ALLEN & OVERY

Mise en conformité, transparence et sécurité des données : la responsabilité des entreprises

Elisabeth GUISSART, 25 mai 2011

Introduction

SOMMAIRE

INTRODUCTION
PRINCIPES DE BASE

Que doivent faire les entreprises?

- Respecter les règles et grands principes de la protection des données
- Respecter les droits des personnes concernées
- Garantir la sécurité et la confidentialité des données
- Notifier les traitements à la CNPD ou obtenir son autorisation

Par principe, tout acte de traitement de données personnelles est soumis à conditions

INTRODUCTION
DÉFINITIONS

Donnée personnelle

Toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une **personne identifiée ou identifiable**

Personne identifiée ou identifiable

Une personne est réputée identifiable si elle peut être identifiée, **directement ou indirectement**, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique

CHAMP D'APPLICATION
TRÈS VASTE

Responsable du traitement

La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, **détermine les finalités et les moyens** du traitement de données à caractère personnel.

Sous-traitant

Personne physique ou morale, autorité publique, service ou tout autre organisme qui **traite des données pour le compte** du responsable du traitement

NE PAS CONFONDRE RESPONSABLE ET SOUS-TRAITANT

IDENTIFICATION DU RESPONSABLE CRUCIALE,
PARFOIS DIFFICILE

INTRODUCTION
CRITÈRES D'APPLICATION

CRITÈRE INDIFFÉRENT

Recours à des moyens automatisés ou informatiques

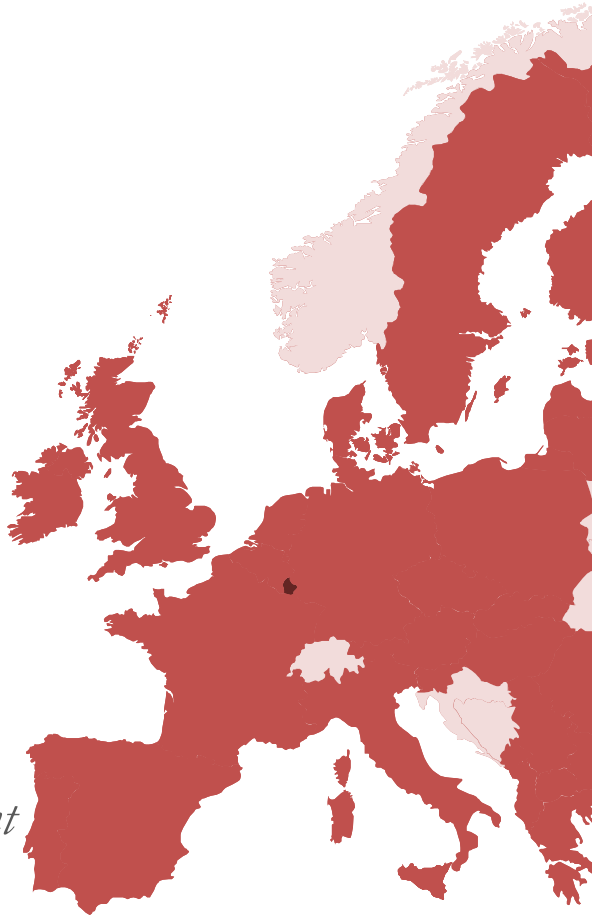
La Loi s'applique également aux traitements manuels

CRITÈRE TERRIORIAL

La Loi s'applique:

- *Lorsque le responsable du traitement est établi au Luxembourg*

- *Lorsque le responsable du traitement est établi en dehors de l'UE mais a recours à des moyens de traitement au Luxembourg (sauf simple transit)*



INTRODUCTION
SANCTIONS

Sanctions administratives

- avertissement ou admonestation
- verrouillage, effacement ou destruction des données
- interdiction temporaire ou définitive du traitement
- publication de la décision

Sanctions pénales

-8 jours à 1 an de prison
-amende de EUR 251,- à 125.000,-
-cessation du traitement
-astreinte

Sanctions civiles

- action en cessation
- responsabilité civile (peu probable)

Risque juridique

- valeur et opposabilité du traitement
- jurisprudence (Wagner, droit du travail)

