Se mettre en conformité au Règlement Général sur la Protection des Données

Agnès Maqua
Nicolas Hamblenne

promAndenne

KOAN

CLOSE TO YOU

KOAN

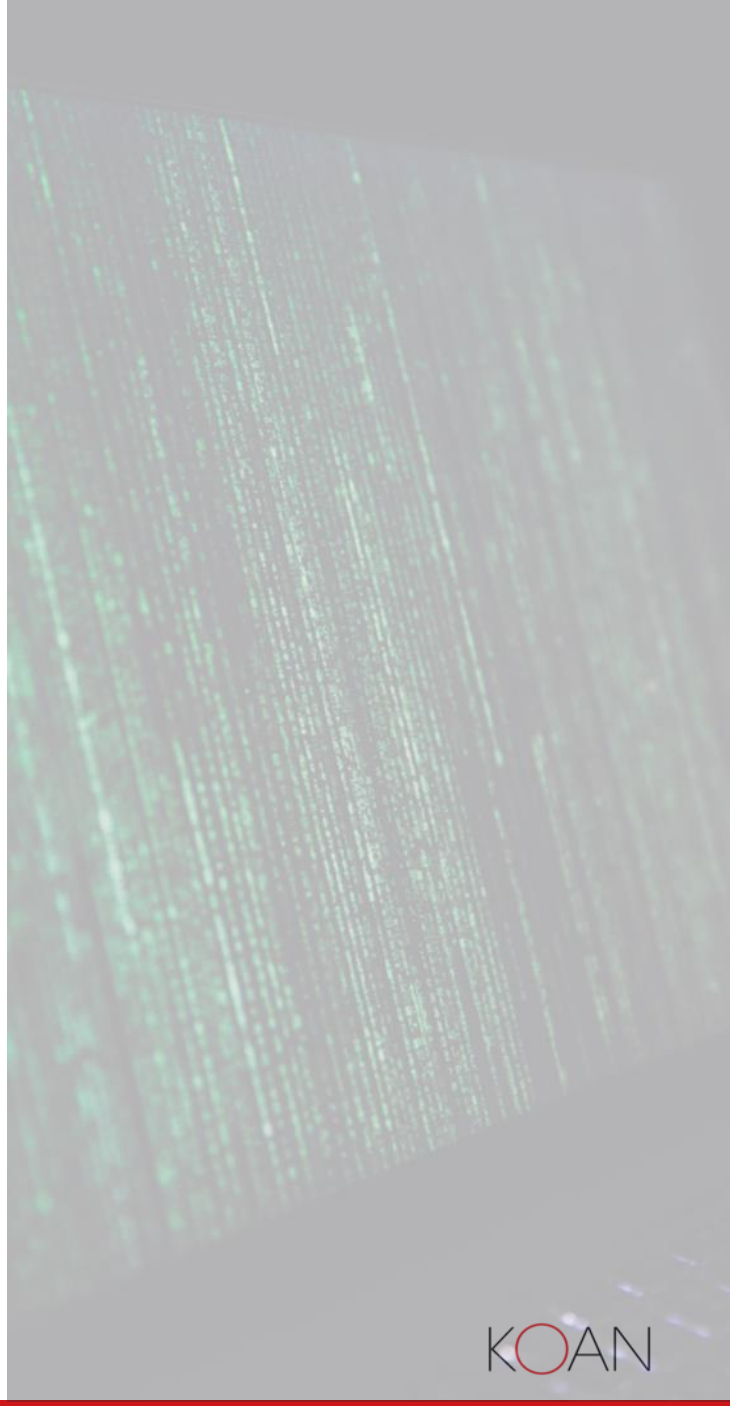
The companies that do the best job on managing a user's privacy will be the companies that ultimately are the most successful.

