Deloitte.

Petit déjeuner des PME et des start-up

RGPD: Grands principes et premières leçons près d'un an après son entrée en vigueur

Dr. Aurélien Rocher – Deloitte Legal Manager – 1 mars 2019

Le RGPD et ses grands principes

Le Règlement européen sur la protection des données personnelles

Adoption et entrée en vigueur de la législation européenne sur la protection des données

Le **Règlement général sur la protection des données dit RGPD** (Règlement européen 2016/679/UE relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données) est entré en vigueur le 25 mai 2018.

Le RGPD uniformise le cadre juridique du traitement des données à caractère personnel dans l'Union Européenne afin d'assurer une meilleure protection contre toute utilisation illicite ou illégitime.

Dans certains cas, le RGPD s'applique également aux entreprises hors UE si elles traitent des données à caractère personnel de personnes concernées qui se trouvent dans l'UE.

L'enjeu est considérable: le non-respect du RGPD peut entraîner non seulement des amendes allant jusqu'à 4 % du chiffre d'affaires annuel mondial, mais aussi un risque réputationnel.

Le Règlement européen sur la protection des données personnelles

Vue d’ensemble – principes directeurs

1. Application territoriale élargie

Le RGPD s’applique aux sociétés situées en dehors de l’UE qui traitent de données à caractère personnel collectées dans l'UE.

2. Droits étendus pour les individus

Le RGPD confère des droits étendus aux individus, afin de contrôler la manière dont leurs données personnelles peuvent être collectées, utilisées, transférées ou supprimées.

3. Principe de responsabilité des entreprises

Les entreprises doivent être en mesure de démontrer que leur organisation est conforme au RGPD, avec une obligation de documentation étendue.

4. Notification en cas de violation de données à caractère personnel

Les violations des données personnelles doivent être signalées à l’autorité de contrôle compétente et/ou aux personnes concernées.

5. Protection des données dès la conception et par défaut

Mise en œuvre des mesures appropriées, à tout moment, pour garantir, par défaut, le traitement des données à caractère personnel au regard de chaque finalité spécifique.

6. Mise en application du RGPD & Sanctions

Les autorités sont habilitées à infliger des amendes allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel global d’une société, le montant le plus élevé étant retenu.

Le Règlement européen sur la protection des données personnelles

RGPD – Champ d'application territorial (Article 3)

Définition du cadre territorial et extraterritorial d'application du RGPD (dans l'UE et en dehors de l'UE) - l'article 3 détermine le champ d'application territorial et, partant, le champ d'application des lois nationales sur la protection des données.

Application du RGPD:

1. Critère de rattachement au lieu d'établissement du responsable du traitement ou d'un sous-traitant

Le RGPD s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'UE, que le traitement ait lieu ou non dans l'UE.

