



Les midis de l'entreprise

Violation de données à caractère personnel :
comment réagir ?

Astrid Wagner

Partner
IP, Communication & Technology

Bénédicte d'Allard

Manager
Arendt Regulatory & Consulting

Plan

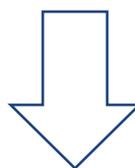
- Comment identifier une violation de données à caractère personnel ?
- Peut-on s'y préparer à l'avance?
- Comment y faire face en pratique ?

Comment identifier une violation de données à caractère personnel ?

« Une violation de la sécurité entraînant, 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 » (RGPD, art 4).



Confidentialité



Intégrité



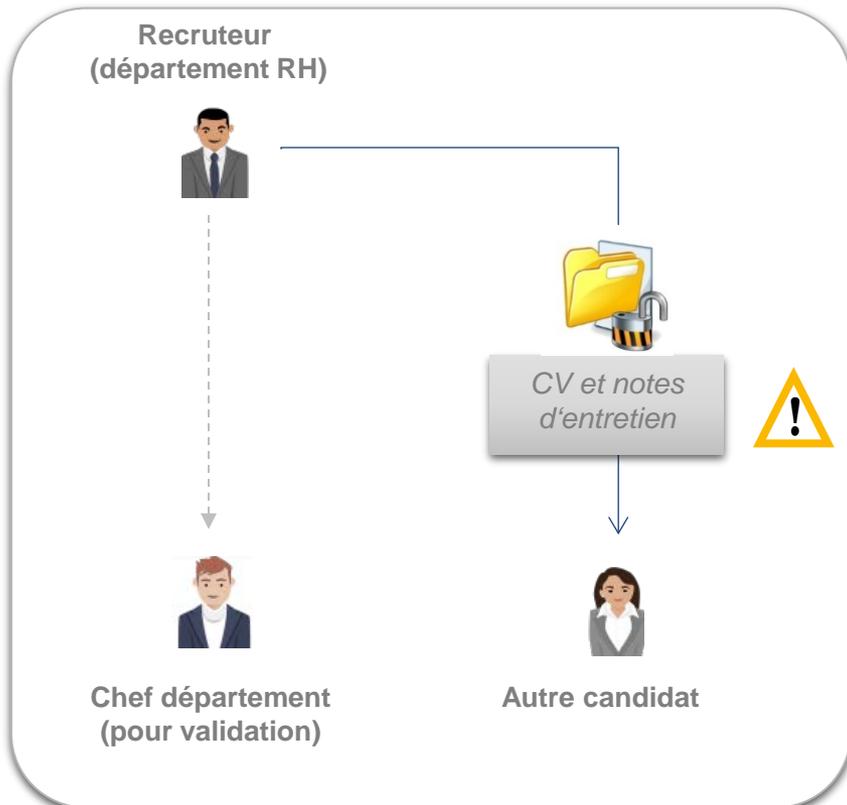
Disponibilité

Une violation de données personnelles est une forme d'incident de sécurité.

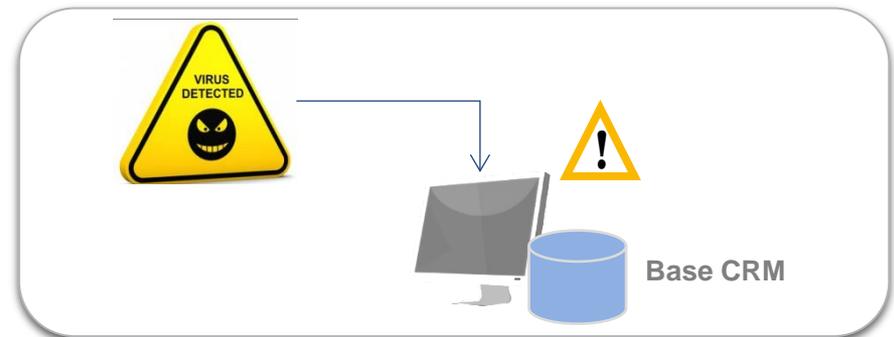


Exemples de violations de données potentielles

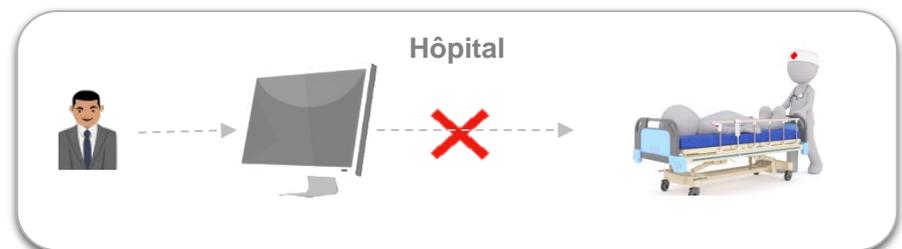
CAS 1 : erreur d'envoi de CV et notes d'entretien d'embauche



