7 avril 2016

Privacy By Design – Anticiper pour mieux protéger

Gérôme BILLOIS
Senior Manager

@gbillois
+33 6 10 99 00 60
gerome.billois@solucom.fr

Raphaël BRUN
Manager

+33 (0)6 10 38 03 00
raphael.brun@solucom.fr

KURT SALMON
SOLUCOM

SOLUCOM AND KURT SALMON'S EUROPEAN BUSINESS JOIN FORCES
TO BUILD A NEW CONSULTANCY

solucom

SOLUCOM, UN ACTEUR MAJEUR DU CONSEIL

- Plus de 25 ans de collaboration avec les plus grandes entreprises, dans tous les secteurs d'activité…

- …pour guider et réussir
leurs transformations les plus structurantes.

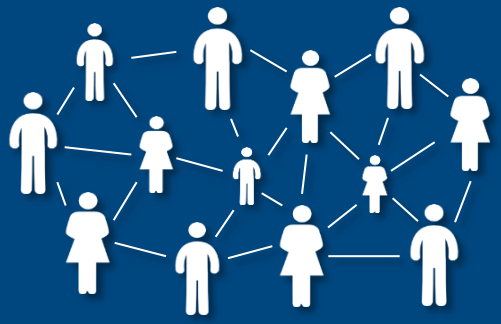
- Depuis le 7 janvier 2016, Solucom s'est rapproché des activités européennes* de Kurt Salmon pour donner naissance à un nouveau leader du conseil.

- **2400 collaborateurs**
- **300 M€ de CA** *en année pleine*
- **Coté en Bourse sur Euronext Paris**

** Les activités retail & consumer goods hors France, notamment Kurt Salmon UK et Germany, ne font pas partie du projet.*

** Partenariat stratégique*

SOLUCOM RISK MANAGEMENT ET CYBERSÉCURITÉ



350 CONSULTANTS

Le leader français de la cybersécurité…

…avec une couverture mondiale

Interventions dans plus de 40 pays sur les 3 dernières années

5 SAVOIR-FAIRE

Risk Management

Continuité d'activité

Cybersécurité

Audit &
réponse à incidents

Identité numérique

EXPERTISE & INNOVATION

Qualifié PASSI et certifié ISO27001 sur l'audit & investigation numérique

Expertises techniques (labs, démonstrateurs, POC…)

Expertises sectorielles (banque, assurance, énergie, transport, télécom)

LA RÉGLEMENTATION EUROPÉENNE

UN RÈGLEMENT EUROPÉEN SUR LES DONNÉES PERSONNELLES

2012 — Proposition de règlement émis par la Commission européenne

2015 — Accord des trois instances européennes sur un texte commun à la suite du Trilogue

2016 — Vote solennel du Parlement européen et du Conseil européen durant le printemps

2018 — Application du règlement dans 28 pays membres

3 années de négociations

2 années pour se mettre en conformité

UN RÈGLEMENT EUROPÉEN…

… qui s'appliquera **en l'état** aux 28 pays membres de l'Union européenne

Un règlement européen s'impose directement aux États, contrairement à une directive européenne qui fixe des objectifs à remplir aux États.

… qui donnera des **leviers d'actions** aux autorités pour sanctionner les organisations

Jusqu'à **20 millions** d'euros d'amende, ou **4% du chiffre d'affaires mondial**

Le montant maximal des amendes de la CNIL est actuellement de 150 000 €

QUELS SONT LES POINTS CLÉS DU RÈGLEMENT ?

209 pages

91 articles

6672 articles de presse

3 années de négociations

Trois impacts majeurs

Privacy by design

« Accountability » / « responsabilisation »

Notification des fuites de données

UN RÈGLEMENT EUROPÉEN…

« Accountability »

Les organisations devront être capables de **démontrer aux autorités** qu'elles respectent les obligations du règlement

Notification des fuites de données

Lorsqu'une faille de sécurité conduit à la destruction, perte, altération ou fuite non autorisée de données personnelles, **l'organisation doit notifier…**

AFCDP Association Française des Correspondants à la protection des Données à caractère Personnel

L'AFCDP organise un groupe de travail sur ce sujet, auquel Solucom participe

QUE DIT LE RÈGLEMENT SUR LE PRIVACY BY DESIGN ?