Fred Wilson (2015)

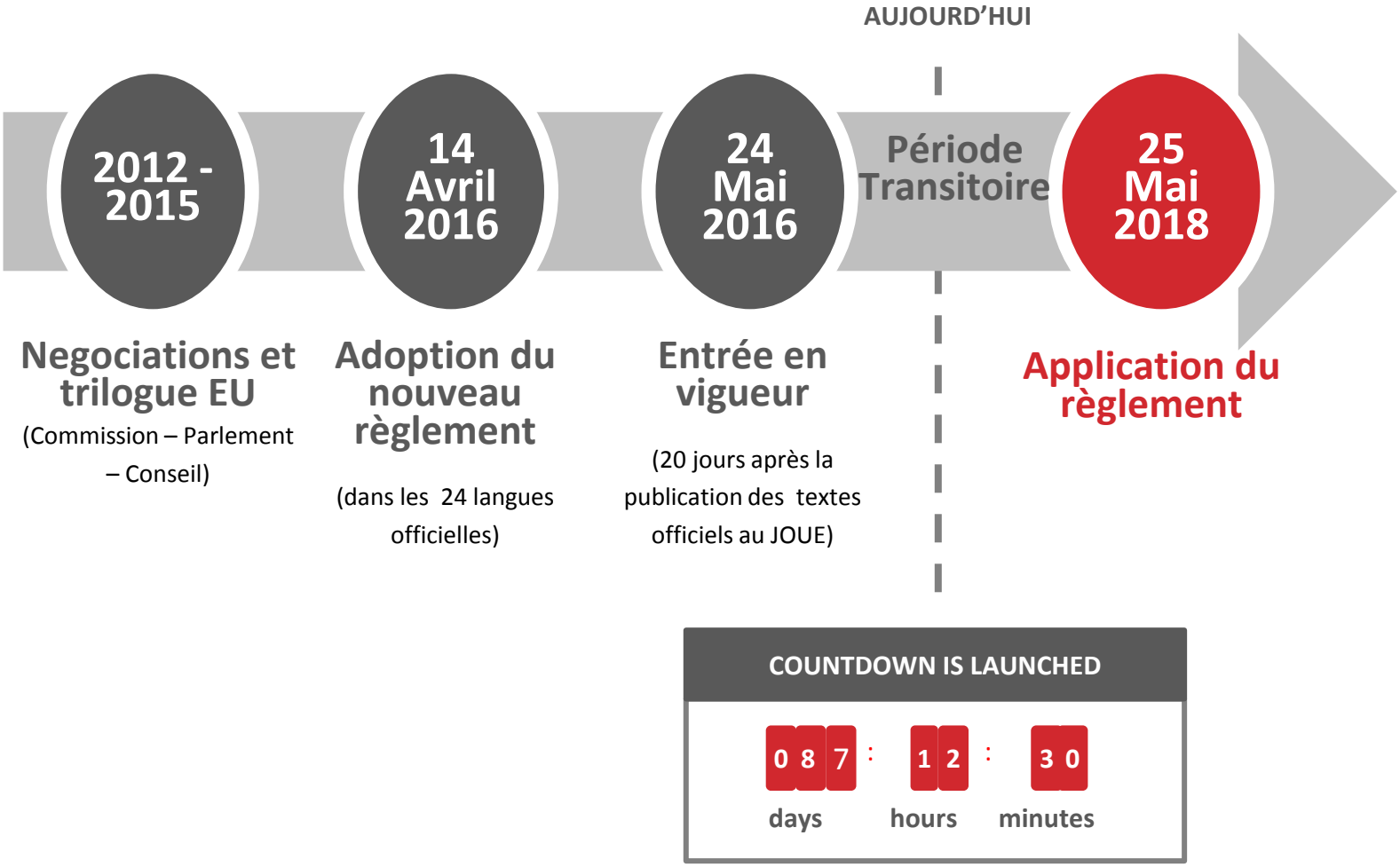
(Venture Capitalist and Co-Founder of Union Square Ventures)

KOAN

TABLE DES MATIERES



GDPR: calendrier et ligne du temps



KOAN

II. VIE PRIVEE
Concepts et Principes

KOAN

Cadre législatif

Loi sur la protection de la vie privée

Loi belge *du* ***8 Décembre 1992*** *sur la protection de la vie privée à l'égard des traitements de données à caractère personnel.*