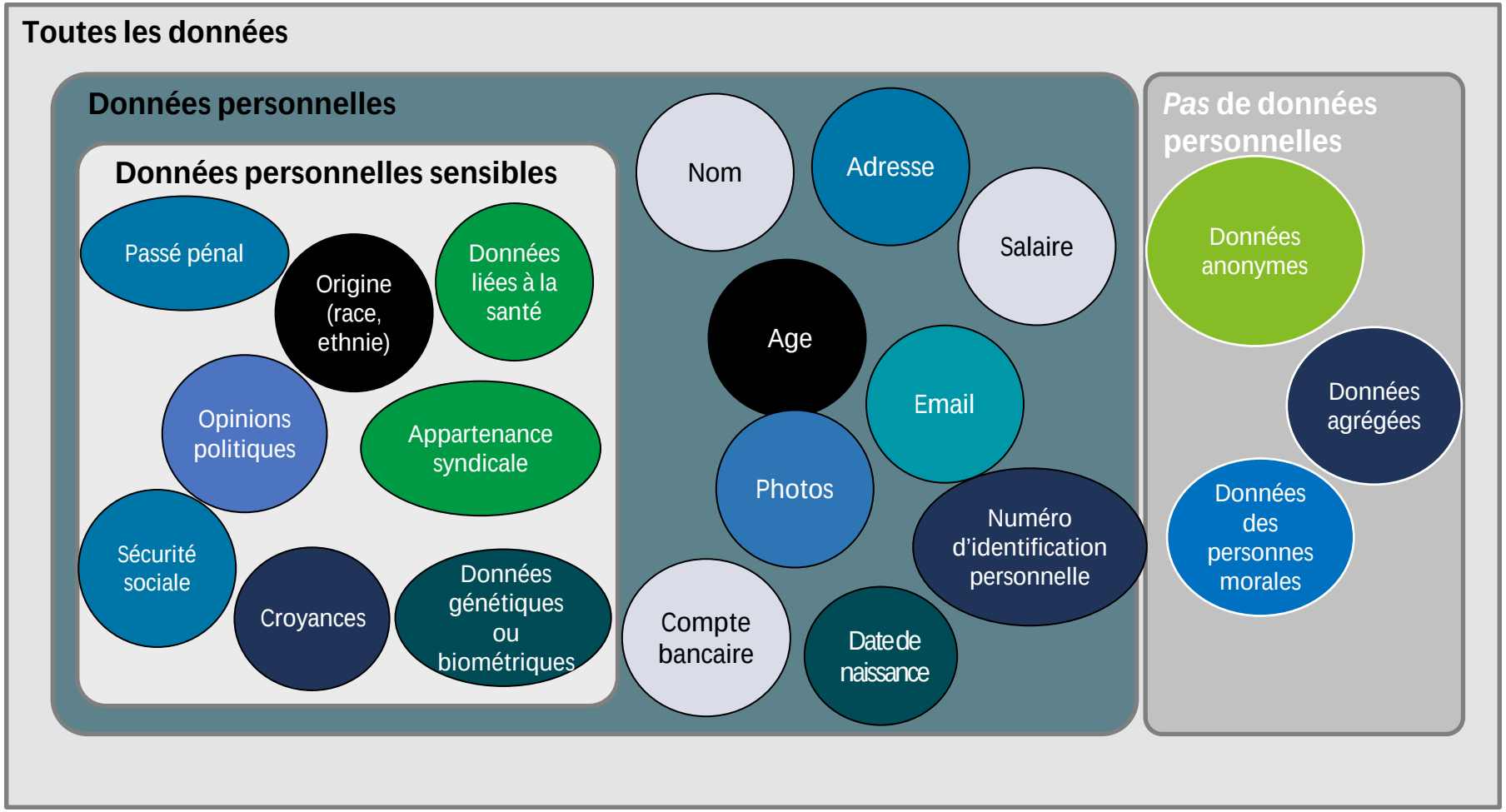
2. Critère de rattachement du lieu de situation des personnes concernées

Le RGPD s'applique au traitement des données à caractère personnel des personnes qui se trouvent sur le territoire de l'UE par un responsable du traitement ou un sous-traitant en dehors de l'UE, lorsque les activités de traitement sont liées à :

- **l'offre de biens ou de services** à ces personnes, dans l'UE
- **suivi du comportement** de ces personnes, dans la mesure où il s'agit d'un **comportement qui a lieu au sein de l'UE**

