GIDE

GIDE LOYRETTE NOUEL

Thème n° 3

Règlement Général sur la Protection des Données

La violation de données personnelles

6 mars 2018

Table des matières

1. Précédents

Etats-Unis	• 47 des 50 Etats ont une règlementation concernant la violation des données personnelles (Etat de Californie dès 2003)
France	• Expérience tirée du régime de la directive 2009/136 applicable aux opérateurs de communications électroniques : art. 34 bis LIL
Corée du Sud	• Obligation de notification selon l'ampleur de la violation et son domaine
Australie	• 22 février 2018 : nouvelle règlementation sur l'obligation de notification des personnes concernées et notification à l'autorité

2. Décisions de la CNIL

- Délibération SAN-2017-010 du 18 juillet 2017 – HERTZ : Sanction 40.000 €

  *« La formation restreinte considère que **la violation de données résulte d'une négligence de la société dans la surveillance des actions de son sous-traitant**. Elle note tout d'abord que la société n'a imposé aucun cahier des charges à son prestataire s'agissant du développement du site. […]**la société aurait dû s'assurer**, à la suite de cette opération, que la mise en production du site avait été précédée d'un protocole complet de test **afin de garantir l'absence de toute vulnérabilité**. »*

- Délibération SAN-2017-011 du 20 juillet 2017 – OUICAR: Avertissement

  *« **Tout en soulignant la bonne foi** de la société OUICAR qui a réagi immédiatement après la révélation de la **violation de données**, la formation restreinte estime **qu'elle n'avait pas pris en amont les mesures élémentaires de sécurité qui s'imposaient**. »*

2. Décisions

- Délibération n°2014-298 du 7 aout 2014 – ORANGE : Avertissement

  *« La formation restreinte entend toutefois rappeler que **l'article 34 bis de la loi du 6 janvier 1978 modifiée impose aux fournisseurs de services de communications électroniques d'informer la Commission de toute violation** affectant la confidentialité de données nominatives traitées dans le cadre de la fourniture au public des services de communication électroniques. »*

  Confirmée par le Conseil d'Etat – Décision du 30 décembre 2015

3. Définitions : Art. 4-12 RGPD

Une violation de 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

3. Définitions : Guidelines Data Breach Notification

- **Destruction des données à caractère personnel** : le cas où les données n'existent plus ou n'existent plus sous une forme utile pour le responsable du traitement.

- **Perte des données à caractère personnel** : le fait que les données peuvent encore exister, mais que le responsable du traitement a perdu le contrôle ou l'accès à ces données ou ne les possède plus.

- **Altération des données à caractère personnel** : les données à caractère personnel ont été modifiées, corrompues ou ne sont plus complètes.

- **Traitement non autorisé ou illicite** : inclut la divulgation de données à caractère personnel à des destinataires (ou l'accès par ceux-ci) qui ne sont pas autorisés à recevoir (ou à accéder) aux données, ou toute autre forme de traitement qui viole le RGPD.

4. Obligation de préparation et de réactivité

Mise en place d'une solution de sauvegarde efficace et sécurisée

Recours à des procédés de cryptage et limitation de l'accessibilité aux données personnelles

Traçabilité des comptes disposant d'un accès global à la base de données et stockage sécurisé des mots de passe

4. Obligation de préparation et de réactivité

Information des salariés des conséquences des potentielles violations des données

Mise en place d'un dispositif de veille sur les menaces actuelles

Mise en place de dispositifs de détection et de remontée d'alertes

5. Obligation de notification à l'autorité : Délais

Art. 33-1 RGPD : Notification par le RT de la violation à l'autorité de contrôle

- Dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance
- à moins que la violation en question ne soit pas susceptible d'engendrer des risques pour les droits et libertés des personnes physiques
- Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard

→ **Art. 33-4**: Lorsqu'il n'est pas possible de fournir toutes les informations simultanément à l'autorité, les informations peuvent être communiquées de manière échelonnée, sans retard indu

5. Obligation de notification à l'autorité : Contenu

Art. 33-3 RGPD - La notification à l'autorité doit notamment contenir:

