18e RENCONTRES NATIONALES DE L'UNAFO

CO-AGIR AU CŒUR DES TERRITOIRES

Nancy 27 & 28 novembre 2018

Protection des données personnelles :

face aux enjeux du RGPD, comment accompagner le secteur dans sa mise en conformité ?

Magali VALLET
Conseillère en politiques sociales - DIUS
Déléguée à la protection des données de l'USH

Le règlement européen relatif à la protection des données personnelles :

Quels impacts pour les organisations ?

réunion du 28 novembre 2018

Département des politiques sociales
DPO - USH

1 Les grands principes du RGPD et les enjeux pour les organisations

Pourquoi un règlement à l'échelle européenne ?

- Un règlement général sur la protection des données (RGPD) car :
  - ✓ Nécessité d'une harmonisation des législations des états membres de l'Union européenne dans un contexte d'accroissement des échanges, y compris des échanges de données à caractère personnel
  - ✓ Le déploiement des outils numériques, des big data, open data et objets connectés, qui brassent de plus en plus de données à caractère personnel, rendent indispensable la mise en place d'un cadre permettant un niveau de protection élevé
- Un règlement qui s'inscrit dans le prolongement de la directive européenne 95/46/CE du 24 octobre 1995, et dans lequel on retrouve les grands principes de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Un règlement directement applicable sans aucune transposition, avec un délai de deux ans pour se mettre en conformité (date butoir : 25 mai 2018)

Un changement de méthode …

- Le RGPD réduit très fortement le régime de déclaration préalable au profit d'une mise en responsabilité des responsables de traitement (« accountability ») et prévoit la prise en compte de la protection des données dès la conception des outils (« privacy by design », « privacy by default »).

- Des analyses d'impacts pour la protection des données (AIPD) devront par ailleurs être menées pour les traitements les plus sensibles et / ou à grande échelle.

- Le RGPD renforce le droit des personnes, la responsabilité des sous-traitants et relève le niveau des sanctions.

- Les correspondants I&L deviennent des délégués à la protection des données (« DPO »).

… mais des principes fondamentaux qui demeurent

- Si certaines dénominations changent, les principes fondamentaux de la loi I&L demeurent :

LES PRINCIPES À APPLIQUER PAR LES ORGANISMES HLM

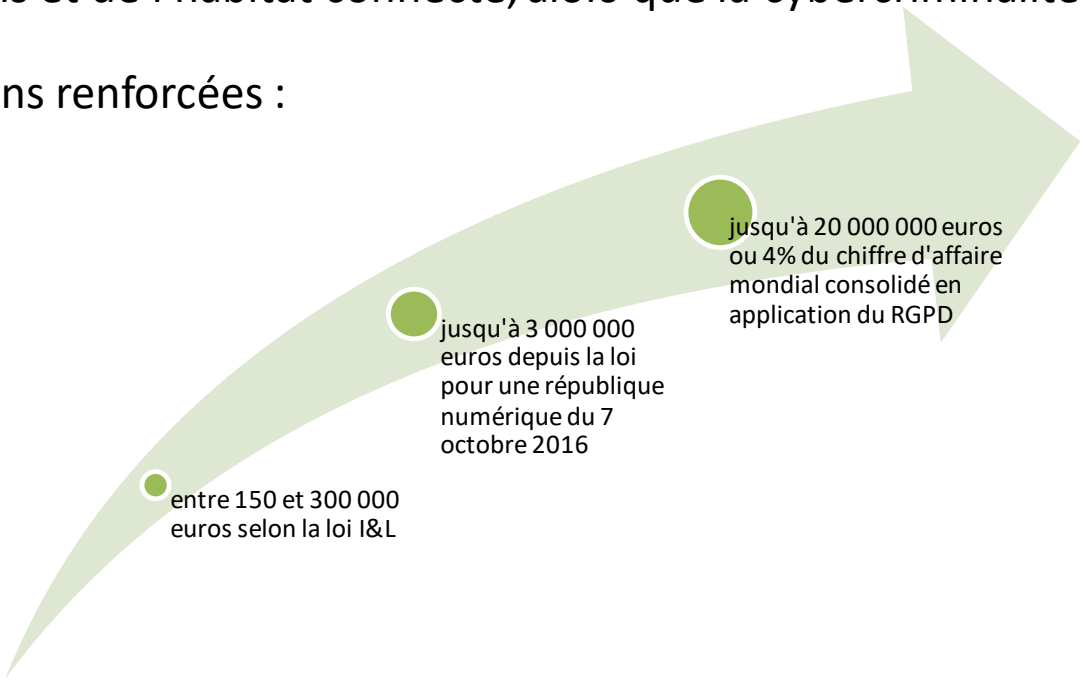
- **Licéité, loyauté et transparence** : des données obtenues et traitées de manière licite, loyale et transparente.
- **Limitation des finalités** : des données collectées pour des finalités déterminées, explicites et légitimes et qui ne sont pas utilisées ultérieurement de manière incompatible avec ces finalités
- **Minimisation des données** : des données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies.
- **Exactitude** : des données exactes et si nécessaire tenues à jour.
- **Limitation de la conservation** : des données conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (Exceptions : archives publiques, recherche scientifique & historique).
- **Intégrité et confidentialité** : il s'agit de prendre toutes mesures, d'ordre technique ou organisationnel, afin d'assurer la sécurité des données et de prévenir toute détérioration, perte ou destruction.
- **Mesures permettant la mise en application du droit des personnes** (Droit d'opposition, d'accès de rectification, de limitation…).

