RGPD by IT
Fondements pratiques

GDPR
EU General Data Protection Regulation

Réunion CLUSIR
18/10/2017

Didier SAVALLE
Correspondant local.
CLUB 27001 Lyon

Plan

- Préambule
- Etape 0: Organiser le projet
- Etape 1: Désigner un pilote
- Etape 2: Cartographier les traitements
- Etape 3: Prioriser les actions
- Etape 4: Gérer les risques
- Etape 5: Organiser les processus
- Etape 6: Documenter la conformité
- Etape 7: Accompagner dans la durée
- Conclusion

Préambule – Méthodologie CNIL

- La méthodologie suggéré par la CNIL, se décline en 6 étapes
- La CNIL étant l'autorité de contrôle en France en charge en charge RGPD, les organisations sont encouragées à etre conforme à cette méthodologie.

Préambule – Méthodologie PSSI

- **Le RGPD est un processus de mise en conformité, au même titre que une habilitation, un agrément, une certification, une rédaction de politique.**

Phase 1

ÉTAT DES LIEUX

Objectif

- Évaluer vos besoins et votre maturité sécurité

Phase 2

FEUILLE DE ROUTE

Objectifs

- Spécifier les mesures à mettre en place
- Formaliser un plan de mise en route

Phase 3

MISE EN ŒUVRE

Objectif

- Dérouler le plan d'actions conformément au calendrier

Préambule - Méthodologie ISO 27001

Phase 0
Votre besoin

ÉTAT DES LIEUX

Objectif
Évaluer le niveau de maturité et de faisabilité de votre projet

Phase 1
Analyse de l'existant

PLAN

ANALYSE DES RISQUES

Objectif
Analyser l'existant en détails et apprécier les risques sur le périmètre retenu

Phase 2
La construction

DO

MISE EN ŒUVRE DU SMSI

Objectif
Construire le SMSI

Phase 3
Le « run »

CHECK
ACT

SUIVI & AMÉLIORATION CONTINUE

Objectif
Dérouler le plan d'actions et les actions de mise en œuvre de suivi et de pilotage

Phase 4
Audit interne

CHECK

AUDIT BLANC DE CERTIFICATION

Objectif
Optimiser les chances de succès à la certification

Phase OPTIONNELLE

CONFIRM

MAINTIEN DE LA CERTIFICATION

Objectif
Conserver la Certification

Quid ISO 27001 / RGPD (2/3)

►Système de Management de la Sécurité de l'Information (SMSI)

- Logique **PDCA: Amélioration continue**
- Documents communs ou pouvant intégrer les spécificités
  - **Analyse de risques** (clause 6)
  - **Politique sécurité** (A5)
  - **Sécurité dans les RH, charte informatique** (A7)
  - **Gestion des incidents de sécurité** (A16)
  - **Sécurité dans les développement** (A14)
  - **Sensibilisation sécurité** (A7)
  - **Revue des contrats fournisseurs** (A15)
  - **Rapports d'audit, de contrôles** (clause 9)

►Projet de certification RGPD:

- **ISO 29134:** sur la réalisation des PIA

Préambule – Méthodologie CNIL

►Ajout de 2 étapes

- Etape 0: **Organiser le projet**

C N I L


- Etape 1: **Désigner un pilote**


- Etape 2: **Cartographier vos traitements**


- Etape 3: **Prioriser les actions**


- Etape 4: **Gérer les risques**


- Etape 5: **Organiser les processus internes**


- Etape 6: **Documenter la conformité**

- Etape 7: **Accompagnement postérieur**

Etape 0: Organiser le projet

- **Projet transverse:**
  - Nécessitant d'impliquer plusieurs métiers
  - Directions générale, juridique, SI, marketing, commerciaux, RH, qualité
  - Implication systématique de la DSI dans toutes les phases du projet => Direction du Projet à la DSI
- **Définition de la stratégie de la Direction, en terme:**
  - De budget additionnel à prévoir pour le RGPD
  - De ressources allouées
  - De marketing pour la RGPD obtenue
- **Besoin de sensibilisation:**
  - en amont
  - à tous les étages:
- **Mise en place de processus de suivi:**
  - Comité de pilotage
  - Revue de direction