ALLEN&OVERY

Grands principes

SOMMAIRE

GRANDS PRINCIPES
LICÉITÉ, LOYAUTÉ

Tout traitement doit être en conformité avec la Loi

Tout traitement doit être conforme aux grands principes et respecter les droits des personnes concernées

GRANDS PRINCIPES
QUALITÉ DES DONNÉES

CE QUE DIT LA LOI

Article 4 de la Loi

[Les données doivent être traitées:]

- pour des finalités déterminées, explicites et légitimes, et ne doivent pas être traitées ultérieurement de manière incompatible avec ces finalités
- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement
- exactes et si nécessaire mises à jour
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités

Les données doivent respecter les principes de:

- *finalité*
- *pertinence*
- *exactitude*
- *rétention proportionnée*

GRANDS PRINCIPES
LÉGITIMITÉ

Rappel

PAR PRINCIPE, TOUT TRAITEMENT
EST SOUMIS À CONDITIONS

Un traitement est légitime
s'il correspond à l'un des cas d'ouverture prévus par la Loi, qui dépendent du type de traitement...

TRAITEMENT «STANDARD»

Données sensibles
Secteur de la santé
Données judiciaires
Surveillance (tiers)
Surveillance (employés)

- OBLIGATION LÉGALE
- INTÉRÊT PUBLIC IMPORTANT
- CONTRAT/MESURES PRÉ-CONTRACTUELLES AVEC LA PERSONNE CONCERNÉE
- INTÉRÊT LÉGITIME DU RESPONSABLE /DROITS ET LIBERTÉS DE LA PERSONNE
- INTÉRÊT VITAL DE LA PERSONNE CONCERNÉE
- CONSENTEMENT DE LA PERSONNE CONCERNÉE

etc...

GRANDS PRINCIPES

FINALITÉ

La finalité est le but recherché par le responsable du traitement et qui justifie le traitement...

LES FINALITÉS DOIVENT ÊTRE DÉTERMINÉES À L'AVANCE

LES FINALITÉS DOIVENT ÊTRE LÉGITIMES

TOUTES LES FINALITÉS DOIVENT ÊTRE DIVULGUÉES (TRANSPARENCE)

LES DONNÉES NE DOIVENT PAS ÊTRE TRAITÉES ULTÉRIEUREMENT POUR DES FINALITÉS INCOMPATIBLES

(«compatible»: ce à quoi la personne concernée peut raisonnablement s'attendre)

TRAITEMENT SECONDAIRE

Consentement de toutes les personnes concernées +autorisation CNPD

GRANDS PRINCIPES
PROPORTIONNALITÉ

LES ACTES
DE TRAITEMENT
DOIVENT ÊTRE
NÉCESSAIRES À ATTEINDRE
LA FINALITÉ RECHERCHÉE

LES MOYENS
DU TRAITEMENT
DOIVENT ÊTRE
PROPORTIONNÉS
À LA FINALITÉ RECHERCHÉE

Clé de voûte du système

DROITS DES PERSONNES CONCERNÉES:
DROIT À L'INFORMATION

CE QUE DIT LA LOI

Loi du 2 août 2002, article 26(1)

[Le responsable du traitement] doit fournir à la personne concernée [...] les informations suivantes [...] :

(a) l'identité du responsable [...];

(b) [les] finalités [..]du traitement;

(c) toute information [...] telle que:
- les destinataires ou les catégories de destinataires [des] données [...];
- le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse;
- l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;

Obligation pour le responsable du traitement de fournir certaines informations sur l'existence et les modalités du traitement

- Ne doit pas être analysé comme un droit pour les personnes, mais comme une véritable obligation pour le responsable du traitement
- N'implique pas le consentement de la personne concernée (amalgame courant)
- Exceptions (limitées) existent

DROITS DES PERSONNES CONCERNÉES:
DROIT D'ACCÈS ET DE RECTIFICATION

CE QUE DIT LA LOI

Loi du 2 août 2002, article 28(1)

[La personne concernée peut] obtenir sans frais, à des intervalles raisonnables et sans délais excessifs:

(a) l'accès aux données la concernant;

(b) la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que [les informations visées à l'article 26(1)];

(c) la communication [...] des données [...], ainsi que de toute information disponible sur l'origine des données;