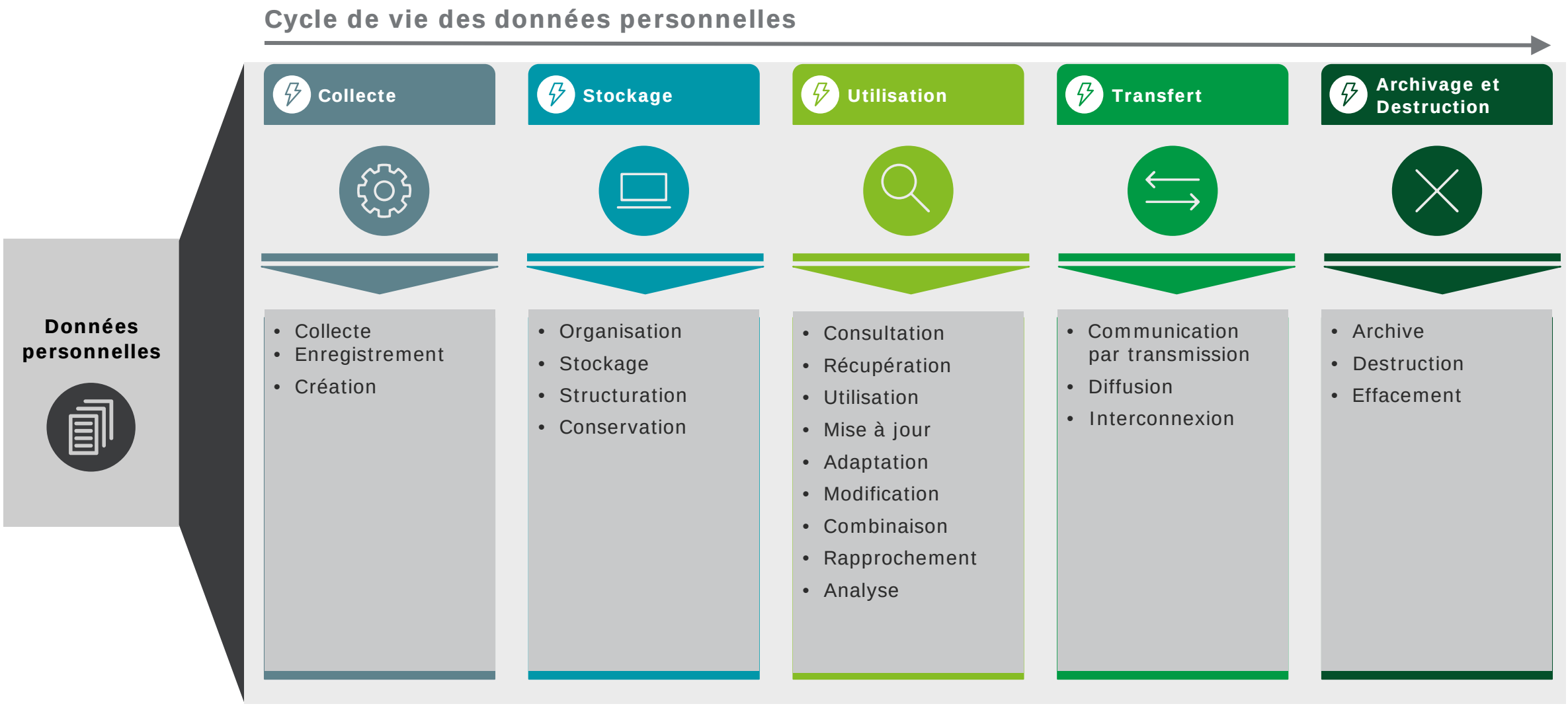
Le Règlement européen sur la protection des données personnelles

«Données personnelles» - Qu'est-ce que cela signifie?



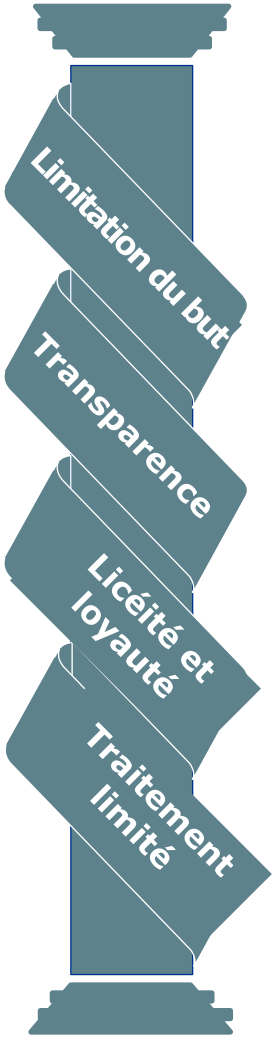
Le Règlement européen sur la protection des données personnelles

Traitement des données personnelles



Le Règlement européen sur la protection des données personnelles

Principes du RGPD



01 Limitation du but

Les données personnelles doivent être collectées pour des finalités **déterminées, explicites et légitimes** et ne pas être traitées ultérieurement de manière incompatible avec ces finalités.

02 Transparence

Traitement des données personnelles d'une manière **transparente** en relation avec la personne concernée.

03 Licéité & loyauté

Le traitement des données personnelles doit être licite, en respectant sa finalité initiale.