Directive sur la protection des données personnelles

Directive *95/46/CE du Parlement européen et du Conseil, du* ***24 octobre 1995****, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.*

Règlement Général sur la Protection de Données

Règlement *(UE) 2016/679 du Parlement européen et du Conseil du* ***27 avril 2016*** *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD).*

KOAN

Directive vs. Règlement

Directive Données Personnelles

- ✓ Directive (1995) non adaptée aux nouvelles technologies
- ✓ Fragmentation et incohérence dues aux interprétations des 28 EM
- ✓ Manque d'application dû à l'absence de sanctions

GDPR

- ✓ Adaptation du cadre légal à une société digitale globalisée
- ✓ "Un seul cadre légal pour tous"
- ✓ Davantage de droits garantis aux individus
- ✓ Davantage d'obligations imposées aux organisations
- ✓ Davantage de sanctions et de contrôle

KOAN

Différents types de données personnelles

DONNÉES PERSONNELLES

Toute information concernant une personne physique identifiée ou indentifiable.

- Nom
- Photo
- Numéro de téléphone (personnel/professionel)
- Numéro de compte bancaire
- Adresse email
- IT (Addresses IPv4, IPv6, Mac address, DeviceID, …)
- Plaque d'immatriculation

DONNÉES PSEUDONYMES

Données qui ne peuvent être associées à une certaine personne sans information complémentaire.

DONNÉES PERSONNELLES SENSIBLES

- Dossier médical (données génétiques et de santé)
- Empreinte digitale (données biométriques)
- Dossier juridique
- Origine ethnique / race
- Orientation sexuelle (comportement ou préférence)
- Préférence politique
- Vue religieuse / idéologique
- Appartenance syndicale

DONNÉES ANONYMES

Données n'étant ni personnelles, ni pseudonymes.

KOAN

Traitement des données et acteurs impliqués

TRAITEMENT

Toute opération effectuée avec des données personnelles, de façon automatisée ou non, telle que:

- La collecte, l'enregistrement, l'organisation,
- Le stockage, l'adaptation ou l'altération,
- L'extraction, la consultation, l'usage,
- La communication par transfert, la dissémination,
- La synchronisation ou la combinaison,
- Le bloquage, l'effacement ou la destruction.

RESPONSABLE DU TRAITEMENT

- La personne qui détermine les **moyens** et les **finalités** d'un traitement.

SOUS-TRAITANT

- Toute personne traitant des données à caractère personnel **pour le compte du responsable du traitement**.

KOAN

Principes généraux

Légalité	Le traitement doit reposer sur une base légale	**Finalité**	But spécifique, adéquat et légitime

Proportionnalité	▪ Données précises, pertinentes et nécessaires (non excessives) ▪ Données exactes et à jour ▪ Période de conservation raisonnable
Sécurité et confidentialité	▪ Protection de l'accès aux données (serveurs sécurisés, mots de passe etc.) ▪ Accords de confidentialité

KOAN

Principes généraux: principe de légalité

6 bases légales permettant un traitement des données personnelles:

Consentement

Nécessaire à l'**exécution d'un contrat**

Obligation légale

Protection de l'**intérêt vital**

Missions **d'intérêt public** ou exercice de **l'autorité publique**

Intérêt légitime du responsable ou de la tierce partie

KOAN

Les droits de la personne concernée

ACCÈS

RECTIFICATION

EFFACEMENT

DROIT À L'OUBLI

REFUS

RESTRICTION

INFORMATION

PORTABILITÉ

POLITIQUE DE CONFIDENTIALITE (Privacy Policy)

KOAN

Transfert de données personnelles à l'étranger

TRANSFERT

AU SEIN DE L'ESPACE ECONOMIQUE EUROPEEN

→ **Pas d'obstacle**

TRANSFERT

VERS DES PAYS HORS ESPACE ECONOMIQUE EUROPEEN

↓

CE PAYS A-T-IL **UN NIVEAU DE PROTECTION ADEQUAT** ?

