveillance sur les lieux de travail
- Suivi du temps de travail
- Gestion des dossiers disciplinaire
- Prévention et suivi des maladies professionnelles et des accidents du travail

# TRAITEMENTS RH : LE REFERENTIEL REGLEMENTAIRE

Différentes délibérations de la CNIL encadrent certains traitements mis en œuvre dans le cadre de la gestion des ressources humaines :

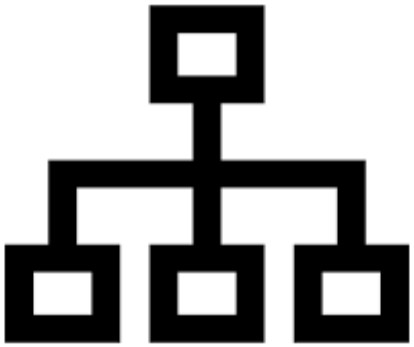
- **Dispense n° 2** - pour la gestion des rémunérations mis en œuvre par les personnes morales de droit privé
- **Norme Simplifiée n°46** - pour la gestion du personnel
- **Autorisation unique AU-004** - pour les dispositifs d'alerte professionnelle
- **Recommandation** - relative modalités d'archivage

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

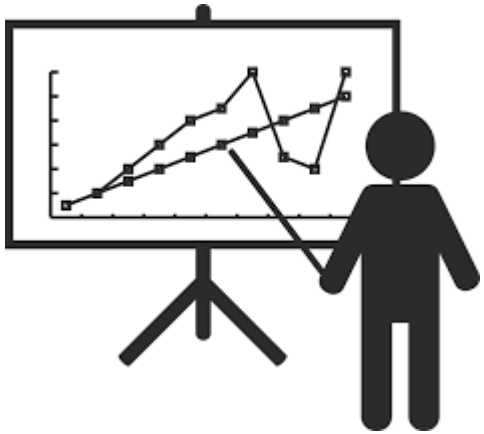
HAAS AVOCATS

# TRAITEMENTS RH : FOCUS SUR LA NORME SIMPLIFIÉE 46

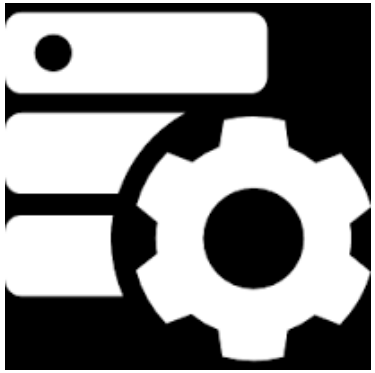
## Gestion du personnel



**Finalités du traitement**



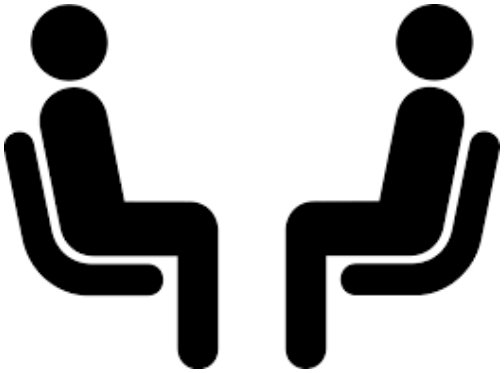
**Destinataires des données**



**Données concernées**

# TRAITEMENTS RH : FOCUS SUR LA NORME SIMPLIFIÉE 46

## Finalités du traitement

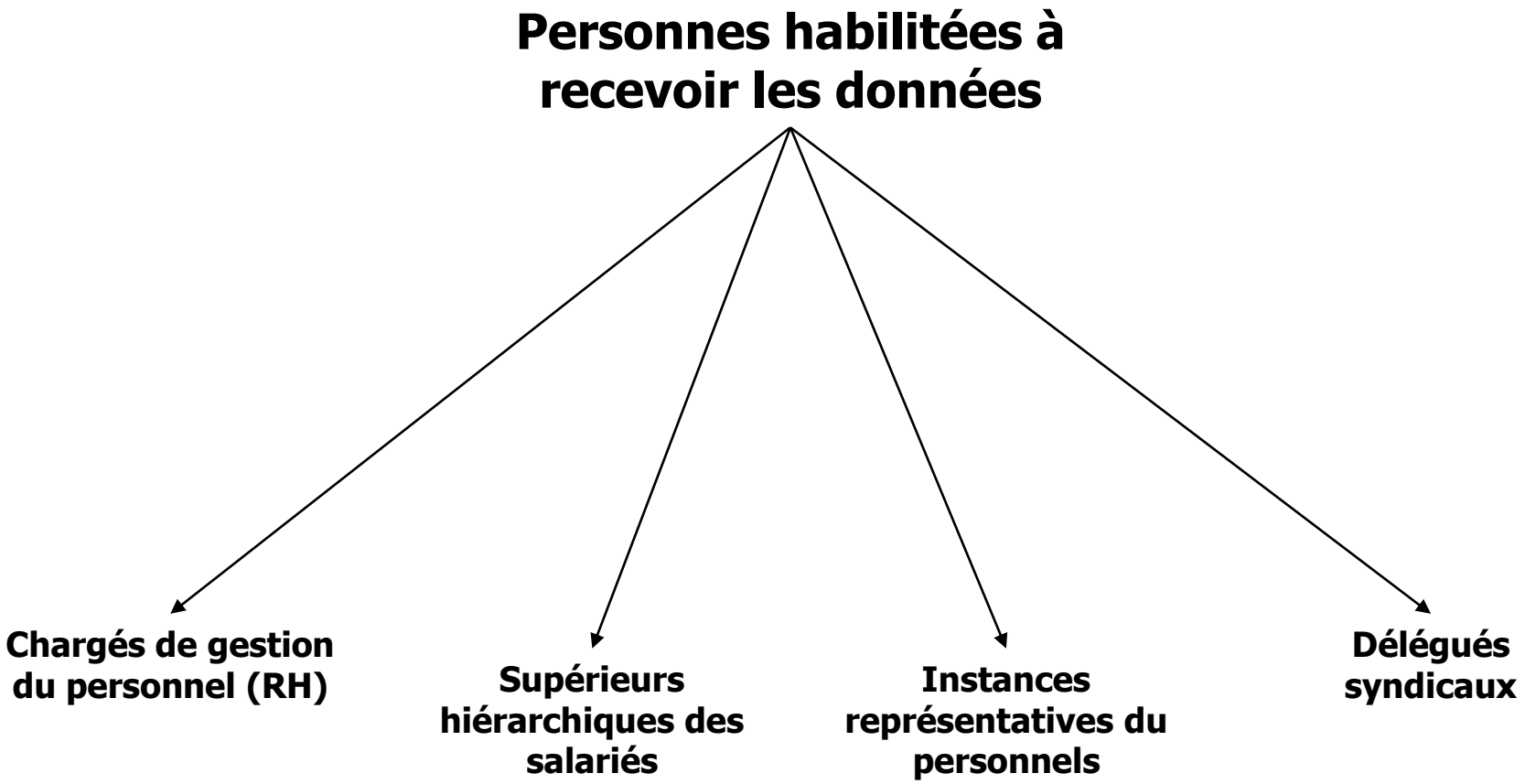