04 Traitement limité des données

Le traitement des données personnelles doit être **adéquat, pertinent et limité** à ce qui est vraiment nécessaire en relation avec le but du traitement**.**

05 Exactitude des données

Les données personnelles doivent être **exactes** et, si nécessaire, **mises à jour**.

06 Conservation limitée

Les données personnelles doivent être conservées dans une forme qui permet l'identification des individus pour une période n'excédant pas celle nécessaire au but poursuivi.

07 Integrité & confidentialité

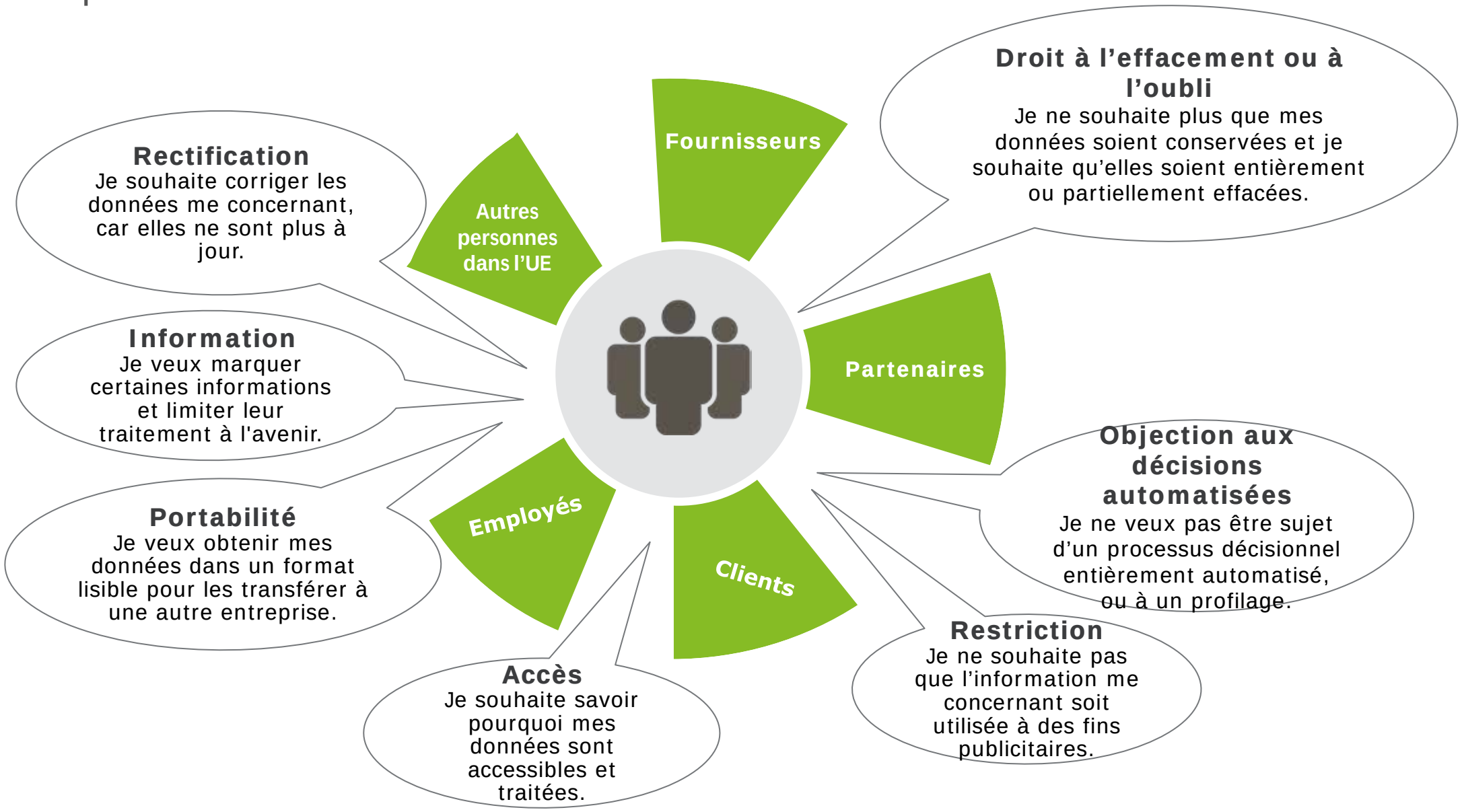
Le traitement des données personnelles doit s'effectuer de manière à assurer une protection adéquate contre tout traitement non autorisé ou illicite et contre toute perte, destruction ou détérioration accidentelle, par des mesures techniques ou organisationnelles appropriées.

