DATA PROTECTION IMPACT ASSESSMENT

Chambre de commerce -Fit4DataProtection

7 mars 2018

Mickaël TOME
AVOCAT À LA COUR

INTRODUCTION

DPIA IN A NUTSHELL
ELEMENTS DE DEFINITION

La notion d'analyse d'impact sur la protection des données (AIPD)

- Un outil de responsabilisation des organismes
- Une démarche d'identification et de gestion des risques pour les personnes
- Une AIPD doit être menée en présence de traitements de données susceptibles d'engendrer des risques élevés pour les droits/libertés des personnes (art. 35, paragraphe 1 GDPR)

DPIA IN A NUTSHELL
PRINCIPAUX OBJECTIFS

Principaux objectifs:

- s'assurer que l'on met en œuvre un traitement respectueux de la vie privée
- apprécier l'impact des traitements de données sur la vie privée
- démontrer que les principes essentiels du GDPR sont respectés

Un corollaire du principe d'*accountability*

- Accountability = être en mesure de démontrer sa conformité
- Documenter les mesures prises pour assurer la conformité

/c

UNE APPROCHE PAR LES RISQUES SUR LA VIE PRIVEE

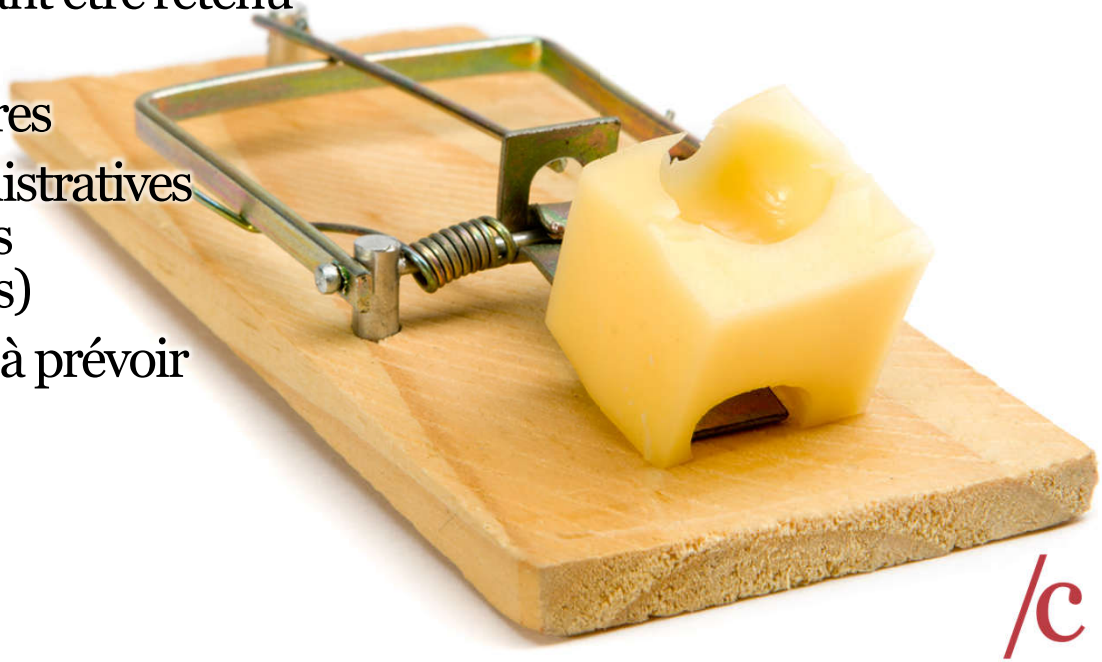
La notion de risque sur la “vie privée”

- Un événement indésirable/redouté (accès non autorisé, modification non désirée ou disparition de données) / impacts potentiels sur les droits & libertés
- Gravité /probabilité: des éléments déterminés en fonction de la nature, de la portée, du contexte et des finalités du traitement
- Des risques à identifier, analyser, évaluer, traiter & réexaminer régulièrement
- Enjeu = apprécier les risques liés à la mise en œuvre du traitement du point de vue des personnes.
- Des traitements susceptibles d’entraîner des dommages physiques, matériels ou un préjudice moral

PROTECTION DES DONNÉES
SANCTIONS – art. 83(4)(a) RGPD

Jusqu'à EUR10mio/2% du CA mondial annuel

- des sanctions «effectives, proportionnées et dissuasives»
- le montant le plus élevé pouvant être retenu
- un moyen d'attirer l'attention
  des directions / des actionnaires
- un système d'amendes administratives
  remplace les amendes pénales
  (non prononcées donc inutiles)
- des sanctions plus fréquentes à prévoir



/c

COMMENT REPÉRER UN TRAITEMENT DE DONNÉES À RISQUE ÉLEVÉ ?

