



**<< DITES-MOI, POURQUOI EXACTEMENT
AVEZ-VOUS BESOIN DE MON NUMÉRO
D'ASSURANCE SOCIALE POUR ME VENDRE
UN HOT-DOG? >>**

La protection des données personnelles

**Large Scale Data Management
27 novembre 2015**

Agenda

» Principes de la loi Informatique et Libertés

- > Notions essentielles
- > 5 règles d'or
- > Focus sur quelques principes fondamentaux
 - + Finalité
 - + Données particulières
 - + Droits des personnes
 - + Formalités préalables
 - + Transferts hors de l'UE

» Les perspectives

- > versus l'Europe, le monde et demain

» Exemple de réutilisation

» Questions/réponses



Notions essentielles

» Donnée personnelle



« Toute information relative à une personne physique identifiée ou qui peut être identifiée, **directement ou indirectement**, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres »

⇒ Pour déterminer si une personne est identifiable, il faut considérer l'ensemble des moyens dont dispose le responsable des traitements ou toute autre personne pour l'identifier

Notions essentielles

» Traitement de données à caractère personnel



Dossier Personnel

Ensemble stable et structuré

Toute opération portant sur des données à caractère personnel que ce soit sur des données sous format papier ou numérique

Exemples d'opération :

- « la collecte, l'enregistrement, l'organisation, la conservation, la modification, l'extraction, la consultation, l'utilisation,
- la communication par transmission, le rapprochement ou l'interconnexion,
- ainsi que le verrouillage, l'effacement ou la destruction »

Notions essentielles

» Les acteurs du traitement

- **Le responsable des traitements** détermine la finalité et les moyens de mise en œuvre
- **La personne chargée du traitement** traite les données en raison de sa fonction
- **Le destinataire**, toute personne habilitée à recevoir communication de ces données
- **La personne concernée** par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement

Exemples

PDG d'une entreprise française

Service Informatique, sous-traitants, ...

L'administration fiscale, URSSAF, auditeur ...

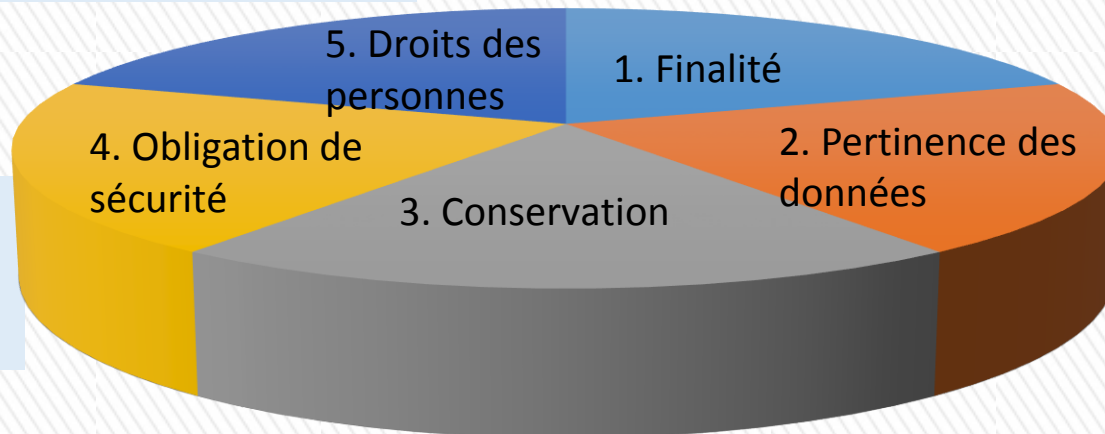
Le salarié, le client, l'utilisateur d'un service

Principes – 5 règles d’or

Respect des droits d’information, d’accès, de rectification et d’opposition

Finalités déterminées, explicites et légitimes

Confidentialité, Intégrité des données



Données adéquates, pertinentes, proportionnelles et exactes

Conservation limitée selon délai défini

Finalité

» « *Les données sont collectées pour des finalités déterminées, explicites et légitimes* »

Exemples :

- Gestion de la paie
- Administration du personnel
- Gestion des remboursements des frais professionnels

» « *et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités* »



Tout détournement de finalité est passible de sanctions pénales :
300 000 € et 5 ans d'emprisonnement