08 Responsabilité

Le responsable du traitement est responsable du respect des principes de protection des données et est en mesure d'en démontrer le respect.

Le Règlement européen sur la protection des données personnelles

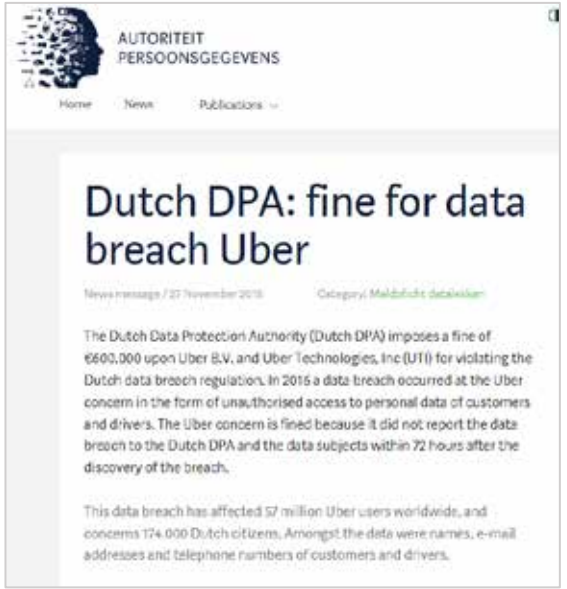
Droits des personnes concernées



Le RGPD: premières leçons près d'un an après son entrée en vigueur

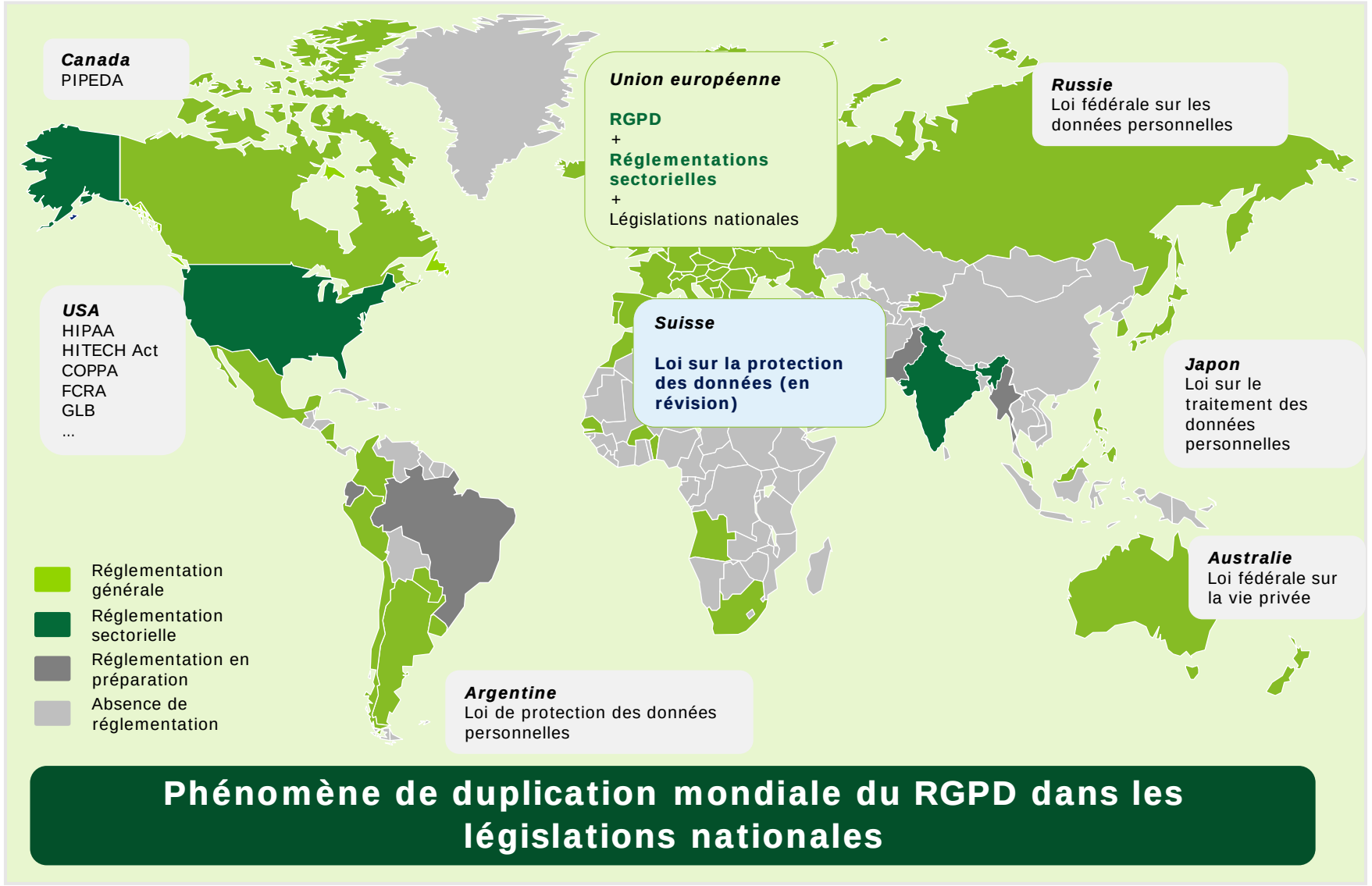
Leçon 1

Le RGPD s’applique aussi aux entreprises hors Union Européenne