« Le responsable du traitement met en œuvre, **tant au moment de la détermination des moyens du traitement qu'au moment du traitement** lui-même, des **mesures techniques et organisationnelles appropriées**, telles que la pseudonymisation, qui sont destinées à donner effet aux principes de la protection des données, par exemple la minimisation des données, **de façon effective** et de manière à ce que le traitement comporte les **garanties nécessaires**, afin de répondre aux exigences du présent règlement et de **protéger les droits de la personne concernée**. »

Article 23

Dans cette perspective, le responsable de traitement tient compte

- De l'état des connaissances et des coûts de mises en œuvre
- De la nature, de la portée, du contexte et des finalités du traitement
- Des risques que présente le traitement pour les droits et libertés des personnes physiques

Article 23

LE PRIVACY BY DESIGN EN PRATIQUE

MAIS EN PRATIQUE, QU'EST-CE QUE LE PRIVACY BY DESIGN ?

- **Penser les projets** en vue de **protéger par défaut** la vie privée des personnes en minimisant les efforts
- Mener une analyse de risques et **identifier les impacts du traitement sur la vie privée**
- Mettre en place des mesures adaptées aux **informations recueillies** et à la **sensibilité** des traitements

Des exemples ?

Un outil de gestion de la relation client qui n'intègre pas la possibilité **d'archiver** les données

Une application smartphone qui ajoute systématiquement la localisation à une photo prise

Un site imposant l'utilisation de **cookies intrusifs**

Rendre obligatoire la saisie d'une **date d'expiration** concernant les **informations publiées** en ligne

Une application smartphone qui **conserve localement** cette information et **propose de la désactiver**

Un **site** dont la plupart des fonctions sont **accessibles sans tracer les utilisateurs**

LE PRIVACY BY DESIGN CHEZ NOS CLIENTS…

« Je n'ai pas le temps de déployer cette méthodologie complexe et peu opérationnelle sur mon périmètre »

« Les opérationnels seront écrasés par le nouveau processus »

« Le nouveau processus de Privacy by Design contredira les processus existants »

« Je ne dispose d'aucun outillage pour m'accompagner à la mise en œuvre du processus »

TROIS FACTEURS CLÉS DE SUCCÈS POUR LA MISE EN ŒUVRE DU PRIVACY BY DESIGN

S'intégrer dans la méthodologie projet existante

Prioriser les efforts d'accompagnement en identifiant les projets sensibles

Outiller les chefs de projet

LE PRIVACY BY DESIGN… EN 3 PHASES !