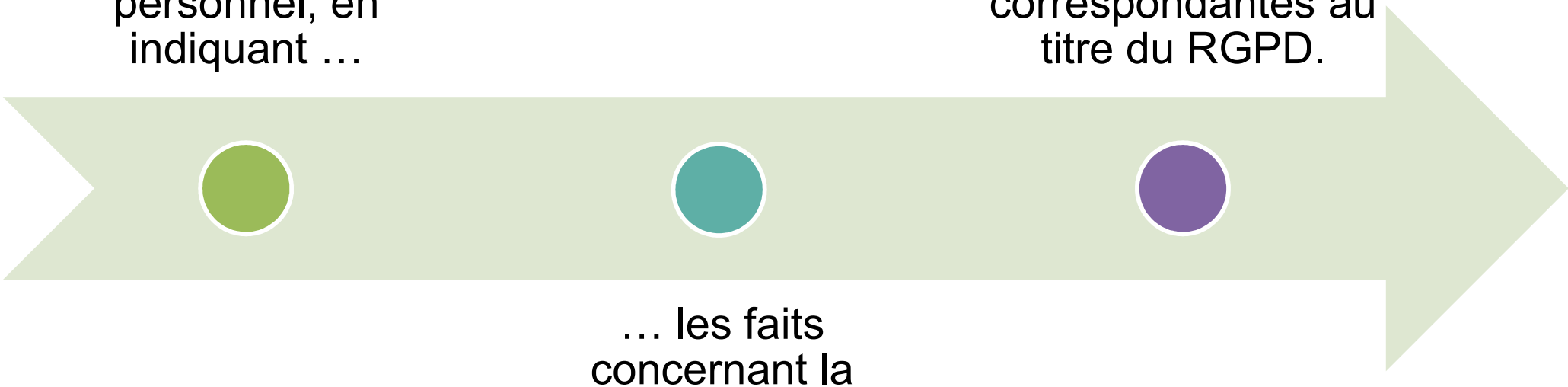
- Nature de la violation : catégories/ nombres approximatifs: personnes concernées et enregistrements
- Nom et coordonnées du DPO / point de contact
- Les conséquences probables de la violation
- Les mesures prises ou envisagées pour remédier à la violation

5. Obligation de notification à l'autorité
Obligation de documentation - Art. 33-5 RGPD

Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant …

… les faits concernant la violation, ses effets et les mesures prises pour y remédier.

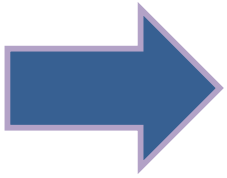
Cette documentation permet à l'autorité de vérifier le respect des obligations correspondantes au titre du RGPD.



6. Obligation de communication aux personnes concernées

Art. 34 RGPD : Communication par le RT de la violation aux personnes concernées

- 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 de données à caractère personnel à la personne concernée dans les meilleurs délais.
- La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation
- et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).



L'autorité de contrôle peut exiger du RT qu'il procède à cette communication.

6. Obligation de communication aux personnes concernées : Exceptions - Art. 34-2 RGPD

Mesures de protection techniques et organisationnelles appropriées mises en œuvre telles que le chiffrement

Mesures ultérieures garantissant que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser

Communication exigerait des efforts disproportionnés. Possibilité de procéder à une communication publique

7. Sanctions

Art. 83 RGPD:

*« Les violations des dispositions suivantes font l'objet […] d'amendes administratives pouvant s'élever jusqu'à **10 M €** ou, dans le cas d'une entreprise, jusqu'à **2 % du chiffre d'affaires annuel mondial total** de l'exercice précédent, le montant le plus élevé étant retenu:*

a) les obligations incombant au responsable du traitement et au sous-traitant en vertu des articles 8, 11, 25 à 39, 42 et 43 […] »

8. Quelques recommandations

- Réfléchir à la mise en place d'une équipe « de crise »
- Dans les groupes, identifier régulièrement les traitements communs
- Suivre la publication des Guidelines du CEPD et du décret CNIL II sur les dérogations à l'obligation d'informer les personnes concernées
- Prendre en compte les règlementations sectorielles pertinentes