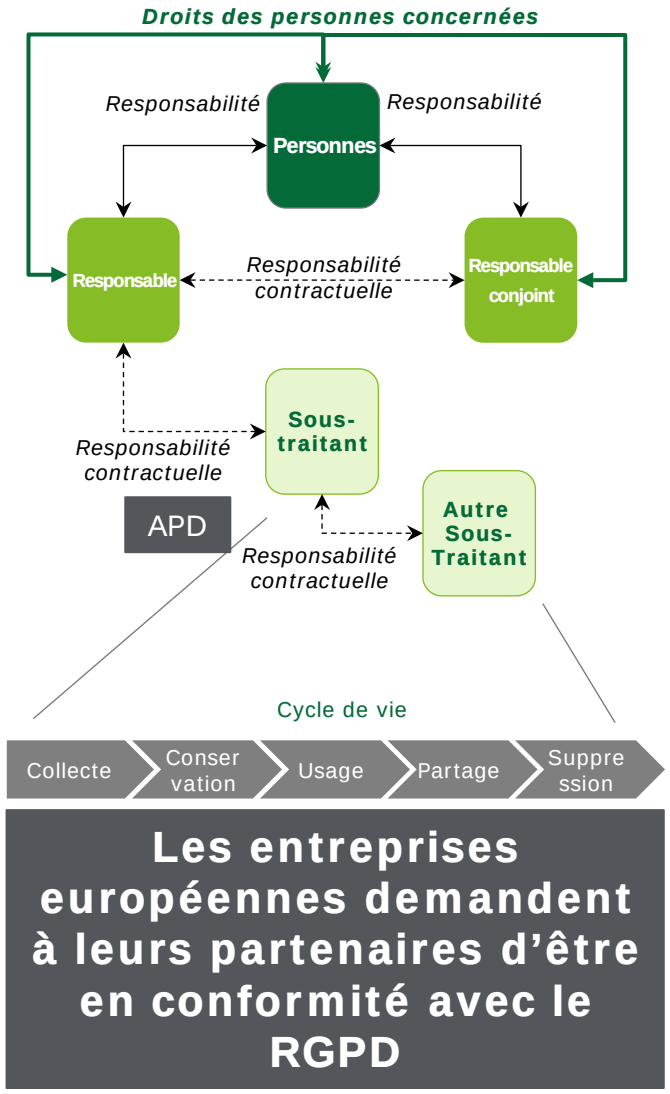


Leçon 1

Le RGPD s’applique aussi aux entreprises hors Union Européenne



Phénomène de duplication mondiale du RGPD dans les législations nationales



Les entreprises européennes demandent à leurs partenaires d’être en conformité avec le RGPD

Leçon 1

Le RGPD s’applique aussi aux entreprises hors Union Européenne

- Succursales ou filiales dans l’Union européenne ?
- Clientèle ou partenaires commerciaux dans l’UE ?
- Gestion de données relatives à des résidents UE ?