Etape 1: Désigner un pilote (DPO)

►Objectif:

- Désigner un délégué à la protection des données (DPO)

►Role du DPO:

- Coopérer avec l'autorité de contrôle et en être le point de contact
- S'informer sur les nouvelles obligations
- Sensibiliser les décideurs et les utilisateurs sur les nouvelles règles
- Réaliser l'inventaire et les études d'impact des traitements
- D'informer/conseiller le responsable de traitement, le sous-traitant, ainsi que leurs employés
- Piloter la conformité en continu

►*Valeur ajoutée*:

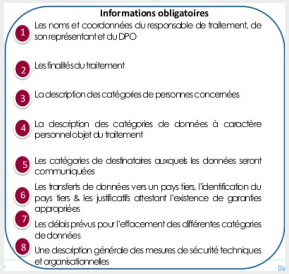
- *une aide à la définition de la fiche du poste du DPO*
- *un transfert de compétences pour la formule DPO choisie*
- *une aide à la gestion du projet, par une participation active aux réunions de suivi*

Etape 2: Cartographier des traitements

►Objectif:

- Tenir une documentation interne complète sur les traitements en conformité avec la RGPD

►Taches:



- Pour chaque traitement de données à caractère personnel:
- Qui? Quoi?
- Pourquoi?
- Où?
- Jusqu'à quand?
- Comment?

►*Valeur ajoutée:*

- *La réalisation de l'inventaire des traitements de données personnelles*
- *La catégorisation de ces traitements, et la réponse aux questions ci-dessus*

Etape 3: Prioriser les actions

►Objectif:

- Identifier les actions à mener pour se conformer aux obligations actuelles et à venir.

►Points d'attention quels que soient les traitements:

- Ne traiter que les données nécessaires
- Vérifier la conformité des sous-traitants
- Tenir compte des droits des personnes concernées
- Vérifier les mesures de sécurité mises en place

►Points d'attention nécessitant de la vigilance:

- Données spécifiques
- Traitements spécifiques
- Transfert de données hors de l'Union Européenne.

►*Valeur ajoutée:*

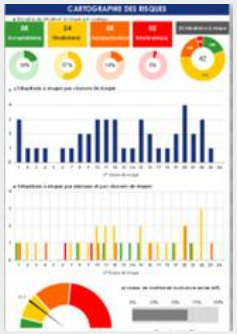
- *qualifier la sensibilité des traitements inventoriés / exigences*
- *vérifier des exigences pour chaque traitement*

Etape 4: Gérer les risques (1/3)

►Objectif:

- Mener, pour chaque traitement, une étude d'impact sur la protection des données (PIA).

►Pourquoi mener une PIA?:



- Pour bâtir un traitement de données personnelles ou un produit, conforme
- Pour apprécier les impacts sur la vie privée des personnes concernées
- Pour démontrer que les principes fondamentaux du règlement sont respectés

►Quand mener une PIA?:

- Avant la collecte des données et la mise en oeuvre du traitement
- Sur tout traitement susceptible d'engendrer des risques élevés

Etape 4: Gérer les risques (2/3)

►Contenu d'une PIA:

- Description du traitement et de ses finalités
- Evaluation nécessité et proportionnalité du traitement
- Appréciation des risques
- Mesures envisagées pour traiter ces risques

►*Valeur ajoutée:*

- *Aide au choix d'outillage de PIA*
- *Identifier les traitements nécessitant un PIA*
- *Réaliser les études d'impact PIA*

Etape 4: Gérer les risques (3/3)

