Violation des données: évaluation, risques et actions exigées

Luxembourg

7 mars 2018

Christophe Buschmann

Membre Effectif

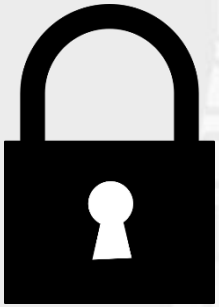
Agenda

Introduction

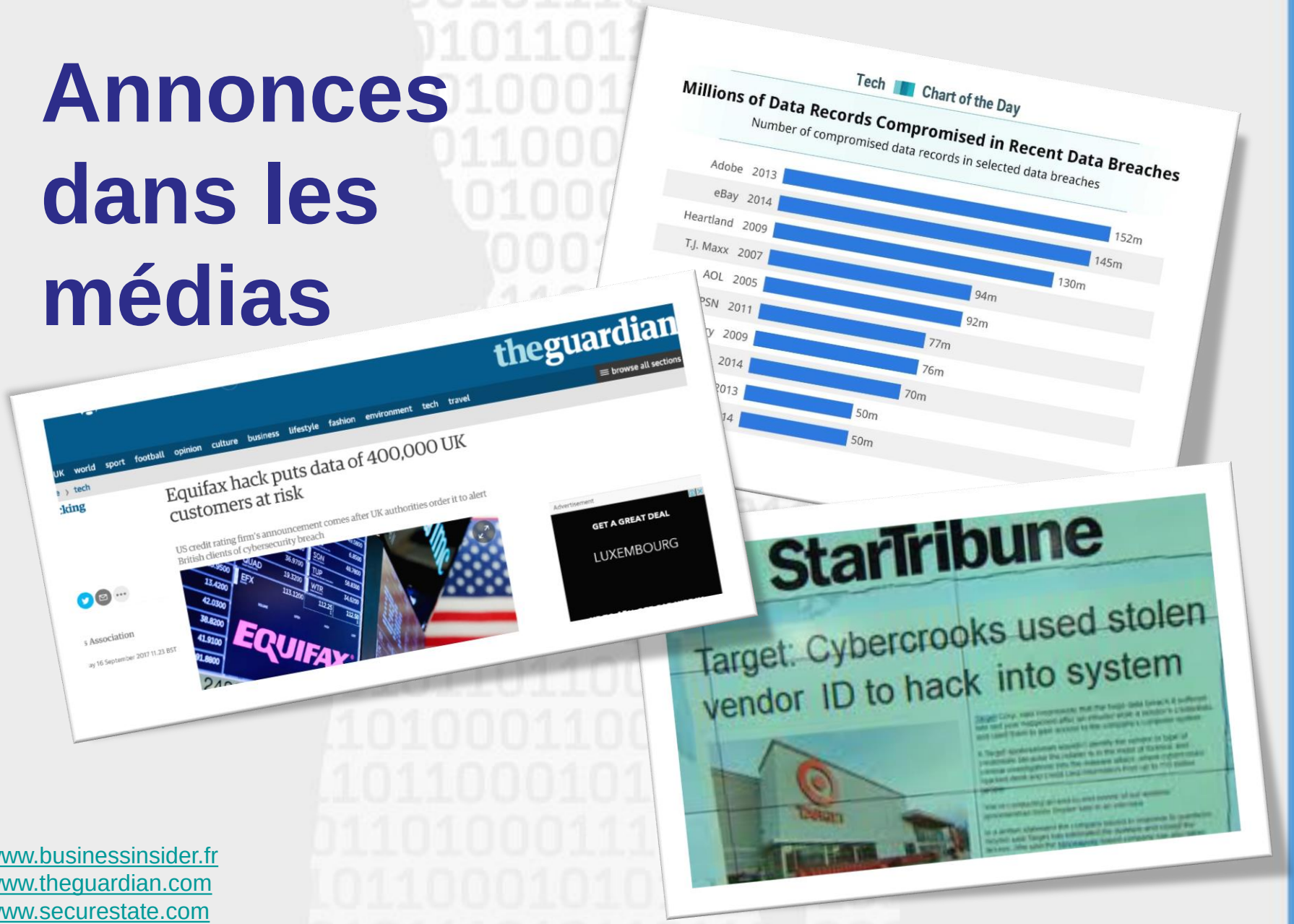
Notions et concepts

Obligations sous RGPD

Elements en place au Lux.



