La protection des données à caractère personnel

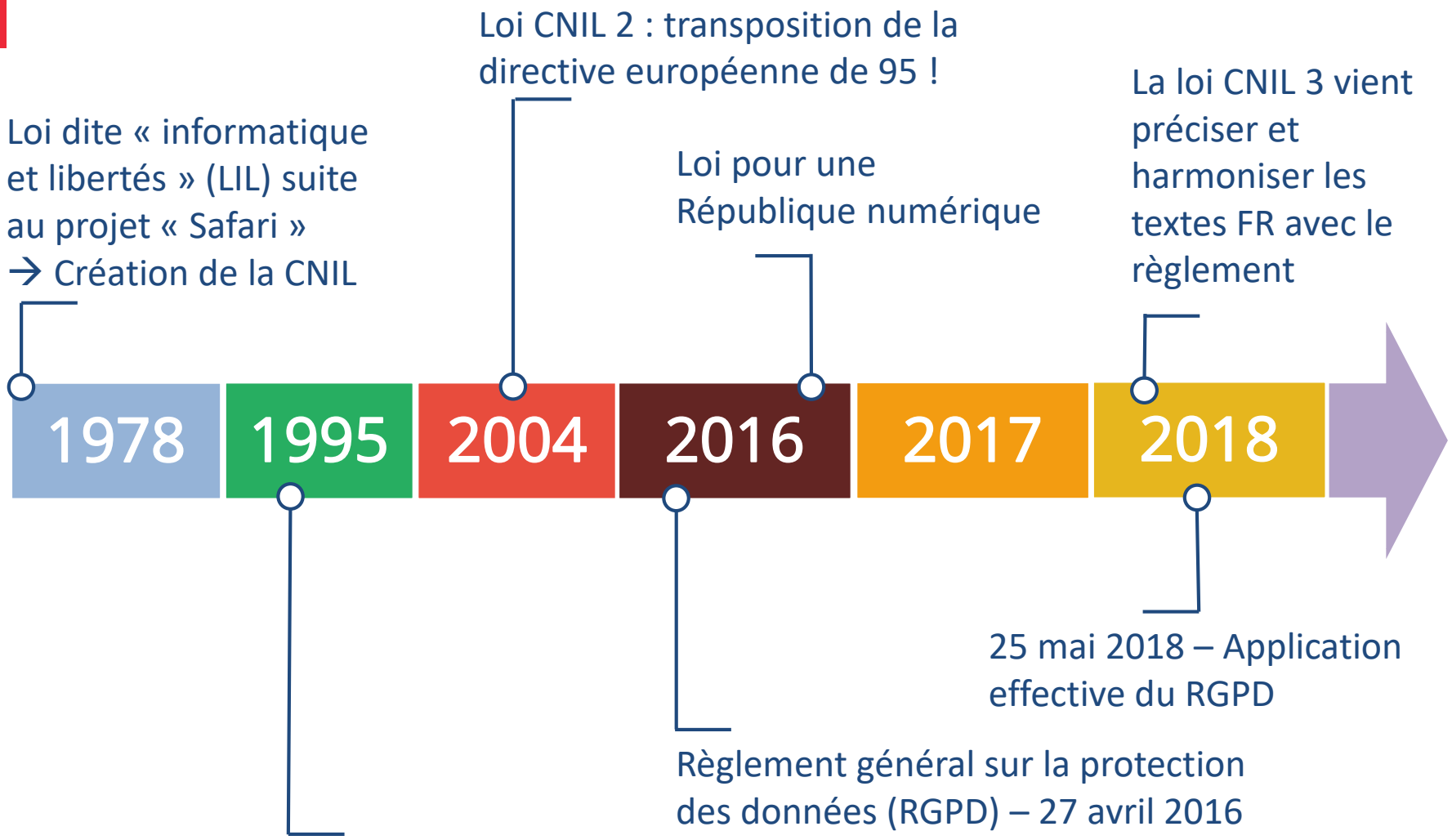
GéoGrandEst - Directive INSPIRE- Open Data

25/09/2018

Un peu d'histoire

Niveau Français

Niveau Européen



Définitions

Données à caractère personnel (DCP) : toute information se rapportant à une personne physique identifiée ou identifiable […] directement ou indirectement…

- ex : coordonnées, vie professionnelle, localisation, habitudes, etc.

Traitement : toute(s) opération(s) effectuée(s) ou non à l'aide de procédés automatisés et appliqué(s) à des données […] telle(s) que « la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction » !

Responsable de traitement (RT): la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement…

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou autre organisme qui traite des DCP pour le compte du RT.

Consentement de la personne concernée : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que les DCP la concernant fassent l'objet d'un traitement.