Le renforcement des droits des personnes

- Obligation de clarté et de transparence pour les mentions d'information.
- Le consentement doit être non seulement libre et spécifique mais également éclairé et univoque. Il doit se manifester par une déclaration ou un acte positif et clair.
- Droit à l'information concernant la possibilité de retrait du consentement.
- Délais raccourci à 1 mois pour répondre à toute demande de droit d'accès.

Les enjeux de la mise en conformité

- La mise en conformité et son suivi entrent dans le champ du respect de la règlementation en vigueur et de la RSE.
- Elle sécurise les organisations en cas de plainte et permet d'assurer la protection des données traitées, dans un contexte de déploiement du numérique dans les organisations et de l'habitat connecté, alors que la cybercriminalité se développe.
- Des sanctions renforcées :



2

Les impacts pour les organisations

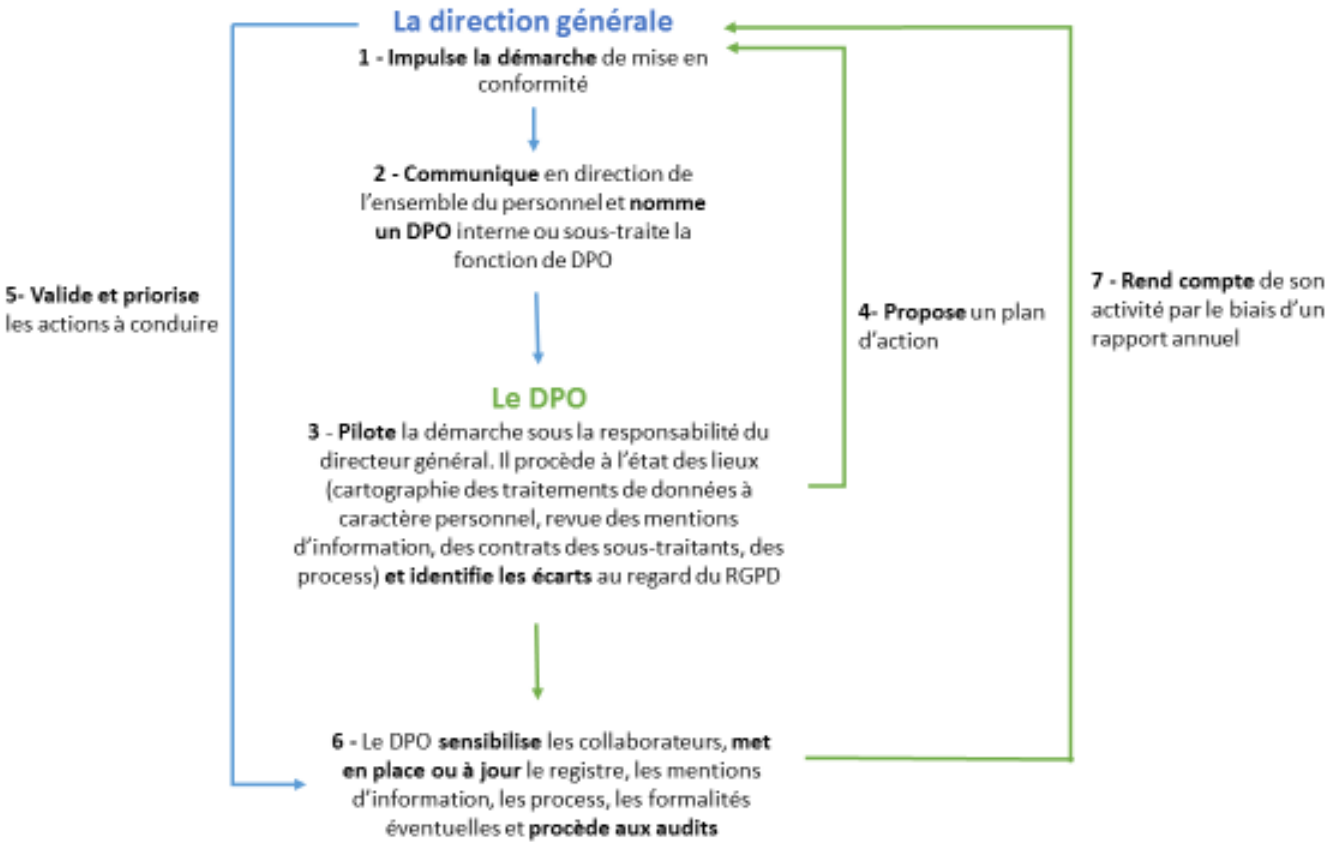
Les impacts organisationnels de la mise en conformité