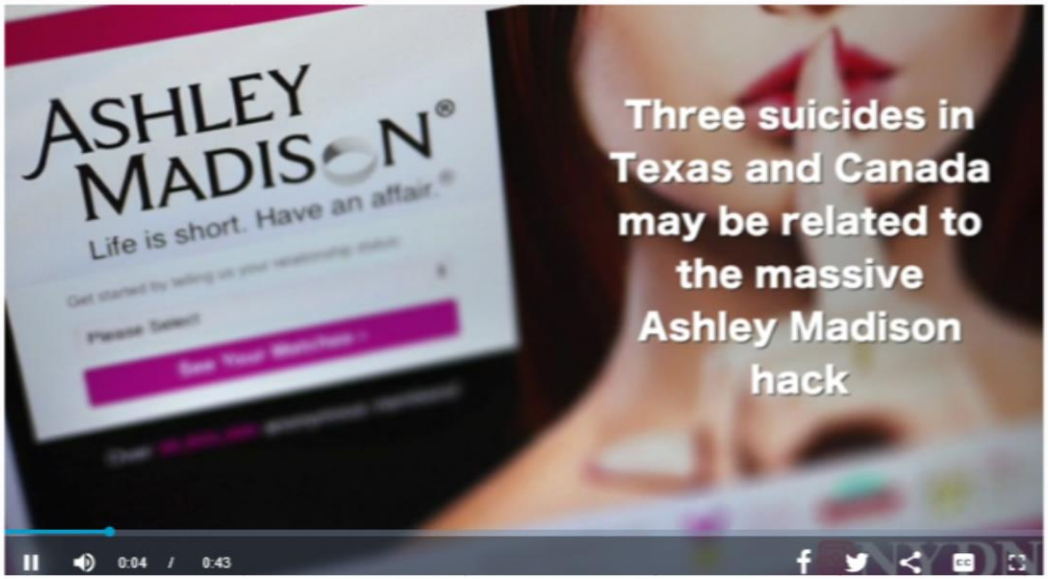
Annonces dans les médias



www.businessinsider.fr
www.theguardian.com
www.securestate.com

Impact sur les personnes

Ashley Madison leak may be linked to 3 suicides, $500,000 reward being offered to identify the hackers



Sujet réel et d'actualité

Will the Equifax data breach impact your Social Security benefits?

Maurie Backman, The Motley Fool — Published 9:05 a.m. ET Sept. 15, 2017 | Updated 9:48 a.m. ET Sept. 15, 2017

The Federal Trade Commission has opened a probe into Equifax's historic data hack, where hackers stole the sensitive personal information of about 143 million people. Jose Sepulveda (@josesepulvedatv) has more. Buzz60

Share your feedback to help improve our site experience!

POPULAR STORIES

Gun stock prices climb after Las Vegas mass shooting

usatoday.com | 13 hours ago

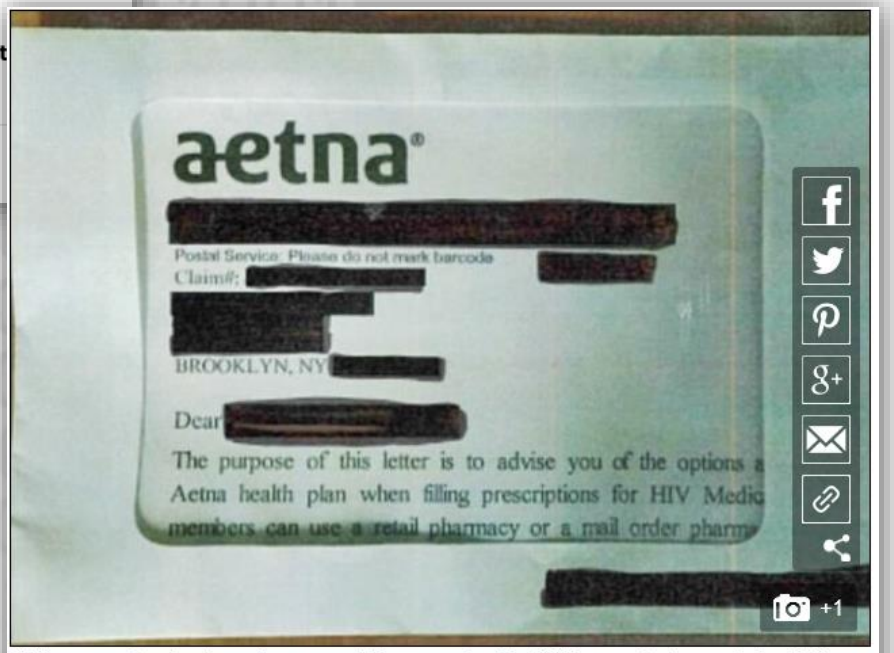
https://www.usatoday.com

Pas limité au domaine IT

Aetna revealed 12,000 patients' HIV statuses by sending letters with giant envelope 'window' that exposed confidential information