QUELS TRAITEMENTS NECESSITENT UNE AIPD?
ARTICLE 35 GDPR

Lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits & libertés

- Risque potentiellement élevé pour les droits & libertés des personnes, compte tenu de la nature, de la portée, du contexte et des finalités du traitement

En particulier dans les cas suivants:

- Evaluation systématique et approfondie de la personnalité, sur base d'un traitement automatisé (not. profilage) + décisions produisant des effets juridiques/significatifs
- Traitement à grande échelle de données sensibles ou judiciaires
- Surveillance systématique à grande échelle de lieux accessibles au public

DANS QUELLES SITUATIONS EST-IL RECOMMANDE DE REALISER UNE AIPD?

LES CRITERES DU G29

En présence d'au moins deux des critères suivants:

- Evaluation ou notation (y compris le profilage)
- Décisions automatisées avec effet juridique ou effet similaire significatif
- Surveillance systématique
- Collecte de données sensibles
- Traitement à grande échelle
- Croisement ou combinaison de différents jeux de données
- Personnes vulnérables
- Technologies innovantes
- Exclusion du bénéfice d'un droit/service/contrat

/c

Ex. d'opérations de traitement	Critères potentiellement pertinents	AIPD potentiellement requise?
Traitement par un hôpital de données génétiques/de santé	- Données sensibles - Données concernant des personnes vulnérables - Données traitées à grande échelle	OUI
Utilisation d'un système de caméras pour surveiller les comportements routiers + dispositif d'analyse intelligente pour isoler les véhicules et reconnaître les plaques d'immatriculation	- Surveillance systématique - Technologie innovante	OUI
Surveillance systématique par une entreprise des activités de ses employés, y compris leur poste de travail, leur activité sur internet…	- Surveillance systématique - Personnes vulnérables	OUI
Collecte de données sur les réseaux sociaux publics dans le but de générer des profils	- Evaluation ou notation - Traitement à grande échelle - Croisement ou combinaison de jeux de données - Données sensibles / à caractère hautement personnel	OUI
Utilisation par un magazine en ligne d'une liste de diffusion pour communiquer à ses abonnés sa newsletter quotidienne	Aucun	NON
Diffusion par un site de commerce électronique de publicités ciblées basé sur les habitudes de consommation des visiteurs	- Evaluation ou notation	NON

QUAND REALISER UNE AIPD?

QUAND REALISER UNE AIPD?

Pour tout traitement susceptible d'engendrer des risques élevés pour les droits & libertés:

