ITEANU
Société d'Avocats | Law Office

Comment aborder le RGPD

Par
Maître Olivier ITEANU
Avocat, Chargé d'enseignement à l'Université Paris I Sorbonne M2 droit du numérique
Auteur de « Quand le *digital* défie l'Etat de droit » Eyrolles Nov. 2016

Paris, le 19 Octobre 2017
Diner Thématique du CDRT sur la Cybersécurité

Présentation Générale du RGPD

- Règlement 2016/679 du 27 avril 2016 **entré en vigueur le 25 mai 2016**
- **Mais application différée** au 25 mai 2018 [Considérant 171]
- **Règlement Général sur la Protection des Données** – RGPD ou RGDP ou GDPR (General Data Protection Regulation)
- Règlement = application directe (≠ de la Directive qui nécessite une Loi nationale de transposition, comme la Directive NIS de juillet 2016)
- Au plus tard le 25 mai 2020 et tous les 4 ans, rapport d'évaluation et de réexamen du RGPD présenté par la Commission (Art. 97)
- 173 considérants, 99 articles: problème de lisibilité

ARTICLE 4 DU RGPD 26 DÉFINITIONS

Notions clefs

- **Donnée à caractère personnel ou donnée personnelle**
  - toute information susceptible d'identifier, directement ou indirectement (élément d'identification propre), une personne physique
- **Traitement**
  - collecte, conservation, modification, extraction, consultation, utilisation transmission, interconnection de données personnelles … toute manipulation de données personnelles
- **Responsable de traitement**
  - le « ficheur » de 1978, celui qui a un pouvoir de décision sur les données personnelles traitées (finalités et moyens)
- **Sous-traitant**
  - traite de données personnelles **pour le compte** du responsable de traitement (prestataire cloud notamment)
- **Personne concernée**
  - le « fiché » de 1978

Le RGPD résumé en cinq points

- **<u>Point 1</u> – Des sanctions à la hauteur des enjeux [ART. 83 et svts]**
  - Des amendes administratives prononcées par les CNIL (« Juge » de la conformité) qui peuvent aller jusqu'à 4% du CA mondial total de l'exercice précédent, au plus.
  - Les sanctions pénales toujours d'actualité – en moyenne le Code pénal prévoit des peines maximales de 300K€ d'amende et 5 ans d'emprisonnement (Juge de l'ordre public)

Le RGPD en cinq points (Suite)

- **<u>Point 2</u> – Un changement de mentalité**
  - Fini les déclarations préalables à la CNIL (consultation obligatoire dans certains cas [art. 36])
  - L'auto-contrôle sous surveillance (*Privacy by design*, Security *by default* : l'entreprise doit démontrer que le RGPD a été anticipé jusque dans la conception du SI [Art. 25] – *Accountability* : l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect du RGPD [Art. 24])
    - *La collaboration obligatoire de la technique, de l'organisationnel et du juridique*

Le RGPD en cinq points (Suite)

- <u>Point 3</u> – de nouveaux droits et de nouvelles obligations

+ de droits pour les personnes concernées	+ d'obligations pour les responsables de traitement et sous-traitants
Droit à la portabilité des données Droit à « l'oubli » (déréférencement) Action de groupe …	Obligations de notification [Art. 33 & 34] DPO obligatoire pour le secteur public et les traitements à risque …

Le RGPD en cinq points (Suite)

- **Point 4 – Quasi assimilation du sous-traitant au responsable de traitement**
  - **Le sous-traitant peut être « co responsable »**
  - Chapitre IV intitulé « Responsable de traitement et sous-traitant »
  - **Encore des différences** – exemple
  - En cas de violation de données à caractère personnel (Art. 33 – 34)
    - *le responsable du traitement notifie la violation [à la CNIL] dans les meilleurs délais et, si possible, **72 heures au plus tard après en avoir pris connaissance***
    - *Le sous-traitant notifie au responsable du traitement toute violation **dans les meilleurs délais** après en avoir pris connaissance.*
    - *Lorsqu'une violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation à la personne concernée **dans les meilleurs délais.***

Le RGPD en cinq points (fin)

- **Point 5 – Des évolutions majeures mais pas de rupture**
  - Ce qui ne change pas ou peu
    - Les objectifs
    - Les concepts clefs
    - Les principes – Les 5 règles d'or de la Loi informatique et libertés sont maintenues *(finalité, pertinence et proportionnalité [nécessaire], durée limitée, sécurité et confidentialité, respect du droit des personnes)*
    - La CNIL comme pivot central des dispositifs
    - L'importance grandissante des Codes de conduite notamment par secteur d'activités, des certifications et labels
    - Dans le sens de l'histoire avec toujours plus de droits pour les personnes concernées et d'obligations pour les responsables de traitement (sous-traitants)

ITEANU
Société d'Avocats | Law Office

Sécurité des données, tu l'exigeras sinon ta responsabilité tu l'engageras

- Art. 34 Loi de 1978

« Le responsable du traitement est tenu de prendre toutes précautions utiles (…) pour préserver la sécurité des données … »

- Art. 35 Loi de 1978

« Le sous-traitant doit présenter des garanties suffisantes pour assurer (…) l'article 34 (…) Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données… »

Sanctions CNIL : 150K€

Art. 226-17 du code pénal: *« Le fait de procéder ou de faire procéder à un traitement sans mettre en oeuvre les mesures prescrites à l'article 34 (…) est puni de 5 ans d'emprisonnement et de 300 000 € d'amende*

Art. 32 du RGPD

« Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques (…) le responsable de traitement ***et le sous-traitant*** *mettent en œuvre des mesures techniques et organisationnalles appropriées .. »*

Mettre en œuvre *« une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement »*

Sanctions CNIL : 10M€ ou 2% du CA mondial total

Sanction pénale : idem (?)