- The health insurer sent letters to patients taking medications for HIV or taking pre-exposure medication to prevent getting the virus
- A photo of the envelope reveals how it exposed confidential information
- Lawyers say some patients' relatives and neighbors learned of their HIV status as a result
- Patients were in Arizona, California, Georgia, Illinois, New Jersey, New York, Ohio, Pennsylvania and Washington, D.C
- Aetna said 'this type of mistake is unacceptable' and promised it won't again

By MIA DE GRAAF FOR DAILYMAIL.COM
PUBLISHED: 18:50 BST, 24 August 2017 | **UPDATED:** 00:49 BST, 25 August 2017



Without opening the letter, it was possible to see details of HIV prescriptions and details for purchasing more. This is a redacted photo of one patient's letter from Aetna

Définition: violation de données à caractère personnel

Art 4 (12) : « 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 »

General Data Protection Regulation

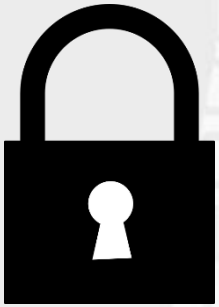
Agenda

Introduction

Notions et concepts

Obligations sous RGPD

Elements en place au Lux.



Les éléments clé

INCIDENT

Faille de sécurité (IT ou organisationnelle)

Attaque ou Accident

Impact (potentiel)

Risque

Différents acteurs: personne concernée, organisation, public, ..

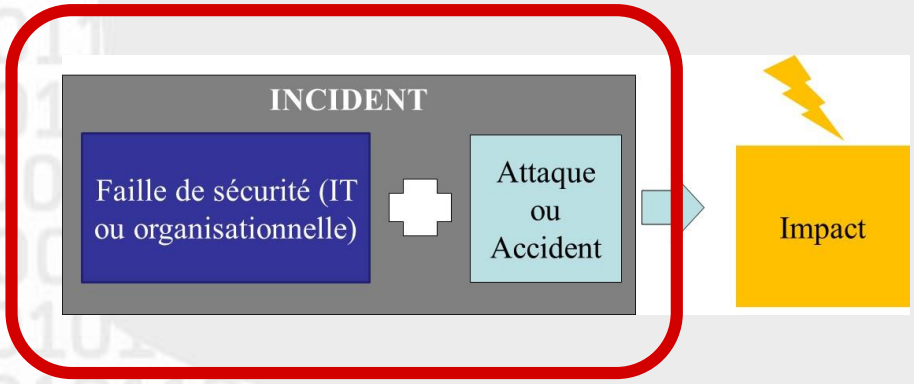
…

Différents impacts (financier, réputation, exclusion sociale, dommage réputationnel, …).

…

L'incident

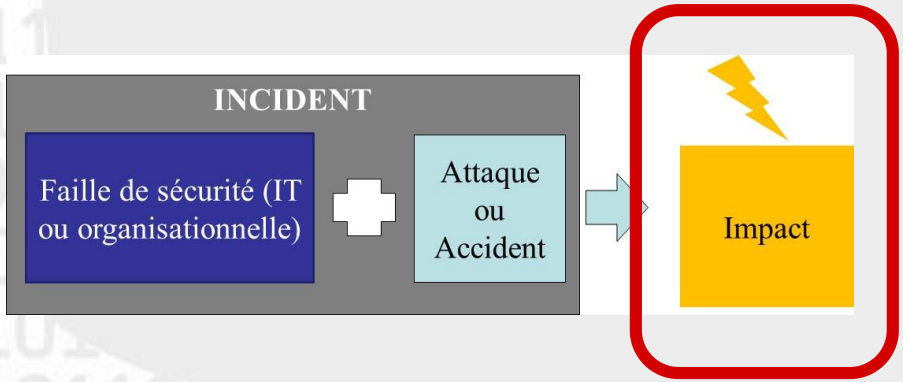
Les critères CIA - type de la violation de données