OUI:

PAYS SUR **LISTE BLANCHE**

(Suisse, Andorre, Argentine, Guernsey, l'île de Man, les Îles Feroes, Jersey, Israël, Nouvelle-Zélande et Uruguay, …)

→ **Pas d'obstacle**

NON:

USA: Binding Corporate Rules, EU Commission's model clauses, or EU-US Privacy Shield

Autres pays: Binding Corporate Rules, EU Commission's model clauses

KOAN

III. 5 ENJEUX CLES DU RGDP

I. Consentement

II. Intérêt légitime

III. Notification de fuite

IV. Responsabilité et sanctions

V. Le Délégué à la Protection de Données (DPO)

KOAN

I. Le consentement

Consentement pour les catégories ordinaires de données

- **Libre**
- **Spécifique**
- **Eclairé**
- **Univoque**

Consentement pour les catégories spéciales de données

Le consentement doit (en plus) être **explicite** (non défini mais plus exigeant encore que le consentement «ordinaire»)

Consentement parental nécessaire pour les **enfants agés de moins de 13 à 16 ans** (appréciation de chaque Etat Membre)

Exemples:

Bandeau cookie (ou cookie policy) sur le site internet

“opt-in” explicite pour un nouveau compte (utilisateur)

KOAN

II. L'intérêt légitime

L'intérêt légitime vs **l'attente légitime**

- Mise en **balance des intérêts** (sur base d'une analyse au cas par cas)

(47) **Les intérêts légitimes d'un responsable du traitement**, y compris ceux d'un responsable du traitement à qui les données à caractère personnel peuvent être communiquées, ou d'un tiers **peuvent constituer une base juridiqu**e pour le traitement, **à moins que les intérêts ou les libertés et droits fondamentaux de la personne concernée ne prévalent**, compte tenu des attentes raisonnables des personnes concernées fondées sur leur relation avec le responsable du traitement. Un tel intérêt légitime pourrait, **par exemple**, exister lorsqu'il existe une relation pertinente et appropriée entre la personne concernée et le responsable du traitement **dans des situations telles que celles où la personne concernée est un client du responsable du traitement ou est à son service**. (…)

Le traitement de données à caractère personnel à des fins de prospection peut être considéré comme étant réalisé pour répondre à un intérêt légitime.

Important à des fins de **Marketing**

- Cartes de visite
- Opt-out
- Documenter l'information

KOAN

III. Notification de fuite

Quand ?

Toute fuite de données personnelles doit être **notifiée par le responsable du traitement à l'autorité de contrôle**, endéans les 72 heures de la découverte

Qui ?

La **notification aux personnes concernées** doit avoir lieu **"dans les plus brefs délais"** si la fuite peut constituer un "**risque élevé**" pour celles-ci

Exceptions

Pas de notification à l'autorité de contrôle si la fuite **n'est pas « susceptible d'engendrer un risque pour les droits et libertés des personnes physiques »**

Pas de notification aux personnes concernées si la fuite **n'est pas « susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique »**

Notification en chaîne

Le **sous-traitant** doit notifier les fuites de données personnelles au **responsable** de traitement qui notifiera à son tour à l'autorité de contrôle

KOAN

IV. Responsabilité…

- **Plus lourde** que dans la Directive (95)
- Réel besoin de **démontrer la conformité** avec le GDPR
  - **Mise en place de procédures internes**
  - **Révision régulière** et **évaluation des mesures** de protection des données
  - Adoption ou approbation de **codes de conduite**
  - **Registre des activités de traitements**

Pas de registre des activités de traitements (exception)

- **Exception** pour les companies comptant moins de 250 employés **à condition que** :

  (i) le traitement ne soit pas susceptible de comporter un risque pour les droits et des libertés des personnes concernées; **et que**
  (ii) le traitement soit occasionnel; **et qu'**
  (iii) aucune **donnée sensible** ne soit traitée.