L'affaire Orange (2014), le RGPD appliqué avant l'heure !

ITEANU
Société d'Avocats | Law Office

- Alerte d'un client
- Plainte pénale d'Orange
- **Notification « violation » à la Cnil le 25 Avril 2014**
- **Dans la presse le 5 Mai 2014**
- Contrôle Cnil sur place les 12 et 14 Mai 2014
- Le 27 Mai 2014 convocation Cnil devant la formation restreinte
- **Le 7 août 2014, Décision de sanction de la Cnil** (avertissement public)
- Confirmé par Conseil d'Etat Décision du **30 décembre 2015**

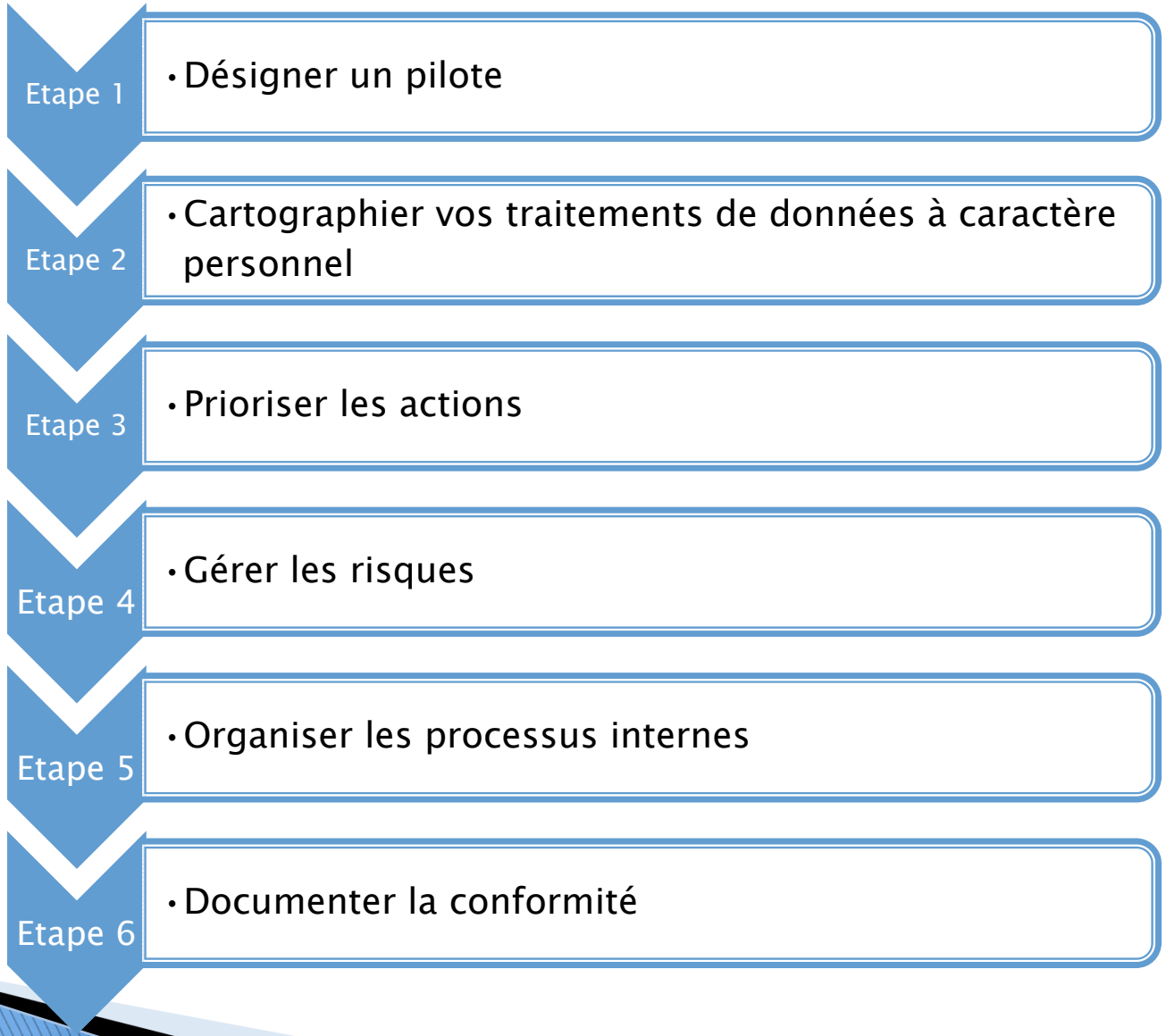
Le cas Orange

- 1,3 millions de données clients impactées les 4 et 5 Mars 2014
- Recours à un sous-traitant et sous-traitant du sous-traitant

Cnil dit Orange n'a pas:

- *« fait réaliser d'audit de sécurité sur la version de l'application spécifiquement développée … »*
- *« communiqué de manière sécurisée les mises à jour de ses fichiers clients à ses prestataires »* (crypto]
- Aucune clause de sécurité et confidentialité des données n'était imposée à son prestataire secondaire

Comment se conformer ? Les conseils de la CNIL



CONCLUSION

- Un texte majeur pour un <u>changement de mentalité</u> dans la gestion des données à caractère personnel (concerne tout SI)
  - Instaurer le réflexe *« données à caractère personnel »*, c'est le principal apport – documenter
  - les bons choix organisationnels et techniques – toujours documenter
  - Un risque juridique accru pour les contrevenants

Merci !

Questions / Réponses

ITEANU
Société d'Avocats | Law Office

www.iteanu.com
blog.iteanu.com
@iteanu