CAS 2 : attaque par un virus qui touche la base CRM et modifie tous les contacts clients

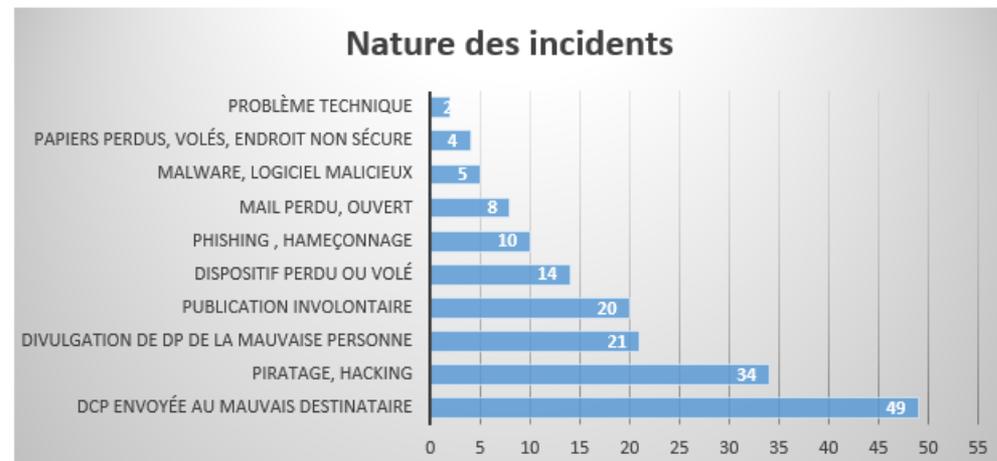
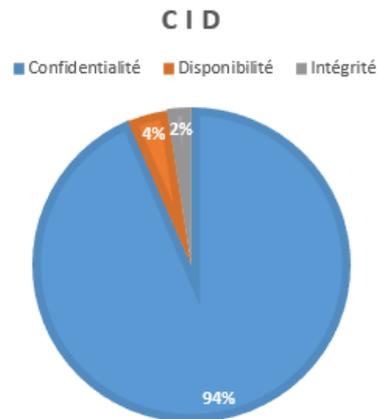


CAS 3 : non-disponibilité de système contenant des données de patients pendant plusieurs heures dans un hôpital



Type de violations de données personnelles

Statistiques depuis le 25 mai 2018* - CNPD



*Du 25/05/2018 au 31/12/2018
 Luxembourg
 26 février 2019

Peut-on s'y préparer à l'avance?

Se protéger au préalable – obligations légales

Réduction du risque d'une violation - Principes consacrés par le RGPD

- Limitation des finalités
- Minimisation des données
- Limitation de la conservation
- Intégrité et confidentialité
 - Mise en place de mesures techniques et organisationnelles appropriées
- Accords avec les sous – traitants
- Transferts transfrontaliers et dans des pays tiers

Peut-on s'y préparer à l'avance?

Les ingrédients pour une bonne préparation

- Sensibilisation des employés
- Test / simulation de situations critiques
- Utilisation d'outils de « ticketing »