8. Quelques recommandations

Art. L521-10 CMF : Notification par les prestataires de services de paiement

- L'ACPR
- La Banque de France
- Les utilisateurs de services de paiement

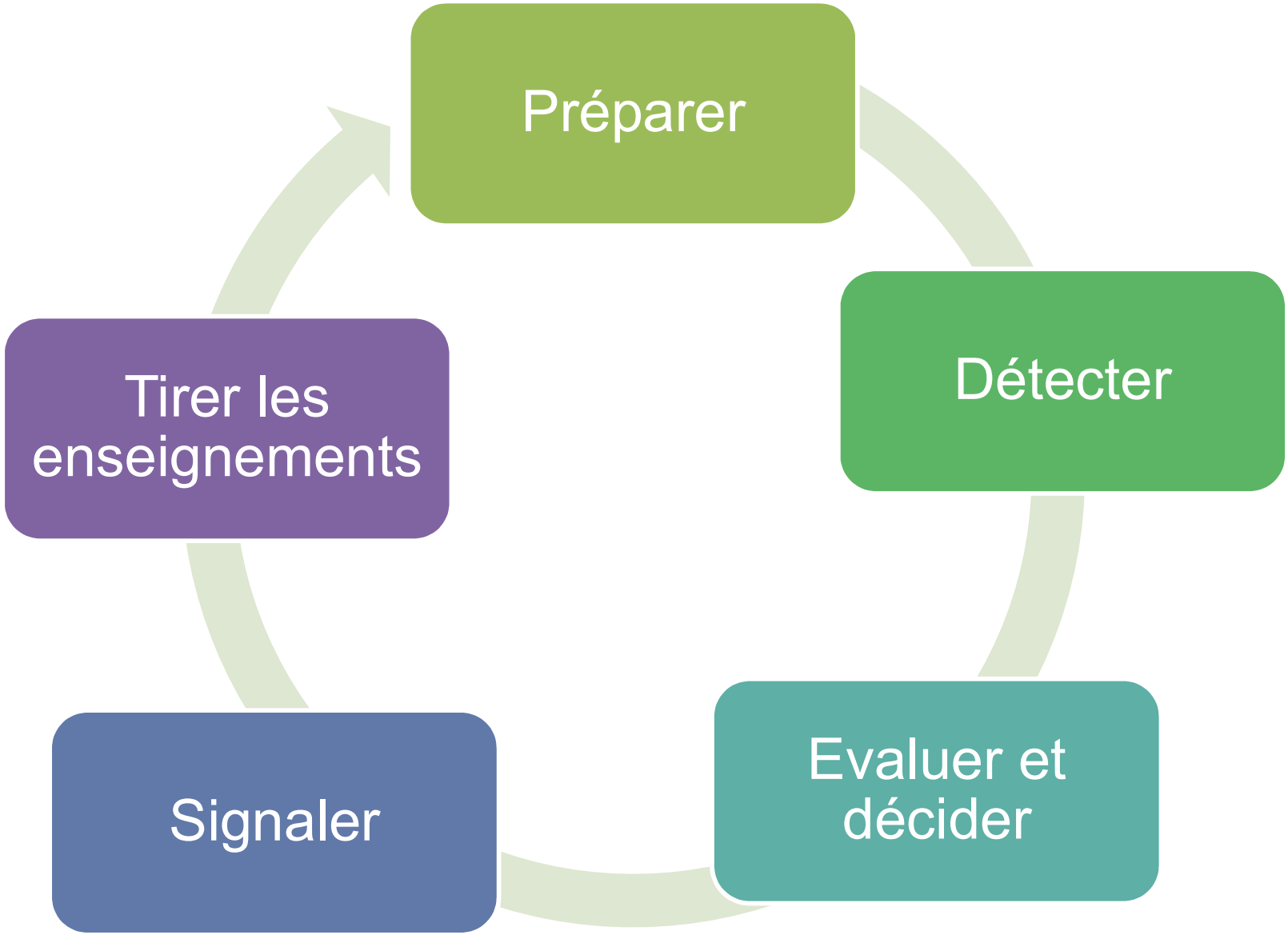
Notification à l'ANSSI par

- Les opérateurs d'importance vitale en cas d'incidents (Code de la Défense)
- Les fournisseurs de services numériques (Directive NIS)
- Les prestataires de services de confiance (Règl. eIDAS)

Notification au DG de l'agence régionale de santé

- Par les établissements de santé

8. Quelques recommandations



GIDE

GIDE LOYRETTE NOUEL

Merci pour votre attention

Questions / Réponses

Thierry Dor

dor@gide.com

Gide Loyrette Nouel A.A.R.P.I.
22 cours Albert Ier
75008 Paris
tél. +33 (0)1 40 75 60 00
info@gide.com - gide.com

ALGER
BRUXELLES
CASABLANCA
ISTANBUL
LE CAIRE
LONDRES
MOSCOU
NEW YORK
PARIS
PÉKIN
SHANGHAI
TEHERAN
TUNIS
VARSOVIE