Critère	Exemple
Confidentialité	- Vol de données d'inscription sur un site de rencontre - Vol de carte bancaire - Perte laptop conseiller bancaire
Intégrité	- Erreur de manipulation dans système IT hospitalier engendre données erronées sur dossier patient
Disponibilité (Availability)	- Attaque via Ransomware sans backup, disque dur crypté

L'impact

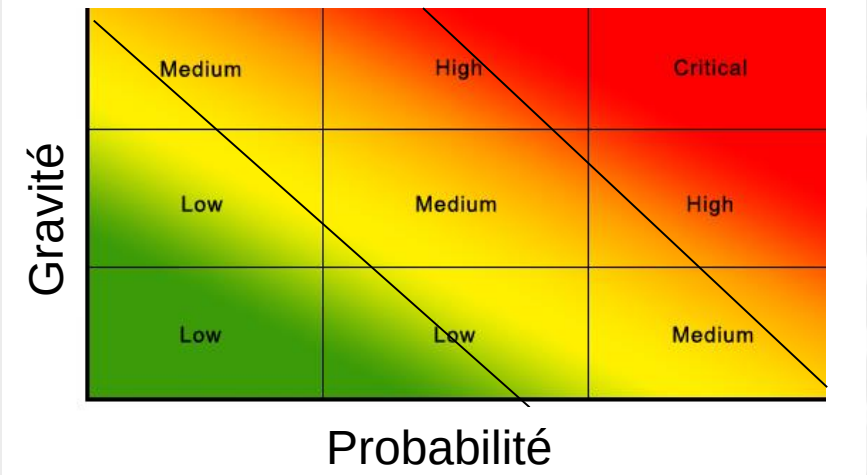
Sur les droits et libertés des personnes concernées



Critère	Exemple	Impact
C	- Vol de données d'inscription sur un site de rencontre - Vol de carte bancaire - Perte laptop conseiller bancaire	- Divorce - Suicide - Perte financière - Perte réputationelle
I	- Erreur de manipulation dans système IT hospitalier engendre données erronées sur dossier patient	- Décès - Mauvais traitement
D	- Attaque d'un hôpital via Ransomware sans backup, disque dur crypté	- Traitement médical interrompu

Le risque

Comment évaluer l'impact



Risque = Probabilité x Gravité

Eléments à prendre en compte:

- Type d'incident (CIA)
- Nature, sensitivité et volume des données
- Facilité d'identifier des personnes
- Sévérité des conséquences pour les personnes
- Caractéristiques spéciales des personnes
- Nombre de personnes concernées
- Caractéristiques spéciales du responsable de traitement

Par rapport à **QUI** et par rapport à **QUOI**

La/les personnes concernée(s)

Les droits et libertés de(s) personnes

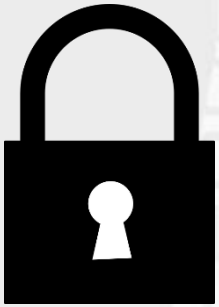
Agenda

Introduction

Notions et concepts

Obligations sous RGPD

Elements en place au Lux.



Principaux éléments à considérer

Sécurité du traitement

↓

Violation de données à caractère personnel

↓

Evaluation / Risque

↓

Registre

Notification

Communication

Violation de données

Principes relatifs au traitement des données à caractère personnel: Les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, 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 (intégrité et confidentialité) (Art. 5 (f))