1) Procédure claire et comprise

2) Respect des délais

- 72h pour notifier l'autorité de contrôle le cas échéant

5) Continuité processus de gestion des incidents



3) Moyens techniques de détection

- Insertion dans processus existants
- Implication du management

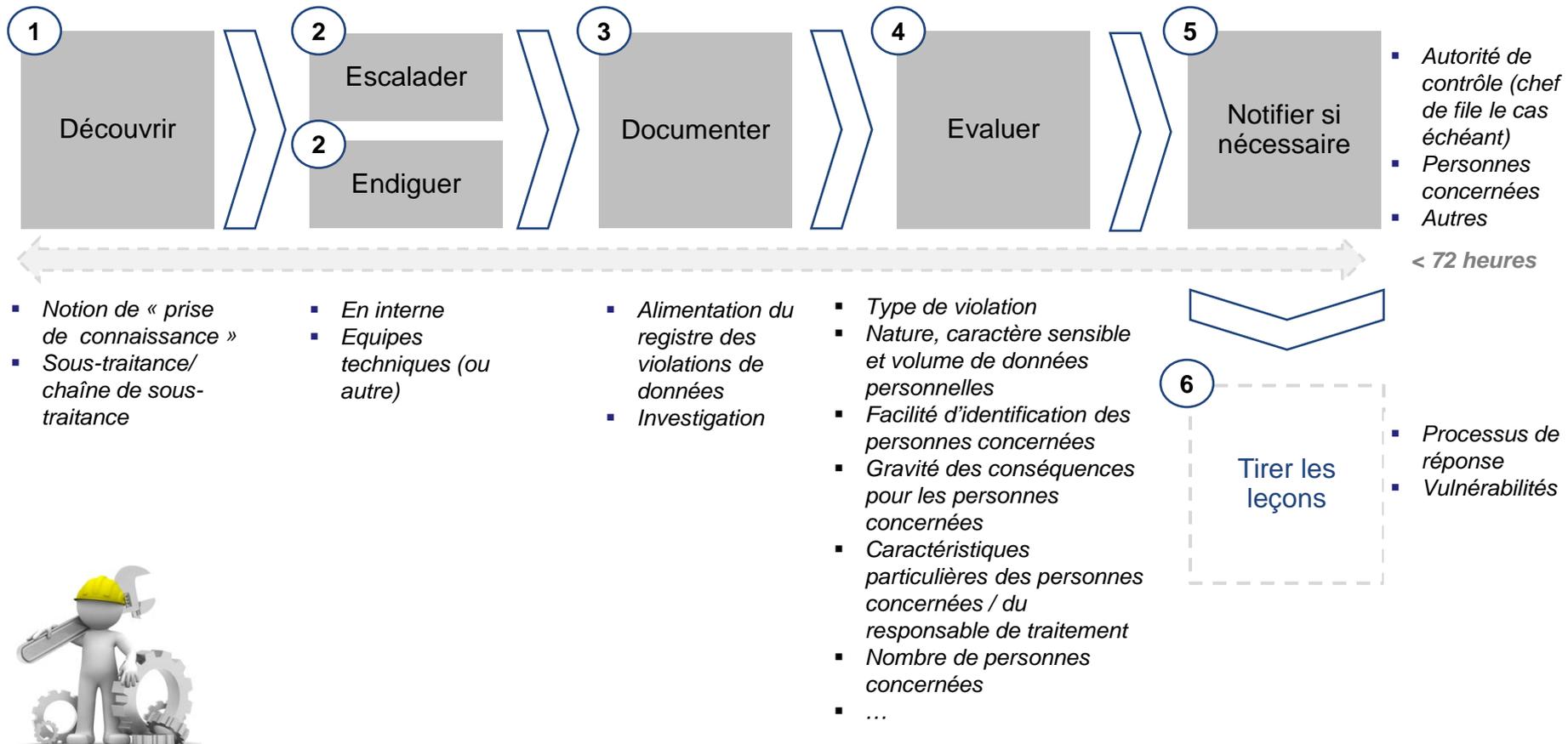
4) Clarté des responsabilités vis-à-vis des tiers

- Capacité à détecter une activité anormale (fréquence, montant,...) – capitaliser sur l'existant
- Systèmes de prévention des pertes de données (DLP)

- Processus d'escalade - contrat de traitement de données et accord de niveau de service

Comment y faire face en pratique ?

Les étapes



5

Quand notifier une violations de données

Les étapes (suite)



«En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, **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 un risque 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.» (GDPR, art 33)

Pour les personnes concernées, la violation engendre:	Aucun risque*	Risque	Risque élevé
Documentation interne, dans registre des violations	X	X	X
Notification CNPD dans délai maximal de 72h	-	X	X
Information des personnes concernées dans les meilleurs délais, hors cas particulier	-	-	X

Questions?

Avez-vous entendu parler d'Arendt Institute ? Nos solutions de formation professionnelle !

Nous fournissons :

- Cours spécialisés et entièrement personnalisés
- Des solutions de formation au contenu adapté à vos besoins précis
- Prochaines formations sur le sujet :

The road to GDPR compliance

3 avril 2019

Surveillance des employés sur leur lieu de travail et protection de la vie privée

8 mai 2019

Intéressés ?

Contact: institute@arendt.com





Contacts



Astrid Wagner

Partner, IP, Communication & Technology
+352 40 78 78 698
astrid.wagner@arendt.com



Bénédicte d'Allard

Manager, Arendt Regulatory & Consulting
+352 26 09 10 77 31
benedicte.dallard@arendt.com

Cette présentation est destinée à fournir des informations sur les récents développements légaux et ne couvre pas tous les aspects des sujets évoqués. Elle n'a pas été rédigée pour fournir des conseils juridiques ou autres, et ne se substitue pas à la consultation d'un professionnel du droit avant tout engagement.