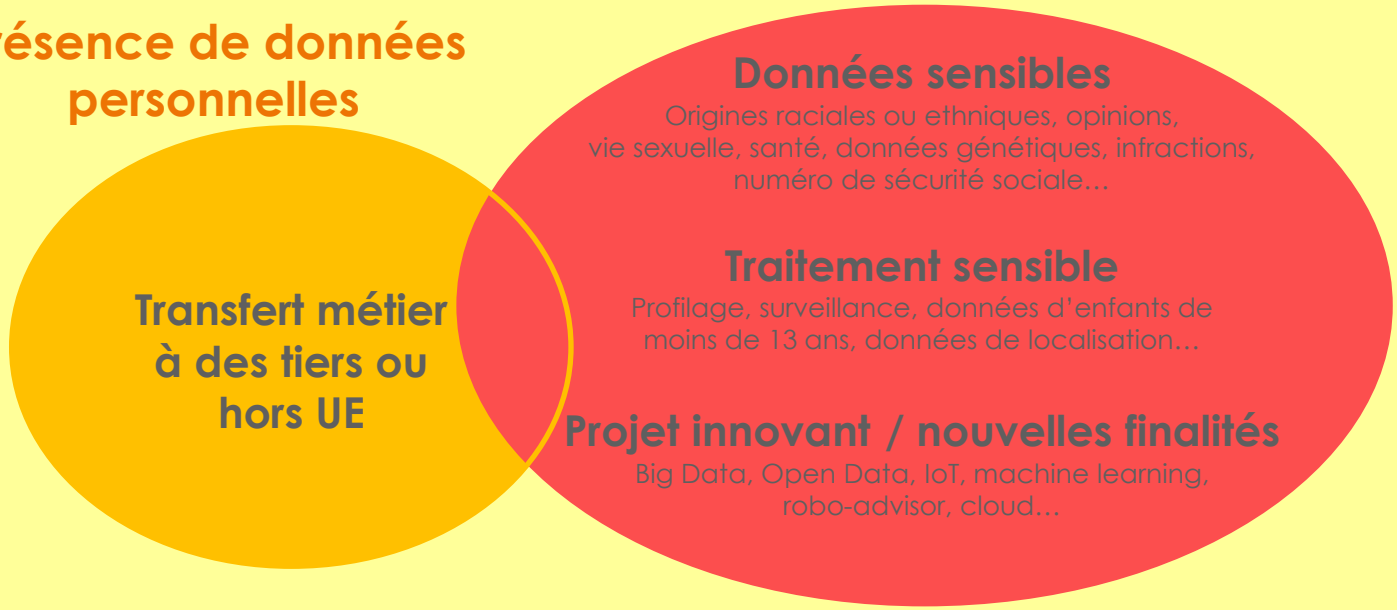
FOCUS – PHASE AMONT
CLASSIFIER LES PROJETS ET ADAPTER L'ACCOMPAGNEMENT

Tout chef de projet doit pouvoir évaluer le besoin d'accompagnement Privacy by Design de son projet à l'aide de critères simples

Pas de données personnelles

Identité, numéros d'identification, coordonnées, données sur la vie privée ou professionnelle, informations financières, habitudes de vie, images, données de communication, données biométriques…

Présence de données personnelles



Pas de suivi

Suivi distant

Suivi simple

Suivi rapproché

FOCUS : PHASE AMONT
INTÉGRER LE PIA AUX MÉTHODES D'ANALYSE DE RISQUE EXISTANTES

Identifier l'existant

- **Méthodes d'analyse de risques déjà existantes** (risk manager, RSSI…)
- **Préconisations de la CNIL**

Ajouter les éléments spécifiques liés au Privacy by Design

- **Événements redoutés sur les données personnelles** (données exploitées à des fins non prévues par le traitement, incapacité à exercer le droit d'accès,…)
- **Exigences spécifiques au Privacy by Design** (information des personnes, durée de conservation de la donnée, encadrement des transferts hors UE…)

Modifier les grilles d'impact

- Grilles qualifiant **les impacts pour l'organisation ET pour la vie privée** des personnes concernées

LE PRIVACY BY DESIGN EN 3 PHASES : PHASE PROJET

L'ensemble des projets doit être **capté** et les **risques et obligations légales** liés à ces projets identifiés

FOCUS : PHASE PROJET
CHOIX ET MISE EN PLACE DES MESURES ADÉQUATES

Les mesures à mettre en place sont à pré-identifier, en adaptant plus ou moins un existants déjà riche

Effort d'adaptation du processus existant

Sécurité	**Les environnement hors production utilisent les données de production**	→ Utilisation de **jeux spécialement conçus** → A défaut, **anonymisation des données** et évaluation du **risque de ré-identification**
Transfert	**Des tiers hors UE auront accès aux données**	→ Utilisation de **clauses contractuelles types ou signature des BCR Groupe**
Conservation	**Aucune durée de conservation n'est définie**	→ Définition d'une **durée de conservation** → **Suppression automatique des données au-delà**
Information	**Les personnes ne sont pas informées de l'utilisation de leurs données au travers d'un dispositif existant**	→ Présence d'une **fiche d'information** au moment de la collecte des données → **Accès possible aux données collectées**
Finalité	**Les systèmes de collecte des données personnelles comportent des champs libres**	→ **Consignes de remplissage**

LE PRIVACY BY DESIGN EN 3 PHASES : PHASE AVAL

Phase Amont

L'ensemble des projets doit être **capté** et les **risques et obligations légales** liés à ces projets identifiés