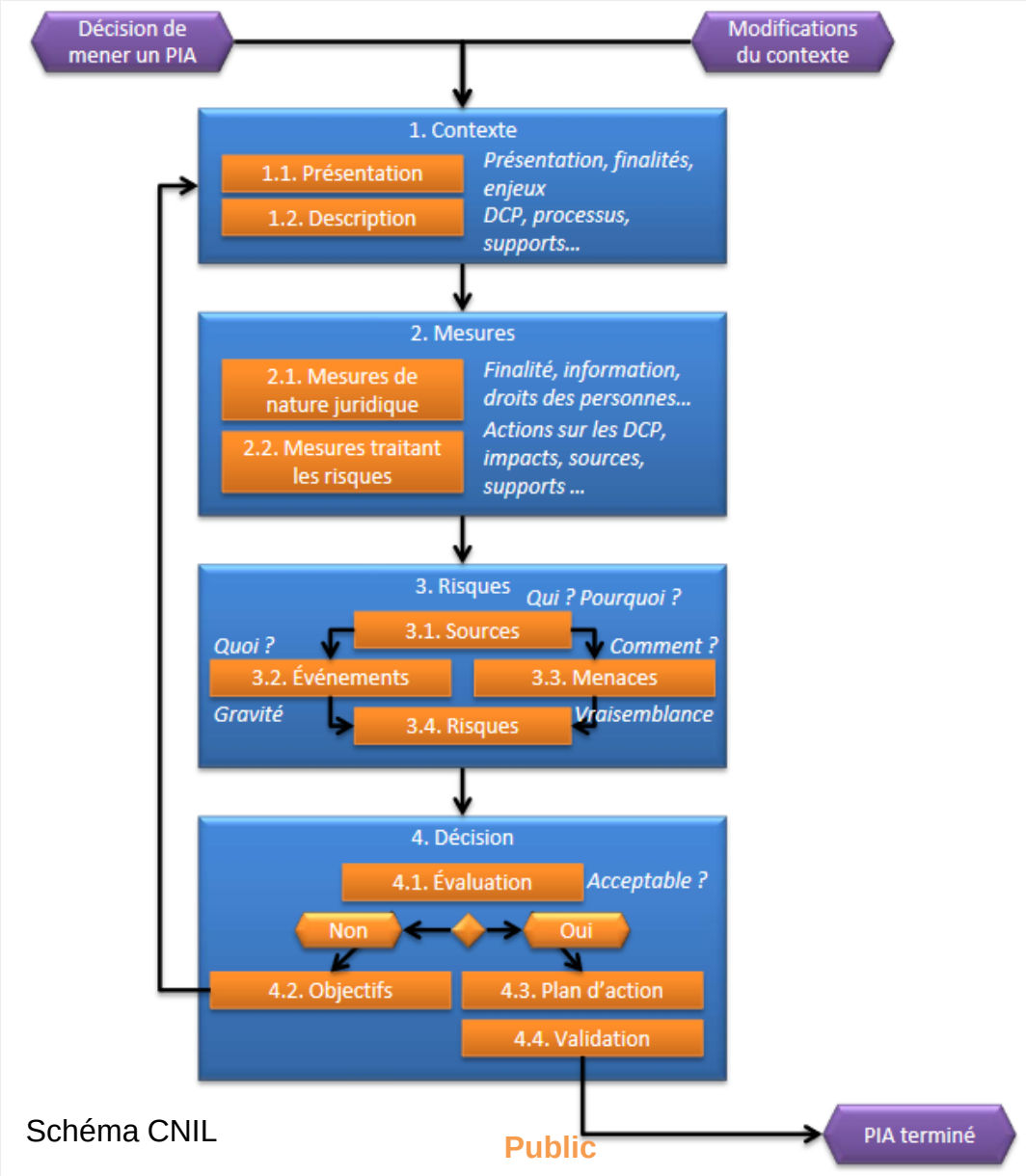


Schéma CNIL

Etape 5: Organiser les processus (1/4)

►Objectif:

- Mettre en place des procédures internes pour la protection des données, au cours des traitements

►Pourquoi organiser les processus:

- Appliquer la conformité dès la conception d'une application ou d'un traitement
- Impliquer les acteurs dans la mise en œuvre de traitements de données
- Sensibiliser via un plan de formation et de communication
- Traiter les réclamations/ demandes des personnes concernées quant à l'exercice de leurs droits
- D'anticiper les violations de données par la notification à l'autorité dans les 72 heures et aux personnes concernées dans les meilleurs délais.