Les principes de la loi repris dans le règlement

Article 5 du RGPD :

- ✓ Les DCP sont traitées de manière licite, loyale et transparente
- ✓ Finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités
- ✓ Proportionnalité (minimisation): adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités
- ✓ Exactitude : toutes les mesures raisonnables doivent être prises pour que les données qui sont inexactes […] soient effacées ou rectifiées sans tarder
- ✓ Limitation de la conservation : conservées […] pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées
- ✓ garantir la sécurité appropriée des DCP, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées

Les principes de la loi repris dans le règlement

Le responsable du traitement est responsable du respect du paragraphe 1 (ndr : les principes de la diapo précédente) et est en mesure de démontrer que celui-ci est respecté (RGPD)

- ➔ Il s'agit du principe d' *accountability* qui désigne l'obligation pour les organismes de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

Mais le responsable du traitement n'est plus seul responsable ! Le RGPD implique le **sous-traitant** dans la bonne gestion des DCP :

- ➔ Obligation de tenir un registre de sous-traitant
- ➔ Désignation d'un délégué
- ➔ Prise en compte des principes de protection des données par défaut et dès la conception

Le CiL (facultatif) devient le délégué à la protection des données (obligatoire)

- ➔ Informe et conseille les acteurs,
- ➔ S'assure de la bonne tenue de la documentation : registre, procédures, études… (accountability),
- ➔ Contrôle le respect du règlement,
- ➔ Coopérer avec l'autorité de contrôle,
- ➔ Faire office de point de contact pour l'autorité de contrôle

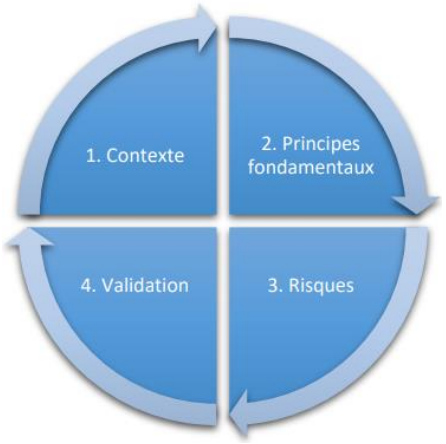
La mise en œuvre des principes

« nouveautés » du RGPD

- ✓ Inscription des traitements au registre de la collectivité
  - ➔ Le registre contient les finalités du traitement, une description des catégories de personnes concernées et des catégories de données à caractère personnel, les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, les délais prévus pour l'effacement des différentes catégories de données, une description générale des mesures de sécurité techniques et organisationnelles.
  - ➔ À priori toutes les anciennes formalités déclaratives sont supprimées

- ✓ Mentions d'information des droits des personnes systématique lors de la collecte et, le cas échéant, recueil du consentement
  - ➔ Sur tous les formulaires de collecte dématérialisés ou pas,
  - ➔ Sur le sites web, attention aux cookies, notamment si l'utilisation d'outils GAFAM qui associent la fourniture d'un service à l'analyse des données à des fins commerciales
  - ➔ Fondement du traitement
- ✓ Respect des droits d'accès, de rectification, d'effacement et d'opposition
  - ➔ En répondant aux sollicitations des personnes sous 1 mois, obligation de publicité des coordonnées DPD
- ✓ Nouveaux droits RGPD : droit à la limitation, droit à la portabilité, transparence en cas de violation de données
- ✓ Sécurité du SI (dont études d'impact sur la vie privée (EIVP (appellation « CNIL ») ou analyse d'impact sur la protection des données AIPD dans le RGPD)

Zoom sur les nouveaux outils



AIPD (art. 35)

1. délimiter et décrire le contexte du(des) traitement(s) considéré(s) ;

2. analyser les mesures garantissant le respect des principes fondamentaux : la proportionnalité et la nécessité du traitement, et la protection des droits des personnes concernées ;

3. apprécier les risques sur la vie privée liés à la sécurité des données et vérifier qu'ils sont convenablement traités ;

4. formaliser la validation du PIA au regard des éléments précédents ou bien décider de réviser les étapes précédentes.

Notification des violations de données

Définition : *une violation de la sécurité entrainant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données*

En cas de violation de données à caractère personnel, **le responsable du traitement** doit notifier à **l'autorité de contrôle** dans les meilleurs délais, si possible **sous 72 heures**, après avoir pris connaissance de la violation.

Lorsqu'une violation de données à caractère personnel est **susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique**, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délai.

Questions

- Cas concrets rencontrés par les géomaticiens
- Autre(s) question(s) ?

Contact : Jean-Sébastien Fiegel, délégué à la protection des données de la Région Grand Est
Mél : dpd[a]grandest.fr

Région **Grand Est**

Maison de la Région · 1 place Adrien Zeller
BP 91006 · F 67070 Strasbourg Cedex
Tél. 03 88 15 68 67 · Fax 03 88 15 68 15

Maison de la Région · 5 rue de Jéricho
CS 70441 · F 51037 Châlons-en-Champagne Cedex
Tél. 03 26 70 31 31 · Fax 03 26 70 31 61

Maison de la Région · Place Gabriel Hocquard
CS 81004 · F 57036 Metz Cedex 1
Tél. 03 87 33 60 00 · Fax 03 87 32 89 33

www.grandest.fr