Phase Projet

Chaque point soulevé lors de la phase amont doit trouver une **réponse technique ou organisationnelle**

Phase Aval

Des **tests sont effectués** afin de vérifier le respect des exigences

PHASE AVAL : CONTRÔLE DES MESURES MISES EN PLACE

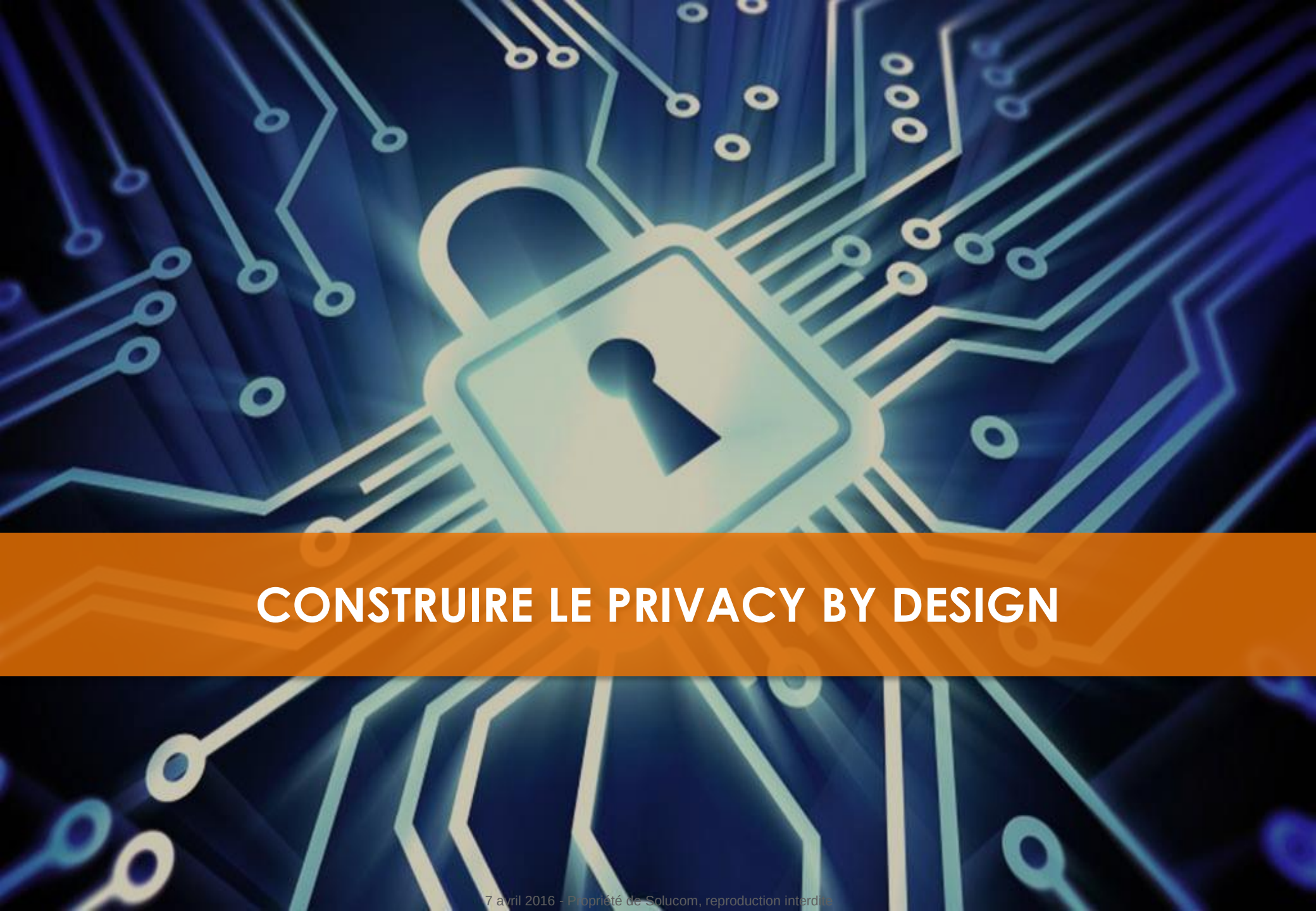
Contrôle de la conformité
(recettes et tests avant mise en production)