- Réglementation américaine?
- Brexit?
- Réglementation chinoise ou coréenne ?
- Autres régions du monde sans réglementation propre?

- Clauses de confidentialité insuffisantes
- Clauses de protection des données dans les contrats clients/fournisseurs
- Convention de traitement des données personnelles

Leçon 2

Le RGPD ne s’applique pas qu’aux multinationales

Champ d’application très large du RGPD impactant toutes les entreprises européennes

- Dynamique de professionnalisation de l’usage des données
- Principe de responsabilité des entreprises (programme de conformité)
- Gravité et portée des atteintes aux données personnelles ne dépendant pas de la taille des entreprises
- Importance des sanctions applicables
- Sensibilisation croissante des individus

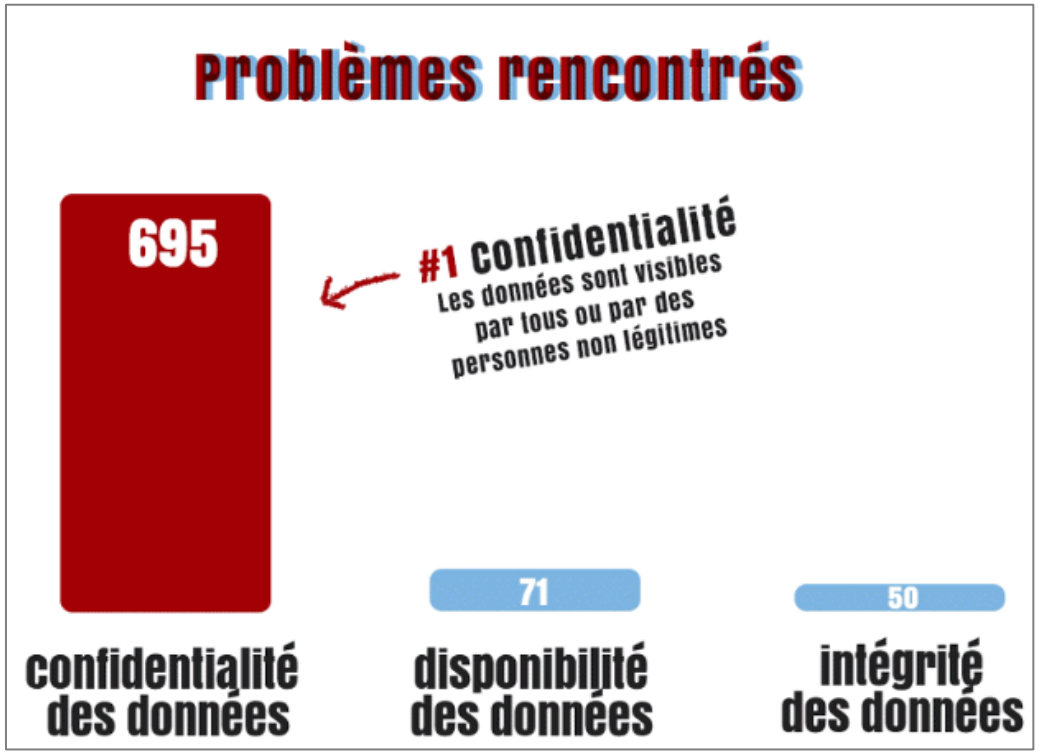
Des sanctions sont aussi prononcées contre des PME

Mais aussi…

- Un hôpital portugais
- Un entrepreneur autrichien et son système de video-surveillance
- Des start-up dans plusieurs pays