KOAN

… Et sanctions

Jusqu'à 10M€ ou 2% du chiffre d'affaire mondial

Pour les affaires portant sur :

- Un échec en matière de **sécurité du traitement**
- Des infractions concernant le respect de la vie privée "**by design / by default"**
- Le **Délégué à la Protection des Données**
- Manquement en matière de **notification d'une violation des données**
- …

Jusqu'à 20M€ ou 4% du chiffre d'affaire mondial

Pour les affaires portant sur :

- **Les données sensibles**
- **Les transferts** de données personnelles
- Le non-respect d'une **décision de l'autorité de surveillance**
- **Le consentement de la personne concernée**
- …

KOAN

V. Le Délégué à la Protection des Données (DPO)

- DPO : **Personne de contact** pour les questions relatives aux **données** d'une **personne concernée**.

- **Rôle central** : Etre associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

DPO obligatoire pour certaines organisations

- ✓ Celles qui sont considérées comme des **autorités ou entités publiques**
- ✓ Dont les activités principales nécessitent un **monitoring** régulier et systématique des **personnes concernées sur une large échelle**.
- ✓ Dont les activités principales consistent en un **traitement** sur une large échelle de **données sensibles**.

KOAN

V. Le Délégué à la Protection des Données (DPO)

Pré-requis

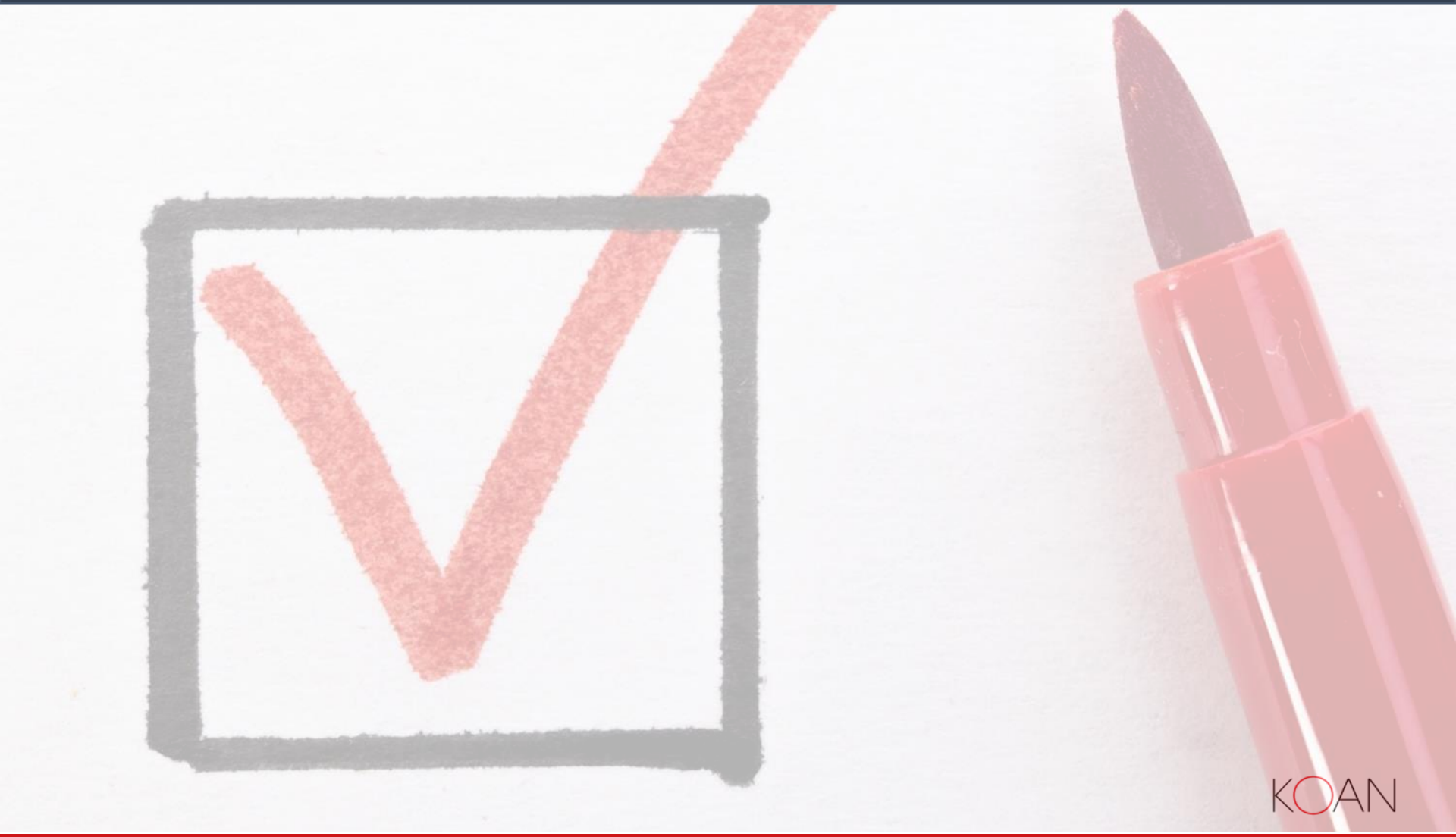
- ✓ Niveau d'expertise
- ✓ Questions liées à la DP (manière appropriée et en temps utile)
- ✓ Ressources nécessaires (personnel, temps, moyens financiers, ...)
- ✓ Autonomie complète (employé OU externe)
- ✓ Aucun conflit d'intérêts (ne peut pas être le CEO, COO, CFO, CMO, etc.)