**Gestion administrative du personnel**

**Mise à disposition d'outils informatiques**

**Organisation du travail Formation du personnel**

# TRAITEMENTS RH : FOCUS SUR LA NORME SIMPLIFIÉE 46

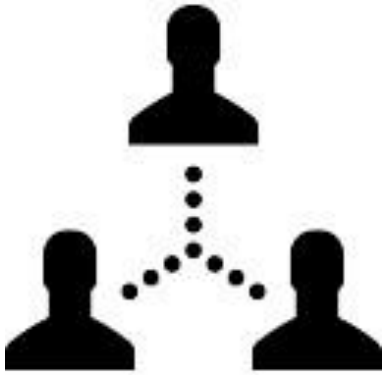


# TRAITEMENTS RH : FOCUS SUR LA NORME SIMPLIFIÉE 46

## Données concernées

**Identification de l'employé**

**Gestion administrative de l'employé**

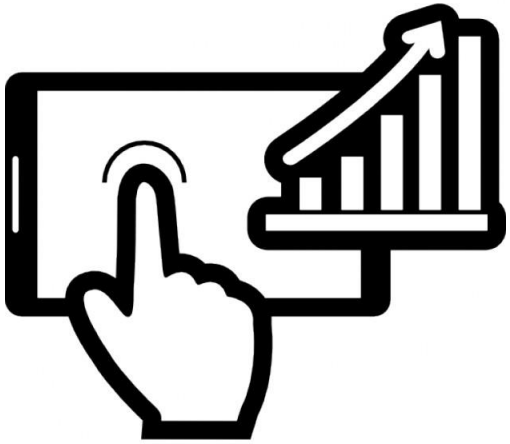


**Organisation du travail**

**Action sociale et représentation du personnel**

HAAS AVOCATS

# TRAITEMENTS RH : RECRUTEMENT DU PERSONNEL



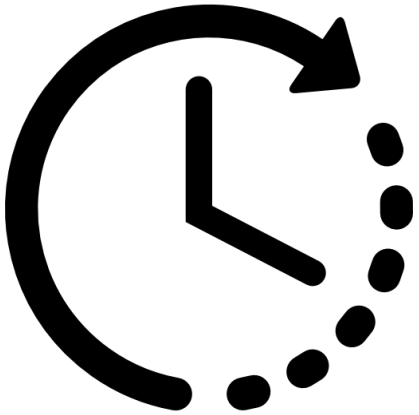
## Données collectées

Ne servir qu'à évaluer les capacités du candidat

## Accès aux données

Limité

Contrôlé



## Durée de conservation

Maximum 2 ans après le dernier contact si le candidat n'en demande pas la destruction

Une fois employé, le temps de sa présence et jusqu'à 5 ans après son départ

HAAS AVOCATS

# TRAITEMENTS RH : POINTS DE VIGILANCE

- Formalités préalables CNIL / Registre des traitements
- Consentement / information des personnes concernées
- Finalité(s) et pertinence, adéquation, proportionnalité des données collectées
- Données sensibles
- Sous-traitants et transferts hors UE
- Durée de conservation
- Sécurité / confidentialité

HAAS AVOCATS

# MERCI POUR VOTRE ATTENTION !

**Avez-vous des questions ?**