Leçon 3

Avec le RGPD, les personnes exercent leurs droits à la protection des données



Extrait rapport d'actualité CNIL

Hausse importante des plaintes portées devant les autorités compétentes

- Premières statistiques officielles des autorités compétentes montrent une hausse importante des plaintes émises par les individus
- Divers sondages révèlent que plusieurs entreprises reçoivent des demandes de la part de clients, anciens employés, employés de partenaires et prestataires, de candidats à des recrutements
- Ces demandes des individus nécessitent la mise en place de procédures et d'une structure appropriée de gouvernance

Leçon 4

Avec le RGPD, la sécurité des données est un enjeu crucial pour les entreprises

1 Prendre conscience

Avoir un degré raisonnable de certitude qu'un incident de sécurité qui a compromis des données personnelles s'est produit.

Enclenche le délai de **72 heures** pour la *notification*

2 Evaluation objective

Lors de l'évaluation du risque, il faut tenir compte à la fois de la probabilité et de la gravité du risque, ainsi que de l'impact sur les droits et libertés des personnes concernées.

3 Notification

RISQUE – Notification de la violation aux autorités chargées de la protection des données.

GRAND RISQUE – Notification de la violation aux autorités chargées de la protection des données et aux personnes concernées

4 Documentation

Documenter toute atteinte à la protection des données personnelles, y compris :

1. **Les faits relatifs à l'atteinte à la vie privée ;**
2. **Ses effets ; et**
3. **Les remèdes entrepris.**

La formation restreinte de la CNIL a prononcé une sanction de 250.000 euros à l'encontre de la société pour avoir insuffisamment sécurisé les données de ses clients effectuant une commande en ligne à partir de son site internet.

Une part importante des violations de données personnelles est liée à des actes malveillants

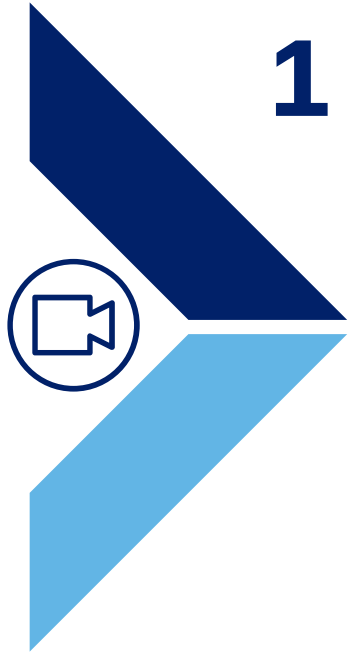
Leçon 5

Avec le RGPD, l’éducation des employés est essentielle

Pour les employés très exposés (RH, marketing, IT), importance d’une formation accrue

- Gouvernance des données personnelles (délégué à la protection des données; conseil d’administration)
- Gestion des demandes des personnes (droit d’accès, droit à l’effacement etc.)
- Mise en place et suivi de la structure de conformité
- Violation des données personnelles (Data breach)
- Suivi et actualisation des relations contractuelles avec les clients, fournisseurs et partenaires de l’entreprise
- Usage des outils technologiques

Synthèse
Conformité au RGPD et compétitivité



1

- Politiques et déclarations de protection des données personnelles
- Registre des activités de traitement
- Modèle d'évaluation des risques
- Procédure de gestion des droits des personnes concernées
- Procédure de gestion des violations de données personnelles
- Procédure d'évaluation des sous-traitants
- Actualisation des modèles de contrats

Mise en place d'une gouvernance des données – Documentation

- Programme de conformité
- Evaluation adaptée aux besoins "gap assessment"

2

- Définition technique et juridique d'une politique de rétention et de suppression des données
- Standardisation des procédures de traitement des demandes des personnes concernées
- Mise en oeuvre d'une capacité de réponse aux cas de violations des données personnelles
- Prise en considération systématique et non pas épisodique des problématiques de données personnelles

Mise en oeuvre opérationnelle de la gouvernance des données

- Approche pluridisciplinaire
- Traduction des exigences du RGPD dans la sphère technologique

Deloitte.

Merci pour votre attention !

Dr. Aurélien Rocher
Manager
Tax & Legal
Deloitte SA, Geneva

Tel.: +41 58 279 8536
Mobile: +41 79 876 9610
E-mail: arocher@deloitte.ch