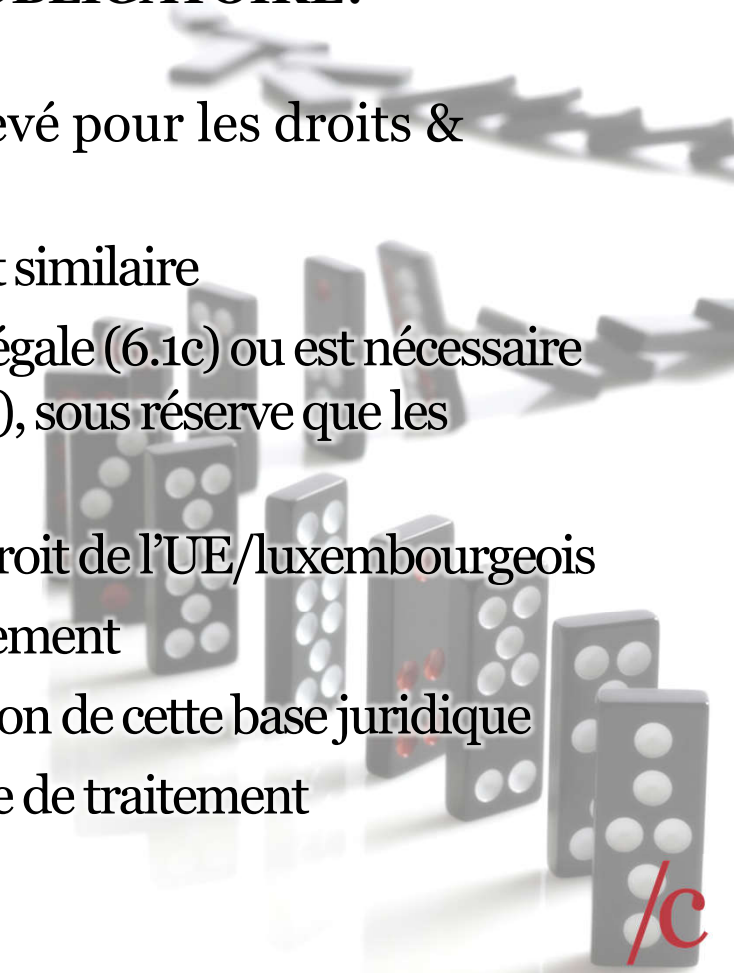
- Avant de collecter des données / mettre en œuvre le traitement, et le plus en amont possible
- La nécessité d'une réévaluation et d'une actualisation régulière et continue, tout au long du cycle de vie du traitement

UNE AIPD PEUT-ELLE ETRE REALISEE SUR UN OU PLUSIEURS TRAITEMENTS?

- Une seule et même AIPD pour un ensemble d'opérations de traitements similaires qui présentent des risques élevés similaires
- Cas dans lesquels il peut être raisonnable et économique d'élargir la portée de l'AIPD au-delà d'un projet unique

QUAND EST-CE QU'UNE AIPD N'EST PAS OBLIGATOIRE?

- Le traitement ne présente pas de risque élevé pour les droits & libertés des personnes
- Une AIPD a déjà été réalisée pour un traitement similaire
- Lorsque le traitement répond à une obligation légale (6.1c) ou est nécessaire à l'exercice d'une mission de service public (6.1e), sous réserve que les conditions suivantes soient réunies:
  - le traitement a une base juridique dans le droit de l'UE/luxembourgeois
  - ce droit règlemente cette opération de traitement
  - une DPIA a déjà été réalisée lors de l'adoption de cette base juridique
- Quand la CNPD n'exige pas d'AIPD pour ce type de traitement conformément à l'article 35(5) GDPR.



LE CONTENU D'UNE DPIA

CONTENU D'UNE DPIA

Description systématique des opérations de traitement et des finalités

Evaluation de la nécessité et de la proportionnalité des opérations de traitement

Evaluation des risques pour les droits et libertés des personnes concernées

Mesures envisagées pour faire face aux risques

/c

QUELLE METHODE POUR REALISER UNE AIPD?

Une liberté de choix de la méthode

- Les cadres européens existants (DE, ES, FR, UK)
- La possibilité de prévoir un cadre sur mesure

Des critères à respecter (recommandations G29)

- Des critères tenant au contenu: description systématique du traitement, évaluation de la nécessité et de la proportionnalité, gestion suffisante des risques pour les droits/libertés
- Une implication des différentes parties intéressées
  - Responsable tu traitement, DPO, experts métiers, sous-traitant, personnes concernées

DANS QUEL CAS CONSULTER LA CNPD?

LA CONSULTATION PREALABLE DE LA CNPD

Consultation obligatoire dans les hypothèses suivantes:

- si le risque résiduel demeure élevé
- si la législation nationale l'exige
- en cas de contrôle de la CNPD

Une obligation de publication de l'AIPD?

CONCLUSION
EN 2 MOTS

- Une démarche rationnelle importante et complexe pour assurer sa conformité à GDPR, mais qui ne doit pas être surjouée
- Un processus itératif à réaliser tout au long du cycle de vie des traitements
- Un changement de mentalités de nature à intégrer la protection des données dans la vie quotidienne des organisations

/c

MICKAËL TOME
Avocat à la Cour
(+352) 691 551 155
mt@claw.lu
24 rue Jean l'Aveugle L-1148 Luxembourg