(d) la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées

Droit pour la personne concernée a normalement accès à toutes les informations la concernant, et peut faire rectifier les erreurs

- Accès illimité en théorie
- Exceptions (limitées) existent
- Prudence recommandée avant tout refus de communiquer les données ou en cas de dissimulation de données

DROITS DES PERSONNES CONCERNÉES:
DROIT D'OPPOSITION

CE QUE DIT LA LOI

Loi du 2 août 2002, article 30(1)

[La] personne concernée [peut] :

(a) de s'opposer à tout moment pour des raisons prépondérantes et légitimes tenant à sa situation particulière, [aux traitement de leurs données];

(b) de s'opposer, sur demande et gratuitement, au traitement [...] des données à des fins de prospection; il incombe au responsable du traitement de porter l'existence de ce droit à la connaissance de la personne concernée;

(c) d'être informée avant que des données la concernant ne soient [...] communiquées à des tiers [...] à des fins de prospection et de se voir [...] offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

Droit (limité) pour la personne concernée de s'opposer au traitement de ses données

- Droit reconnu pour les traitements à des fins de prospection commerciale
- Obligations d'informer la personne concernée de ce droit
- Pour les autres traitements, le droit d'opposition est délicat à mettre en oeuvre

Sécurité

SOMMAIRE

SÉCURITÉ

OBLIGATION DE SÉCURITÉ, PRINCIPE

CE QUE DIT LA LOI

Loi du 2 août 2002, article 22(1)

Le responsable du traitement doit mettre en œuvre toutes les mesures techniques et l'organisation appropriées pour assurer la protection des données qu'il traite contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

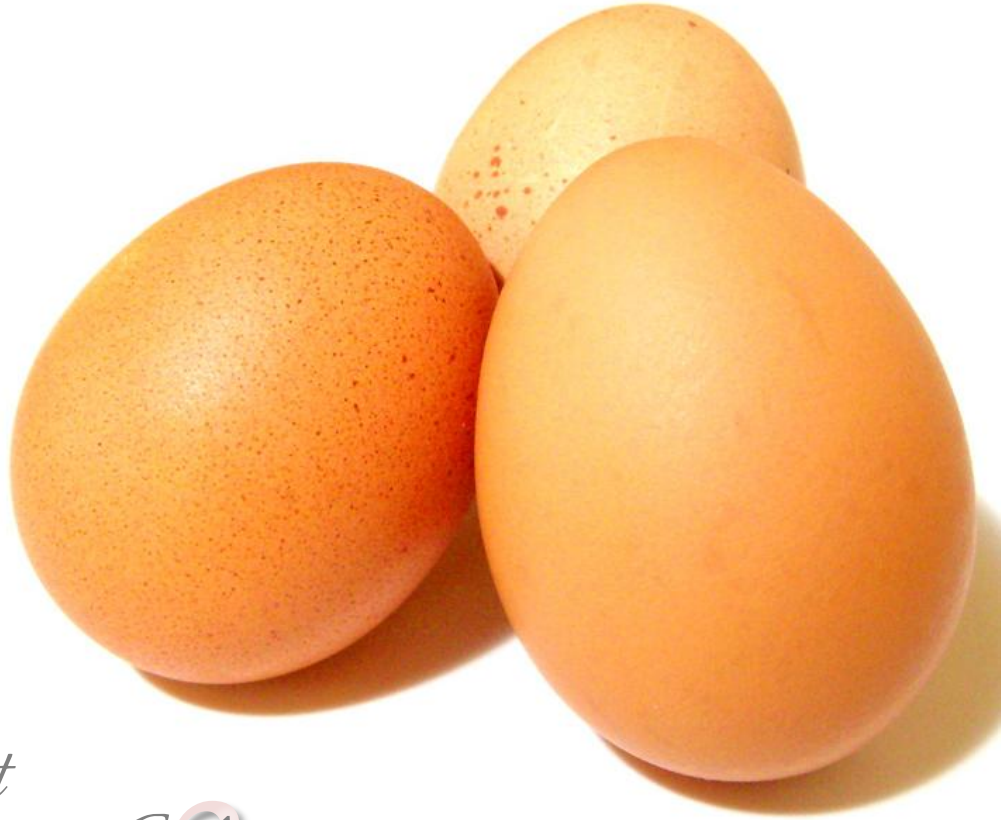
Le responsable du traitement et ses sous-traitants doivent garantir la sécurité et la confidentialité des données