- Une nécessaire implication des directions générales, mais aussi de l'ensemble des collaborateurs

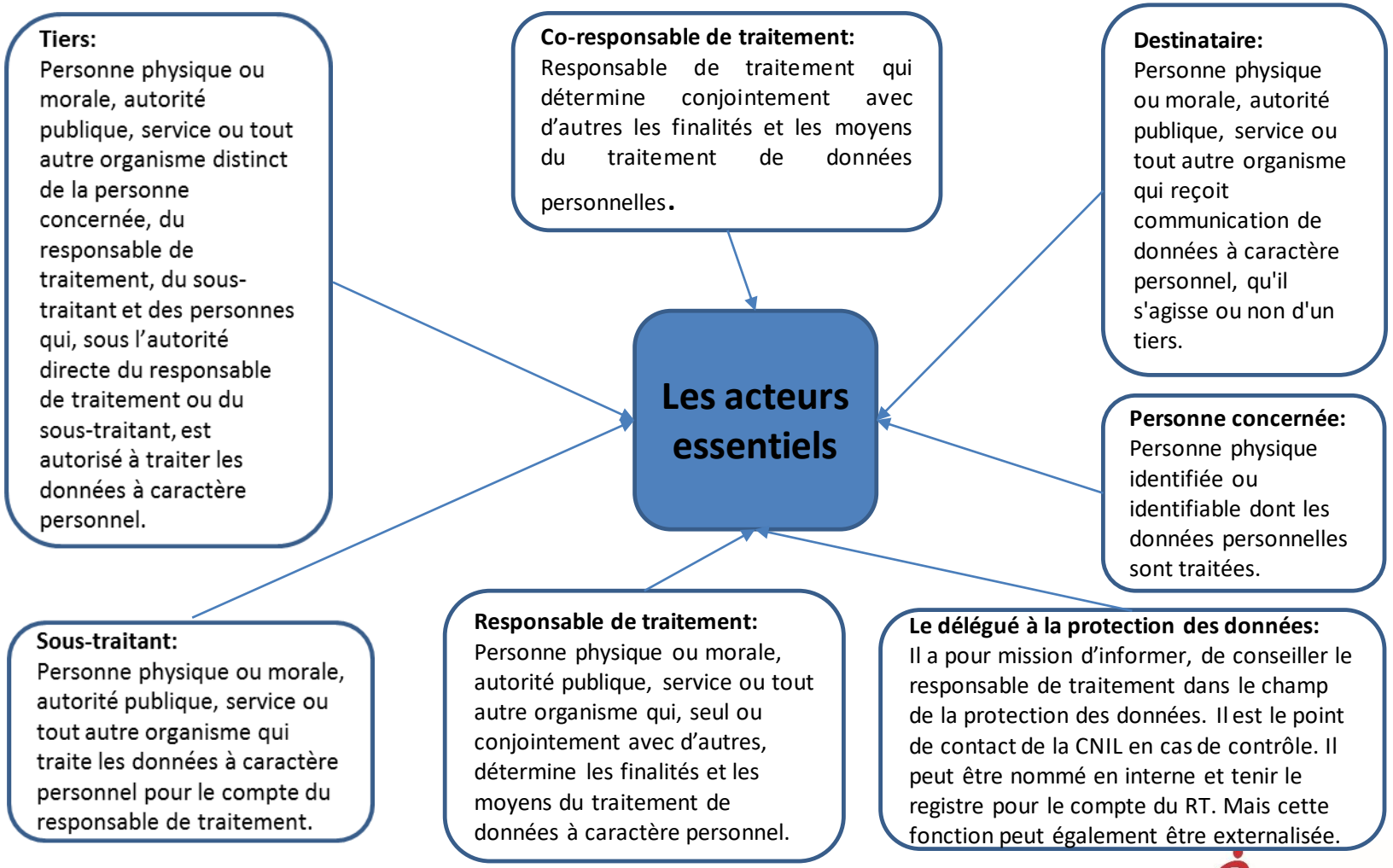
- La nécessité de nommer un pilote : le rôle central du délégué à la protection des données (DPO)