Check-list conformité

(à partir des questions de la phase Projet)

Alimentation du plan de contrôles et collecte d'enregistrements/preuves *(accountability)*

Définition d'un plan de gestion des incidents et des crises *(notification)*



CONSTRUIRE LE PRIVACY BY DESIGN

UNE OCCASION DE RÉNOVER LE PROCESSUS D'INTÉGRATION DE LA SÉCURITÉ DANS LES PROJETS

INTÉGRATION DE LA SÉCURITÉ DANS LES PROJETS : LA SITUATION DANS LES GRANDS COMPTES

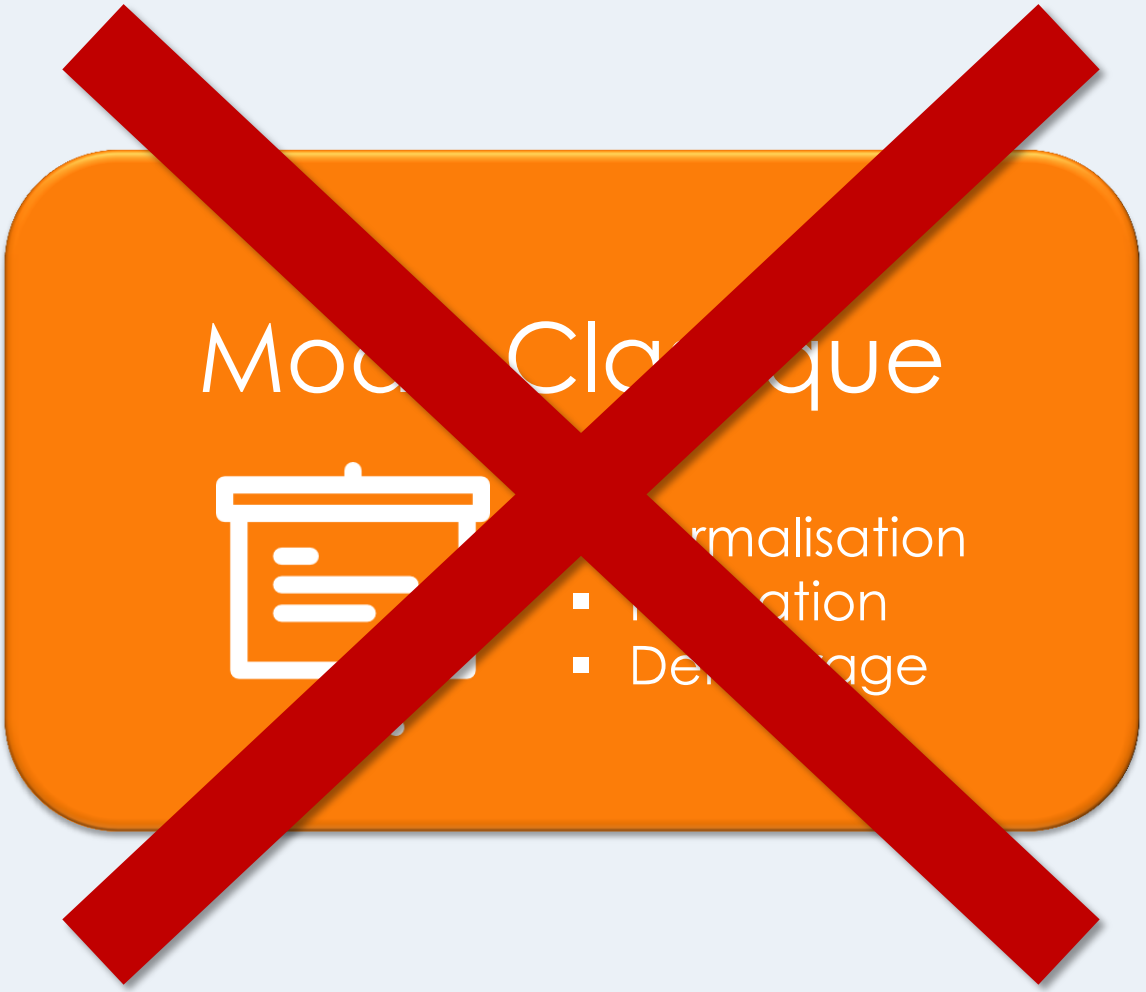
Une majorité de comptes où le **process n'existe** pas ou reste uniquement **théorique**