Tâches

- ✓ Informer , éduquer et conseiller le responsable / sous-traitant et les employés
- ✓ Assurer la conformité avec le GDPR
- ✓ Point de contact et coopération avec l'autorité de surveillance
- ✓ + ...

KOAN

IV. COMMENT SE PREPARER AU GDPR EN 6 ETAPES



Se préparer en 6 étapes

Votre “to-do” liste :

Désigner un pilote (ou DPO/Personne responsable)

Procéder à un audit interne des traitements de données (Registre des activités de traitements)

Assurer le suivi et l’implémentation du rapport d’audit (actions et priorités)

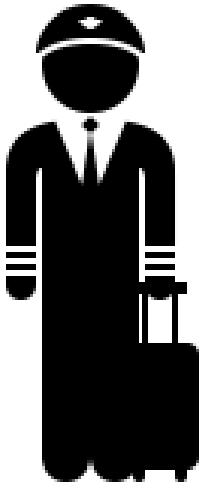
Gérer les risques (PIA)

Organiser les procédures internes

Documenter la conformité

KOAN

Étape 1. Désigner un pilote



NOS RECOMMANDATIONS

Désigner un PILOTE, dès maintenant

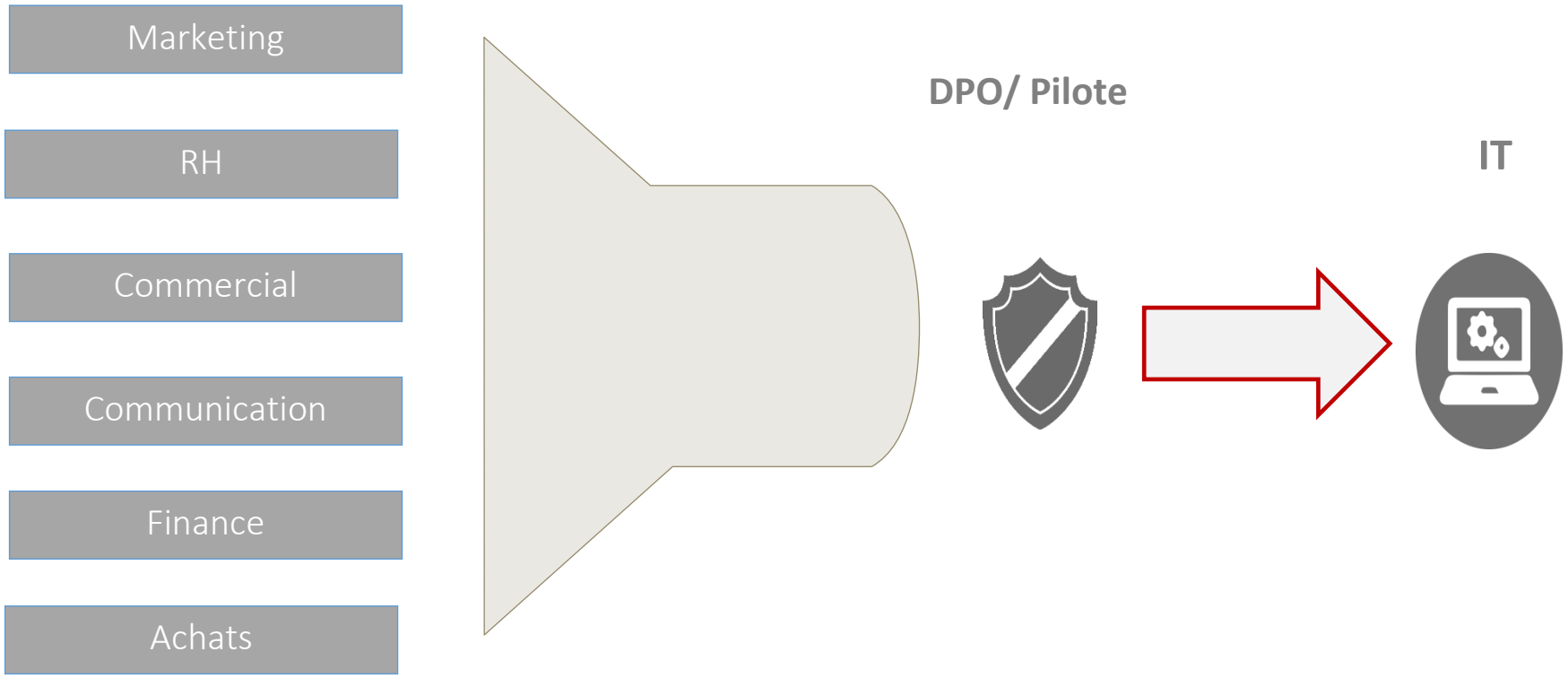
Définir ses missions et tâches

Officialiser sa nomination et ses missions en interne

Assigner les ressources humaines et financières adéquates

KOAN

Étape 2. Procéder à un audit interne des traitements de données (Registre) – Approche Top-down