Finalité

» Exemple de détournement

- Utilisation du fichier des salariés pour de la prospection commerciale

Exception :

« Un traitement ultérieur à des fins statistiques, ou de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et procédures (...) et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées »

Données particulières



» Leurs collecte et traitement sont INTERDITS sauf exceptions limitatives par autorisation de la CNIL :

- Données sensibles : origines raciales, ethniques, opinions politiques, philosophiques ou religieuses, ou appartenance syndicale des personnes, les mœurs, les données relatives à la santé et à la vie sexuelle
- Données relatives aux infractions, condamnations et mesures de sûreté
 - ✓ Uniquement mis en œuvre par les juridictions, auxiliaires de justice, autorités publiques
- Le NIR (Numéro d'Inscription au Répertoire National d'Identification des Personnes Physiques)
 - ✓ Utilisation essentiellement limitée à la sphère «social-travail»
- Les données biométriques

Droit d'information



- » Pour être **loyale**, la collecte doit s'accompagner d'une information précise (RT, finalité, destinataire, ...)

- » Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée :
 - ✓ L'information doit lui être fournie dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données

 - ✓ Ces dispositions ne s'appliquent pas lorsque la personne concernée est déjà informée ou quand son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche.

Droit d'opposition

» Toute personne physique a le droit de s'opposer pour des motifs légitimes

- sauf si obligation légale ou si le droit d'opposition a été écarté par l'acte réglementaire autorisant le traitement

» Prospection commerciale : Droit à la tranquillité

- Toute personne a le droit de s'y opposer sans motif légitime
- Prospection commerciale par voie électronique : **Consentement préalable** – OPT IN

Formalités préalables

» Déclaration :

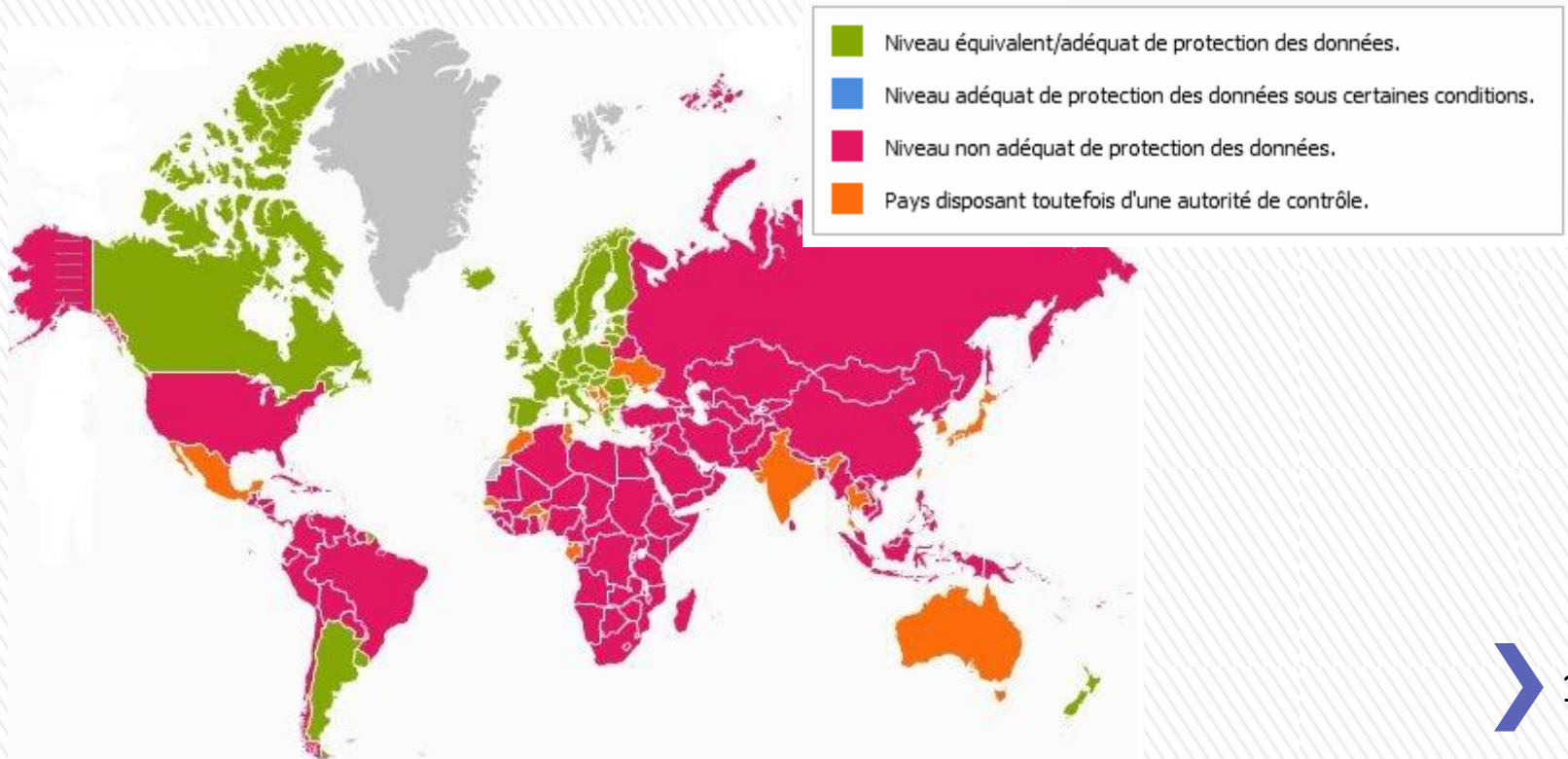
- Pour être licite, les traitements de données personnelles doivent faire l'objet d'une déclaration à la CNIL :
 - ✓ Si l'organisme a désigné un Correspondant Informatique et Libertés (CIL), pas de déclaration