Le Privacy by design est une occasion de se réinventer

Des initiatives qui peuvent être améliorées mais **qui sont fonctionnelles** et délivrent des résultats (analyses de risques, recettes sécurité…)

Adapter l'existant aux spécificités du Privacy by design

OBJECTIF PRIVACY BY DESIGN 2018 : QUELLE FEUILLE DE ROUTE POUR Y ARRIVER ?



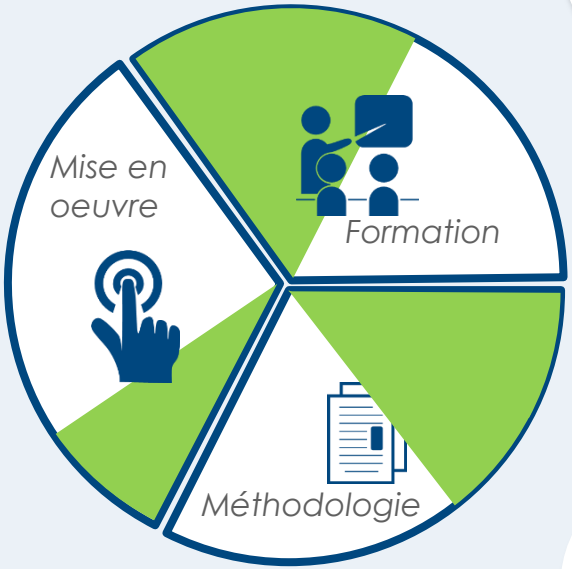
OBJECTIF PRIVACY BY DESIGN 2018 : QUELLE FEUILLE DE ROUTE POUR Y ARRIVER ?

Mode Agile

MODE AGILE : ROADMAP 2018
OBJECTIF 2016

2016

2016 | 2017 | 2018



Ébauche de la méthodologie et des outils

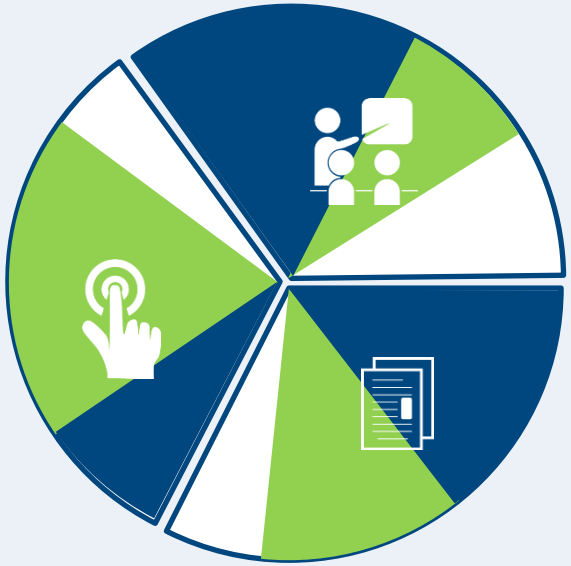
Identifier 2 ou 3 projets pilotes à accompagner (rétro privacy by design, projet innovant type IoT…)

Identifier les chefs de projet et les experts, puis les former à l'accompagnement et au pilotage des projets

MODE AGILE : ROADMAP 2018
OBJECTIF 2017

2016 | **2017** | **2018**

- Ébauche méthodologie et outils
- Choix des projets pilotes
- Choix et formation des chefs de projet



Accompagnement des projets identifiés par les chefs de projet et experts formés

Adaptation de la méthodologie et des outils par chaque projet en parallèle, en fonction de ses besoins et remarques, **et confrontation des retours d'expérience**