KOAN

DATA PROTECTION AUDIT

KOAN

GDPR AUDIT CHECKLIST

- Quelles données?
- Quelle base légale?
- Combien de temps?
- Comment sont-elles collectées ?
- Qui les collecte?
- Où sont-elles stockées ?

KOAN

IDENTIFICATION DU TRAITEMENT				ACTEURS	FINALITE DU TRAITEMENT	TRANSFERT HORS UE	DONNEES SENSIBLES
Nom / sigle	N° / REF	Date de création	Dernière mise à jour	Responsable du traitement	Finalité principale	Oui /non	Oui/non
	ref-001						
	ref-002						
	ref-003						

REGISTRE EUROPEEN GDPR | **FICHE DE TRAITEMENT** | **ref-001** | KOAN Law Firm

DESCRIPTION DU TRAITEMENT

Nom / sigle	
N° / REF	ref-001
Date de création	
Mise à jour	

ACTEURS	Nom	Adresse	CP	Ville	Pays	Tél
Responsable du traitement						
Délégué à la protection des données/Data Manager						
Représentant						
Responsable(s) conjoint(s)						

FINALITE (S) DU TRAITEMENT EFFECTUE

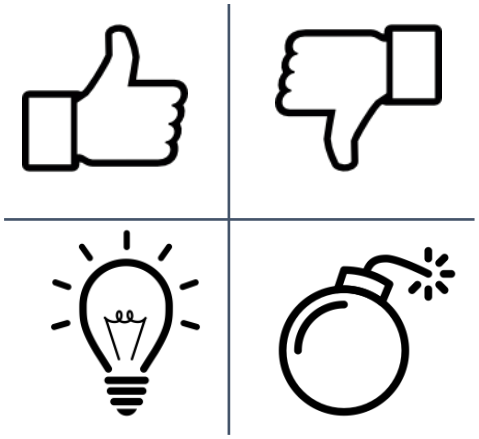
Finalité principale	
Sous-finalité 1	
Sous-finalité 2	
Sous-finalité 3	
Sous-finalité 4	
Sous-finalité 5	