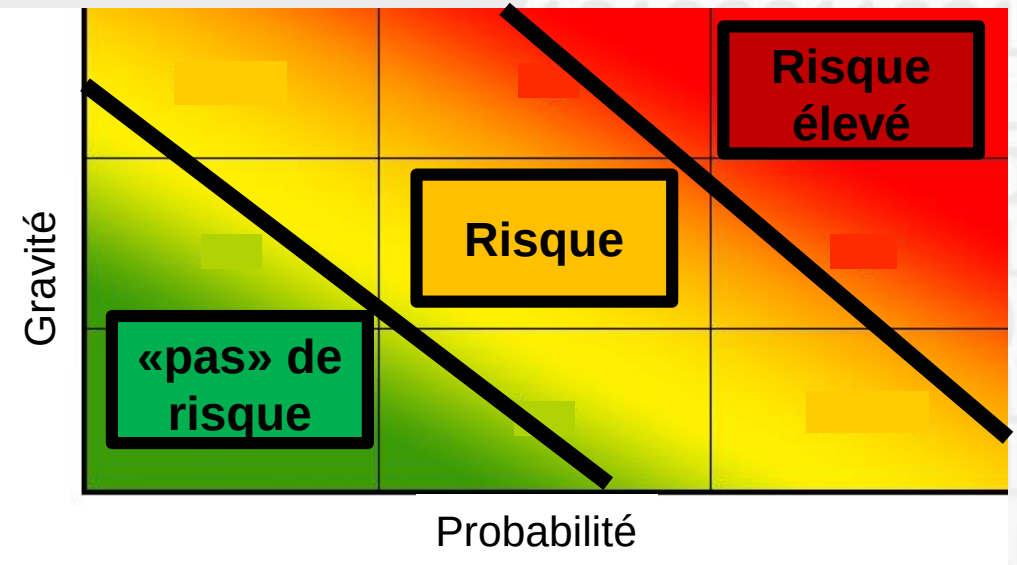
General Data Protection Regulation

- **Mesures de sécurité** obligatoires (éviter ou mitiger l'incident)
- Etre capable de **détecter et gérer** les incidents (mitiger l'impact)

- **Un incident peut toujours arriver – même si toutes les précautions possibles et raisonnables ont été prises**
  - **L'incident ne déclenche pas automatiquement de sanction** – il est tenu compte des mesures techniques et organisationnelles mises en œuvre (Art. 83 (d)) – si amende administrative applicable
  - **La non-notification d'un incident est un critère aggravant** – il est tenu compte de la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable de traitement ou le sous-traitant a notifié la violation (Art. 83 (h)) – si amende administrative applicable

Evaluation / Risque

- Lors de l'évaluation du risque le degré de probabilité la gravité sont à considérer.
- La RGPD prévoit 3 niveaux de risque:
  - (1) «pas» de risque
  - (2) risque
  - (3) risque élevé



Risque = Probabilité x Gravité

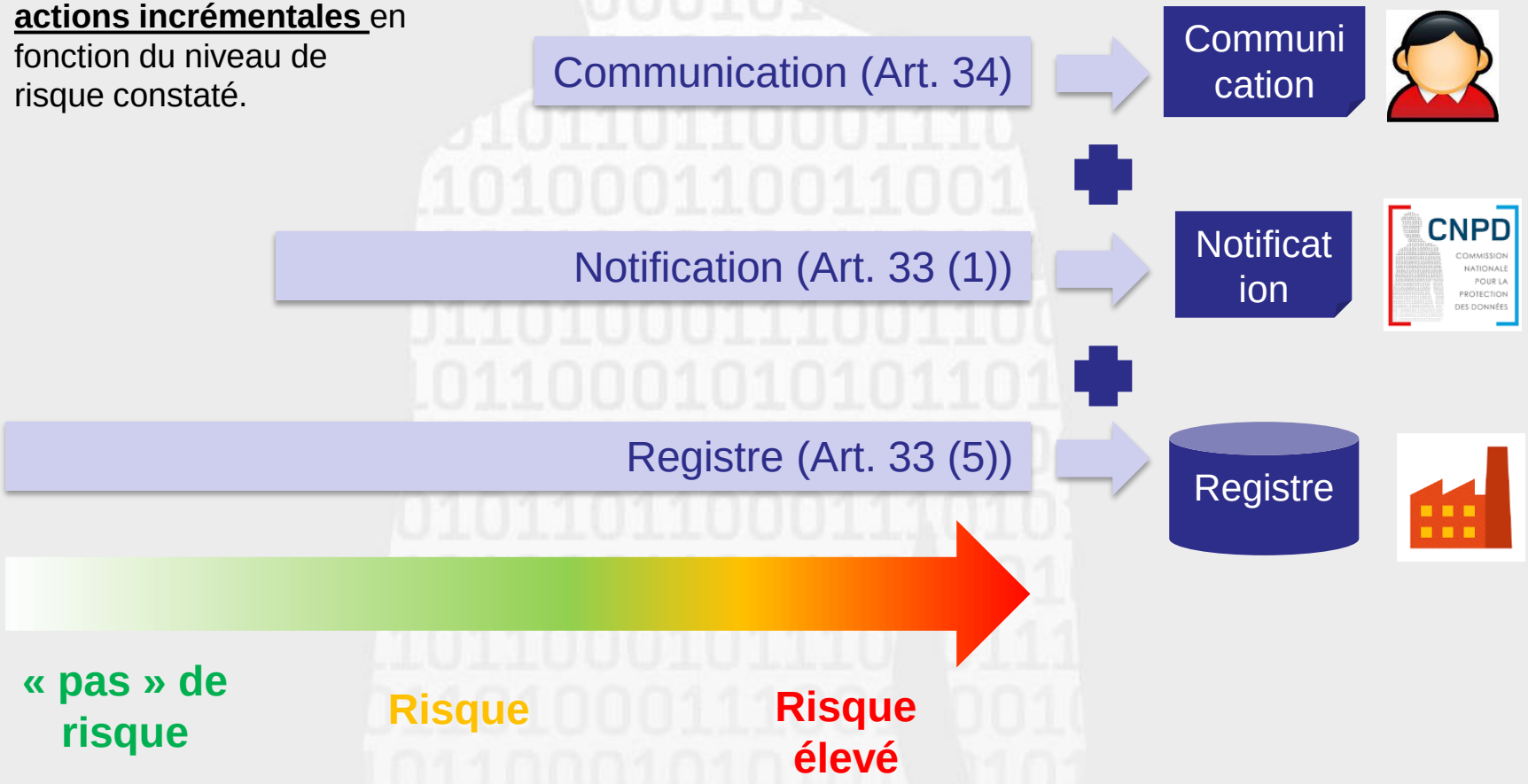
Des **risques pour les droits et libertés des personnes** physiques, dont le **degré de probabilité et de gravité varie**, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier…. (considérant 75)