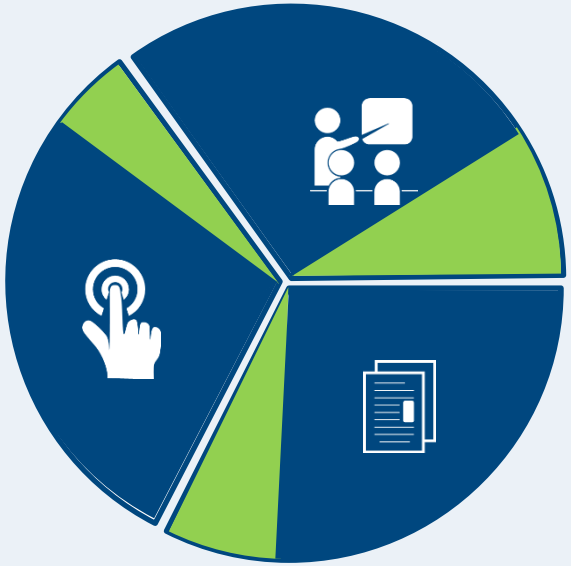
Au cours de la mise en œuvre, sensibilisation des acteurs métiers et IT de ces trois projets, et d'autres acteurs éventuellement

2017

MODE AGILE : ROADMAP 2018
OBJECTIF 2018

2016 — **2017** — **2018**

- Ébauche méthodologie et outils
- Choix des projets pilotes
- Choix et formation des chefs de projet
- Mise en œuvre pilotes
- Adaptation méthodologie
- Sensibilisation



Déploiement de la méthodologie issue des retours d'expérience (formalisation et validation de la documentation, sensibilisation de tous les acteurs, outillage…)

Formation de tous les chefs de projet

Conception et déploiement des KPI et des contrôles permettant de s'assurer du bon fonctionnement

2018

POUR ALLER + LOIN :
CATALOGUE DES SOLUTIONS DE SÉCURITÉ ESSENTIELLES

Faire un **bilan des solutions techniques de protection** des données sensibles et/ou à caractère personnel :

- Authentification : utilisateur, administrateur, client
  En environnement : client lourd, navigateur, application smartphone/tablette
- Chiffrement en stockage et en transit, en interne et dans le cloud
- Traçabilité et alerting : accès utilisateur, administrateur
- Anonymisation : dynamique ou par batchs
- Administration technique à sécurité renforcée ou équipe dédiée

Suite à ce bilan, **intégrer ces chantiers dans les feuilles de route** : ces éléments seront nécessaires ultérieurement

POUR ALLER + LOIN :
QUI EST EN CHARGE DE DÉPLOYER LE PBD ?

Le sujet du moment, et pour l'instant, aucune réponse à priori …

Comment répartir les rôles et responsabilités entre ces acteurs ?

- ✓ **Pas de solution unique, car chacun devra participer à la définition du Privacy by Design et à sa mise en œuvre**
- ✓ **Avec un DPO qui sortira de plus en plus de son rôle d'alerte pour devenir le responsable / garant de la conformité**

Compliance / Legal

Du CIL vers le DPO

CISO

Mais un enjeu au-delà de cette question : **sortir d'une posture juridique qui présente les contraintes** pour évoluer vers une posture de **conseil conformité**

CONCLUSION :
PRIVACY BY DESIGN, NOTIFICATION ET « ACCOUNTABILITY »

Déployer le Privacy by Design…

en mode agile, s'appuyant sur le terrain et l'existant

…c'est **disposer de preuves** requises par le principe d'« **accountability** »…

via les résultats du Privacy Impact Assessment, des mesures identifiées en phase Projet, des résultats des recettes et contrôles…

…et éviter/faciliter la notification de fuites

en évaluant (Privacy Impact Assessment) et en diminuant les risques sur la vie privée des personnes en cas de fuites

KURT SALMON
SOLUCOM

www.solucom.fr

@cabinet_solucom

Contact

Gérôme BILLOIS

Senior Manager

@gbillois

+33 6 10 99 00 60

gerome.billois@solucom.fr

Raphaël BRUN

Manager

Tel : +33 (0)6 10 38 03 00

Mail : raphael.brun@solucom.fr