» Autorisation :

- Pour être mis en œuvre, les traitements sur les catégories de données suivantes doivent faire l'objet d'une autorisation préalable de la CNIL
 - ✓ Données particulières cf. page 9
 - ✓ Traitements susceptibles du fait de leur nature, de leur portée ou de leurs finalités, **d'exclure des personnes** du bénéfice d'un droit, d'une prestation ou d'un contrat
 - ✓ Traitements comportant des appréciations sur les difficultés sociales des personnes
 - ✓ Traitements automatisés ayant pour objet **l'interconnexion de fichiers**

Transfert hors UE

» Interdiction de transférer des données personnelles vers un pays « non adéquat »



Perspective : Quels avantages ?

» « *La protection des données nous donne un avantage attractif. Il faut construire la confiance sur des principes de proportionnalité et de maîtrise des données* » (Axelle Lemaire – Salon Big Data mars 2015)

» Principes reconnus internationalement

- Europe :
 - ✓ Article 8 de la charte des droits fondamentaux
 - ✓ Directive européenne n°95/46/CE du 24 octobre 1995
- OCDE :
 - Lignes directrices sur la protection de la vie privée et les flux transfrontières
- Pays avec une législation équivalente :
 - ✓ Argentine, Israël, Canada, Suisse, Nouvelle-Zélande, Uruguay

Perspective : renforcement

» Française : Loi numérique

- CNIL : plus de prérogatives – renforcement des sanctions
- Réaffirmation du secret des correspondances
- Droit à l'oubli des mineurs
- Directives des personnes décédées, ...

» Europe : Projet de Règlement

- Accountability
- Sanction : 3 millions d'Euros ou % CA mondial
- Privacy by design
- PIA – Preliminary Impact Assessment
- Notification des violations
- DPO – Data Protection Officer
- Portabilité, référencement, renforcement du consentement,

Exemple de réutilisation statistique

- » Le service des routes souhaite utiliser les données de localisation des téléphones mobiles pour élaborer des actions d'information de modération de trafic et réduire les accidents
 - Evaluation de la compatibilité de la nouvelle finalité :
 - ✓ Finalité : sécurité routière
 - pas de décision à l'égard des personnes
 - nouvelle finalité différente et non prévisible
 - sensibilité des données de géolocalisation des téléphones et donc des personnes
 - Mesures de protection :
 - ✓ Anonymisation, « séparation fonctionnelle »
 - ✓ Information, sécurité,...

Merci pour votre attention



Anne Goliro
Expert protection des données personnelles
agoliro@live.com