Sanctions pénales possibles en cas de rupture de sécurité/confidentialité

(PEINES PLUS FORTES QUE POUR L'AUTEUR D'UNE ATTAQUE)

SÉCURITÉ

NIVEAU DE SÉCURITÉ, FACTEURS



1

Risque pour la vie privée des personnes concernées

CRITÈRE ESSENTIEL

2

Etat de l'art

OBLIGATION
DE MISE À JOUR DES
MESURES DE SÉCURITÉ

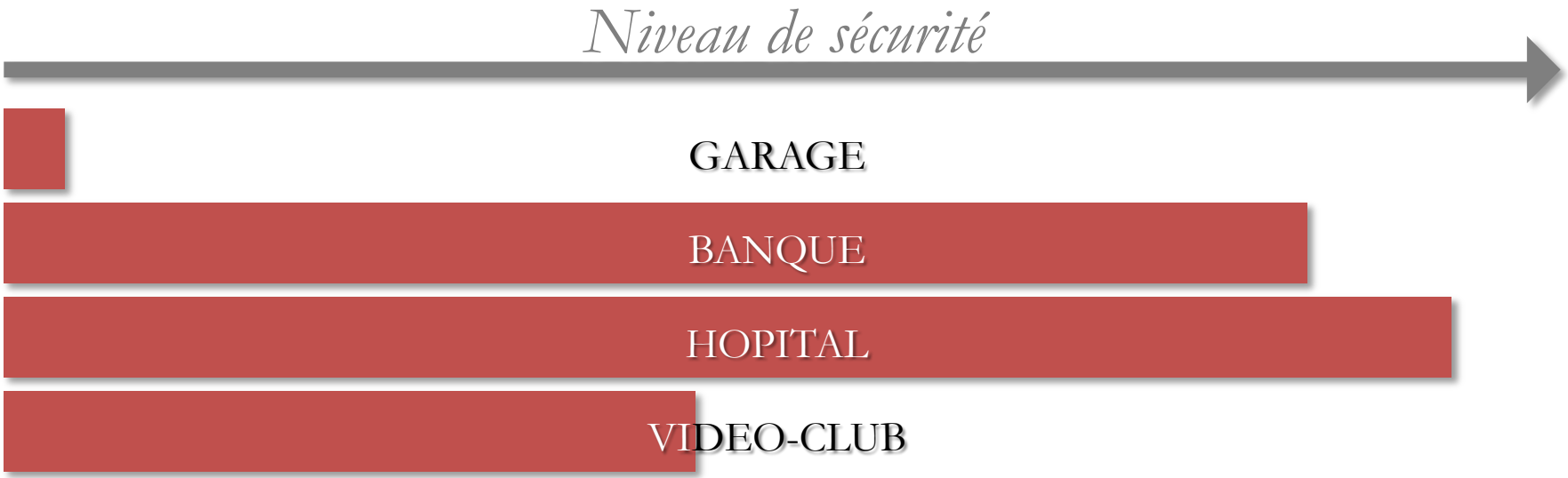
3

Coûts

FACTEUR
SUBSIDIAIRE

SÉCURITÉ

NIVEAU DE SÉCURITÉ



SÉCURITÉ

NIVEAU DE SÉCURITÉ, TYPOLOGIE

1

Contrôle à l'entrée des installations

(empêcher toute personne non autorisée d'accéder
aux installations utilisées pour le traitement de données)

ACCÈS SÉCURISÉS, SURVEILLANCE

SÉCURITÉ

NIVEAU DE SÉCURITÉ, TYPOLOGIE

2

Contrôle des supports

(empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée)

SUPPORTS CONSERVÉS SOUS CLÉ

SÉCURITÉ

NIVEAU DE SÉCURITÉ, TYPOLOGIE

3

Contrôle de la mémoire

(empêcher l'introduction non autorisée de données, toute prise de connaissance, modification ou effacement non autorisés des données)

RESTRICTION D'ACCÈS AU SYSTÈME

SÉCURITÉ

NIVEAU DE SÉCURITÉ, TYPOLOGIE

4

Contrôle de l'utilisation

(empêcher que les systèmes puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmissions de données)