MESURES DE SECURITE

Mesures de sécurité techniques	
Mesures de sécurité organisationnelles	

Étape 3. Assurer le suivi et l’implémentation du rapport d’audit

- Le rapport d'audit révèle des problèmes et des opportunités
- Planification et implémentation immédiate des solutions en ce qui concerne les problèmes les plus urgents.
- Mise en place des autres solutions en vue d’éliminer tous les problèmes
- Évaluation des politiques internes



KOAN

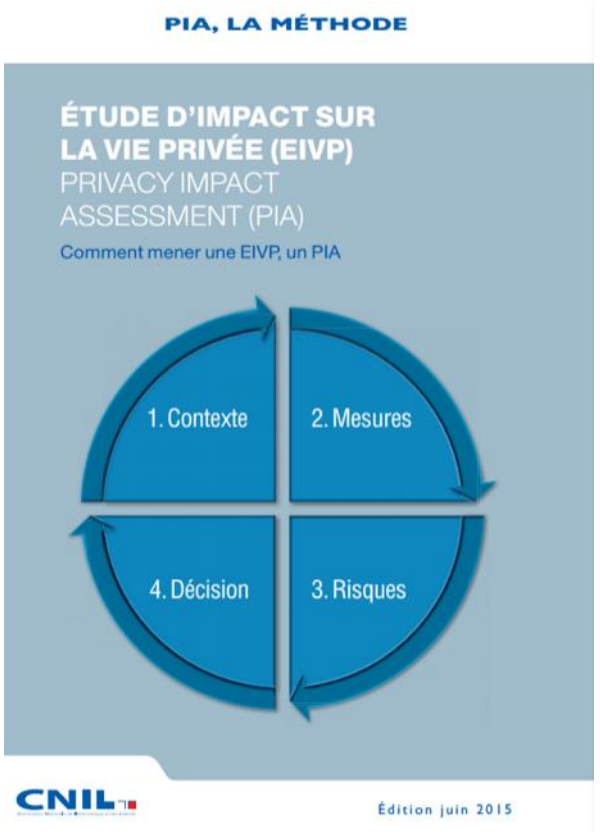
Étape 4. Gérer les risques (PIA)

Risques substantiels ➔ PIA ou EIVP (Etude d'Impact sur la Vie Privée)

- Quand doit-on conduire une EIVP ?
- Ex: Geolocalisation system for corporate vehicules

- Qu'en est-il pour cette EIVP ?
- Privacy by design

Prendre en compte l'**impact des futurs produits**, **processus** et **technologies** sur la protection des données personnelles, au moment de leur implémentation (anticiper, réfléchir préventivement)



Étape 5. Organiser les procédures internes

- **Information**, **éducation**, **conscientisation** des collaborateurs;
- Analyses, mises-à-jour et ajustements **réguliers;**
- Guidelines;
- Procédures pour les réclamations et les demandes d'informations;
- Reflexe du « privacy by design »
- BUT = **la protection de la vie privée doit faire partie de l'ADN de l'entreprise (intuitive)**

KOAN

Étape 6. Documenter la conformité

- Registre des activités de traitement
- Etude d'Impact sur la Vie Privée (si nécessaire)
- Lignes directrices et documents internes
  - Data Breach Scenario (Scenario de violation/fuite des données personnelles)
  - IT Security policy (Politique de sécurité en matière d'IT)
  - Working rules (Règlement de travail)
- Contrats et clauses vie privée
  - Responsable du traitement / Sous-traitant / Sous-contractant

KOAN

Processus de mise en conformité

INDIVIDUEL

COLLECTIF

KOAN

V. Q&A

KOAN

Thank you

Agnès Maqua: am@koan.law

Nicolas Hamblenne: nha@koan.law

Ch. de la Hulpe 166 Terhulpsesteenweg
B-1170 Brussels
Belgium

+32 2 566 90 00

47 rue de Monceau
F-75008 Paris
France

+33 1 56 69 71 20

www.koan.law

@KoanLaw

www.linkedin.com/company/koan