Le risque devrait faire **l'objet d'une évaluation objective** permettant de déterminer si les opérations de traitement des données comportent un risque ou un risque élevé. (considérant 76)

General Data Protection Regulation

Actions exigées

Le RGPD exige des **actions incrémentales** en fonction du niveau de risque constaté.



Le registre des violations

Le responsable du traitement **documente toute violation** de données à caractère personnel, en **indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier.** La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article. (art. 33 (5))

- La nécessité de documenter toute violation résulte du **principe de responsabilité** (Art.5 (2)
- Il n'est **pas exigé d'établir un registre à part / exclusif** à ce effet. Il peut par exemple être intégré dans un registre de gestion des incidents plus large – mais les informations obligatoires doivent y figurer.
- Le registre doit être **disponible sur demande de la CNPD** notamment en cas de contrôle
- Si la violation ne comporte **pas de risque** pour les personnes concernées la **RGPD n'exige pas d'autres démarches**
- **«lessons learned»** des incidents.

Notification à l'autorité de contrôle

- La notification est à faire **en plus** de l'enregistrement dans le **registre interne**
- Attention les **délais sont courts (72 heures)**. Il faudra **préparer une procédure** afin de pouvoir tenir les délais – intégration dans procédures.
- Il est **possible de compléter la notification** – lorsque tous les détails n'étaient pas connus au moment où elle a été faite.
- Possible de **retirer une notification**
- **La CNPD a mis des outils en place** pour réceptionner les notification (p.ex. email sécurisé, formulaire en ligne, téléphone)

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. (Art. 33)

General Data Protection Regulation

Notification à l'autorité de contrôle d'une violation de données à caractère personnel

CNPD COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Communication à la personne concernée

- La notification est à faire **en plus** de l'enregistrement dans le **registre interne** et **en plus de la notification à la CNPD**
- **Objectif important: Donner à la personne concernée, si applicable, la possibilité de se protéger** (p.ex. changer mots de passe, prévenir des proches,…)
- **Des exceptions existent** (p.ex. données chiffrées, mesures déjà prises, communication publique en cas d'effort disproportionné) – recommandation **restez transparent!**

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 délais.** (Art. 34 (1)
La communication à la personne concernée visée au paragraphe 1 du présent article **décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33**, paragraphe 3, points b), c) et d).