- Un DPO obligatoire pour :
  - les organismes du secteur public (critère organique) ;
  - ou lorsque les traitements mis en œuvre **au titre des activités principales du responsable de traitement** entraînent, du fait de leur nature, de leur portée et/ou de leurs finalités, le **suivi régulier et systématique** des personnes **à grande échelle ;**
  - ou lorsqu'un organisme met en œuvre un **traitement à grande échelle de données sensibles** ou relatives à des **infractions, condamnations ou mesures de sûreté**.

La gouvernance



Les acteurs de la conformité



Comment documenter la démarche de mise en responsabilité ?

- La tenue d'un registre des traitements de données à caractère personnel,
- Un bilan annuel I&L,
- D'autres éléments peuvent venir alimenter la documentation, comme une étude d'impact pour les traitements les plus sensibles, une note de procédure relative à la mise en œuvre du droit d'accès, à toute tentative de violation de données à caractère personnel, un plan de formation / sensibilisation des collaborateurs, une charte informatique, une procédure d'audit des traitements de données à caractère personnel, etc.

Comment mettre en œuvre la protection dès la conception ou par défaut ?

- Ceci requiert l'intervention du DPO le plus en amont possible et une collaboration très étroite avec les services, en particulier les DSI.
- D'appliquer les recommandations suivantes :
  - Minimiser les données collectées,
  - Réduire voire supprimer les zones de commentaires libres,
  - Privilégier les menus déroulants,
  - S'assurer de durées de conservation limitées, etc.

4

La démarche à engager et les actions prioritaires à conduire

Le plan d'actions

- Nomination d'un Délégué à la protection des données
- Élaboration d'une première feuille de route à partir d'un état des lieux ou d'un plan d'actions pour les organismes les plus avancés, tenant compte des nouvelles exigences du RGPD
- Sensibilisation / information des collaborateurs
- Revue des mentions d'informations dans le bail et sur tout formulaire de recueil d'information à caractère personnel
- Revue des modalités de recueil du consentement + retrait du consentement et du process concernant le droit d'accès

Le plan d'actions

- Revue des contrats de sous-traitance, et pour les plus avancés suivi / audit des sous-traitants
- Constitution du registre ou poursuite de la mise à jour du registre pour les plus avancés (intégration dans les fiches de traitement des mesures de sécurité techniques et organisationnelles + durée de conservation)
- Adaptation / paramétrage du SI pour intégrer les nouvelles exigences notamment en matière de violation de donnée
- Conduite des analyse d'impact pour les traitements les plus sensibles

5 Impacts du RGPD sur les systèmes d'informations

Les effets sur les SI

- Exemples de mesures organisationnelles et techniques destinées à démontrer la prise en compte des exigences de sécurité :
  - Documenter la sécurité pour chaque application / système informatique
  - Documenter l'analyse de risques pour l'ensemble des traitements comportant des données à caractère personnel
  - Pour chaque traitement ou système de traitement, tenir le schéma des flux (au besoin processus par processus)
  - Définir une politique de sécurité adaptée aux risques présentés par les traitements et à la taille de l'organisme (cette politique devra décrire les objectifs de sécurité physique, logique et organisationnelle permettant de les atteindre)
  - Définir une politique d'accès et habilitation limitant l'accès aux données à caractère personnel identifiées aux seules personnes autorisées
  - Assurer la formation et la sensibilisation des utilisateurs aux règles de sécurité
  - Tenue du registre des violations de sécurité
  - Tenue du registre des demandes d'effacement et de limitation du traitement

7

Les outils mis à disposition par l'Ush pour les organismes Hlm

Accompagnement des organismes HLM par l'Ush

- Diffusion du guide « repère n° 41 » relatif au RGPD à destination des organismes
- Création dès 2014 d'un réseau des référents et correspondants I&L
- Animation d'un espace collaboratif I&L sur lequel les organismes Hlm trouvent des outils, de l'information, échangent (www.union-habitat.org)
- Des réunions au national et en région
- Outils complémentaires mis à disposition par la CNIL sur son site internet et par le biais de l'association AFCDP

Merci de votre participation