PROTECTION RÉSEAU (FIREWALLS)

SÉCURITÉ

NIVEAU DE SÉCURITÉ, TYPOLOGIE

5

Contrôle de l'accès

(garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données relevant de leur compétence)

GESTION DES COMPTES, SUIVI

SÉCURITÉ

NIVEAU DE SÉCURITÉ, TYPOLOGIE

6

Contrôle de la transmission

(garantir que puisse être vérifiée et constatée l'identité des tiers auxquels des données peuvent être transmises par des installations de transmission)

VPN, CRYPTAGE, SIGNATURE ÉLECTRONIQUE

SÉCURITÉ

NIVEAU DE SÉCURITÉ, TYPOLOGIE

7

Contrôle de l'introduction

(garantir que puisse être vérifié et constaté a posteriori l'identité des personnes ayant eu accès au système et garantir le traçabilité des accès)

LOGGING (AUTRE TRAITEMENT? SURVEILLANCE?)

SÉCURITÉ

NIVEAU DE SÉCURITÉ, TYPOLOGIE

8

Contrôle du transport

(empêcher que, lors de la communication /transport de supports, les données puissent être lues, copiées, modifiées ou effacées sans autorisation)

CRYPTAGE DES SUPPORTS

9

Contrôle de la disponibilité

(sauvegarder les données par la constitution de copies de sécurité)

BACKUPS

Conformité

SOMMAIRE

CONFORMITÉ

CONTRÔLE INTERNE ET EXTERNE

Responsabilité dans l'entreprise

Chargé de la protection des données

Contrôle interne

LE RESPONSABLE DU TRAITEMENT
DOIT VÉRIFIER ET GARANTIR À TOUT MOMENT
LA LÉGALITÉ ET LA LOYAUTÉ DU TRAITEMENT

Contrôle externe

LA CNPD EST COMPÉTENTE
ET DISPOSE DE POUVOIRS
D'INVESTIGATION ET DE SANCTION

ALLEN&OVERY

CONFORMITÉ
FORMALITÉS

1 *Principe*

NOTIFICATION PRÉALABLE

2 *Exception*

EXCEPTION DE NOTIFICATION

3 *Exception*

AUTORISATION PRÉALABLE

4 *Exception*

AUTORISATION PAR R.G.D.

ALLEN&OVERY

CONFORMITÉ

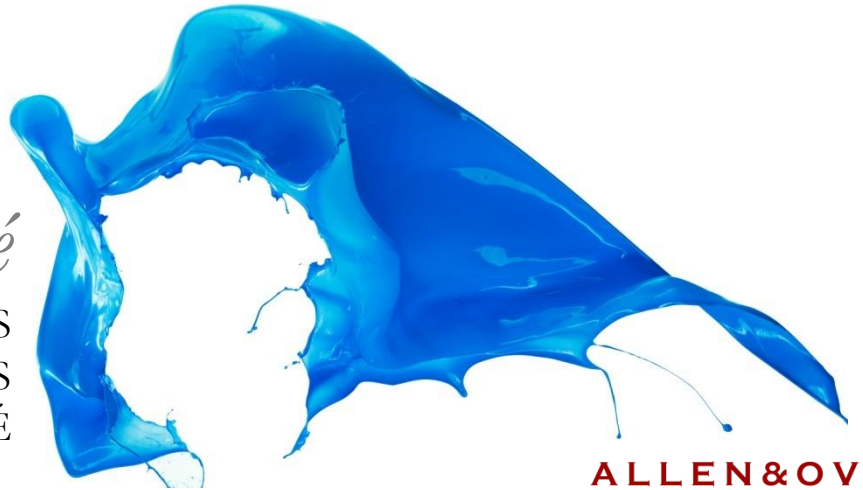
LA CONFORMITÉ DANS LE TEMPS

Mise en conformité initiale

NOTIFICATIONS
AUTORISATIONS PRÉALABLES
INFORMATION DES PERSONNES CONCERNÉES

Maintien en conformité

RESPECT DES FINALITÉS
PRINCIPE DE QUALITÉ DES DONNÉES
MISE À JOUR DE LA SÉCURITÉ



Questions?

ALLEN&OVERY