General Data Protection Regulation

Communication à la personne concernée d'une violation de données à caractère personnel

La relation responsable de traitement et sous traitant

Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance. (Art. 33 (2))

General Data Protection Regulation

Sans délai

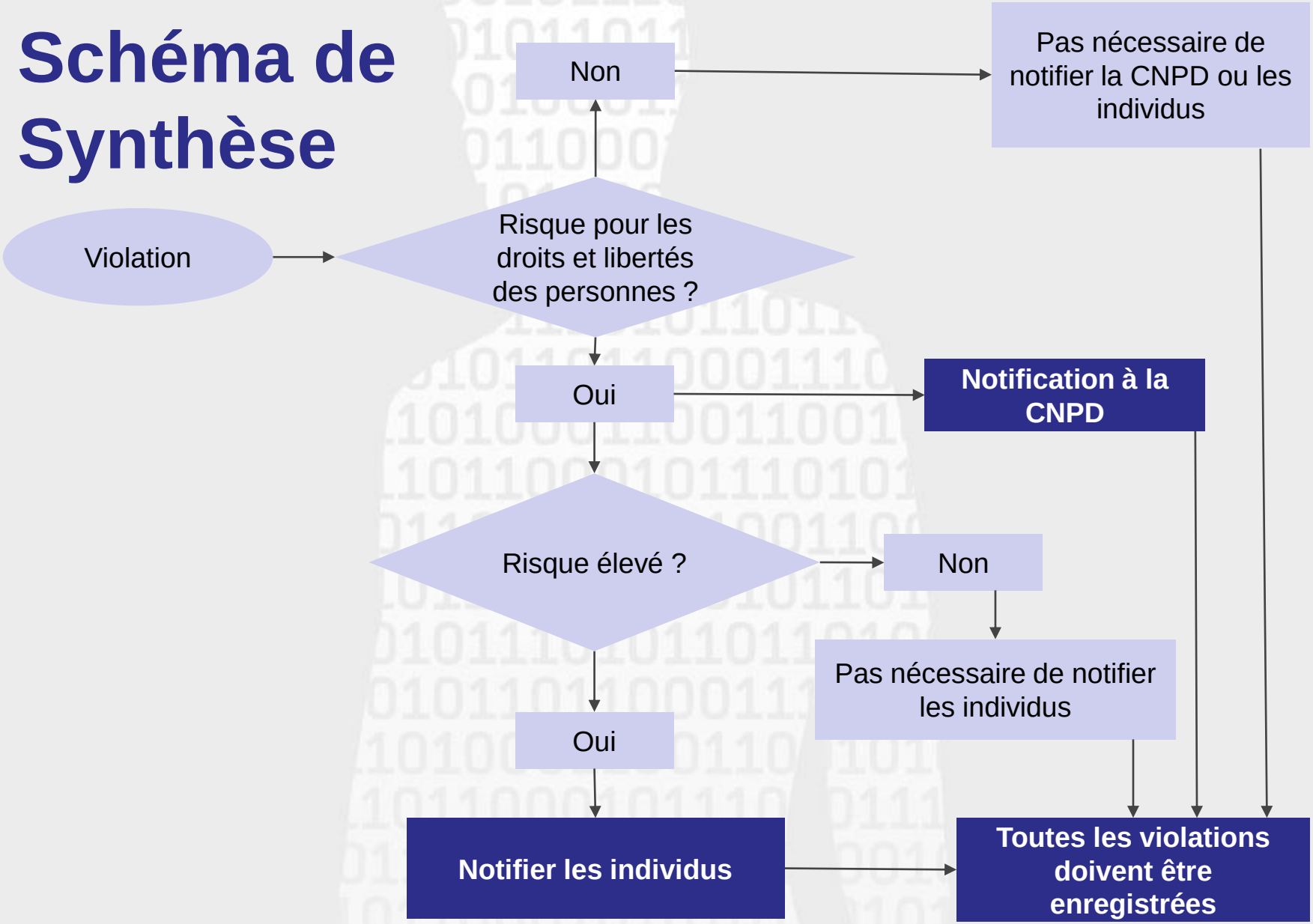
72H

CNPD COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Sous traitant

Responsable de traitement

Schéma de Synthèse



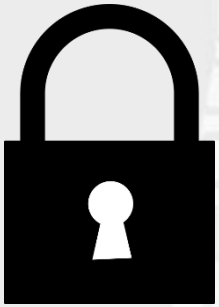
Agenda

Introduction

Notions et concepts

Obligations sous RGPD

Elements en place au Lux.



Section dédiée sur le site cnpd.lu

- Une section FAQ
- Une adresse email pour notifier
- Un formulaire (EN/FR)
- Utilisation sur une base volontaire jusqu'au 25/05/2018

Commission nationale pour la protection des données

1, avenue du Rock’n’Roll
L-4361 Esch-sur-Alzette (Belval)
261060-1
www.cnpd.lu
info@cnpd.lu