►*Valeur ajoutée:*

- *Construire un plan de sensibilisation des développeurs et responsable applicatifs*
- *Spécifier les évolutions du SMSI et des mesures de sécurité*

Etape 5: Organiser les processus (2/4)

►Mise en œuvre de mesures pour la conformité RGPD

- Maitrise des accès aux données
  - Gestion des profils, des accès, traçabilité des accès et des actions
- Chiffrement / masquage des DCP
  - Chiffrement des données lors de la collecte, des échanges internes et externes, du stockage
- Le blocage des attaques
  - Pare-feux, reverse-proxy, IDS/IPS, WAF (pare-feu applicatif)
- Supervision des fichiers et des données
  - Supervision et alertes sur les accès, des actions sur les DCP
- Audit et reporting de conformité
  - Gestion des logs, centralisation, corrélation des logs pour identifier des alertes (SIEM : security information and event management)
- Plan de reprise d'activité sur les applications critiques en disponibilité et contenant des DCP
  - Mise en œuvre d'une organisation, des procédures techniques et tests réguliers

Etape 5: Organiser les processus (3/4)

►Mise en œuvre de mesures de sécurité

- Tests d'intrusions infrastructure
  - Vérifier que les mesures « privacy by default » sont existantes et efficaces
- Tests d'intrusions applicatifs
  - Vérifier que les mesures « privacy by design / by default » sont existantes et efficaces
- Indicateurs techniques / contrôles techniques
  - Sécurité du SI (mise à jour des serveurs, SLA…)
- Indicateurs organisationnels
  - Revue des registres de traitement, revue des comptes et habilitations, revue des contrats

Etape 5: Organiser les processus (4/4)

►Elaboration de Supports de Sensibilisation

- Utilisateur du SI
  - Registre des traitements
  - Organisation DPO
  - Notification d'une fuite de données
- Chef de projet / développeur
  - Intégration de la privacy by design / privacy by default
  - PIA
  - Notification d'une fuite de données
- Equipe infrastructure / applicatif
  - Intégration de la privacy by design / privacy by default
  - Audit technique
  - Notification d'une fuite de données
  - Suivi des réclamations des personnes
- Management
  - Impact sur la non-conformité au RGPD
  - Organisation DPO
  - Impact et révision des contrats client et fournisseur
  - Notification d'une fuite de données

Etape 6: Documenter la conformité (1/2)

►Objectif:

- Constituer et regrouper la documentation nécessaire, à chaque étape

►Contenu d'un dossier (1/2):

- La documentation sur les traitements de données personnelles
  - Le registre des traitements ou des catégories d'activités de traitements (pour les sous-traitants)
  - Les analyses d'impact (PIA)
  - L'encadrement des transferts de données hors de l'UE
- L'information des personnes
  - Les mentions d'information
  - Les modèles de recueil du consentement,
  - Les procédures mises en place pour l'exercice des droits

(…)

Etape 6: Documenter la conformité (2/2)

►Contenu d'un dossier (2/2):

- Les contrats avec les rôles et les responsabilités des acteurs
  - Les contrats avec les sous-traitants
  - Les procédures internes en cas de violations de données
  - Les preuves du consentement des personnes concernées
  - traitement de leurs données repose sur cette base.

►*Valeur ajouté:*

- *Construire la documentation de la conformité*

Etape 7: Accompagner dans la durée

►Objectif:

- Installer un accompagnement du client pour maintenir la conformité au RGPD dans le temps

►Activité:

- Gouvernance de la Politique de Protection des Données
- Action ponctuelle: audit, sensibilisation
- Intervention dans les phases amont des projets (« privacy by design / default »)
- Co-animation des Comités de Suivi et Revues de Direction

►*Valeur ajoutée:*

- *Accompagner, sur demande, dans l'exploitation du RGPD*
- *Sous une forme modulaire et indépendante des phases d'audit et opérationnelle*

Conclusion

- **Convergence nécessaire entre:**
  - La Politique de Protection de Données
  - La Politique de Sécurité du Système d'Information
- **Première urgence pour les organisations:**
  - Désignation d'un DPO ou d'un dispositif équivalent (étape 1)
  - Réaliser l'état des lieux de conformité (étape 2)
  - Réaliser le plan d'actions (étape 3)
- **Le compte à rebours RGPD étant à 8 mois:**
  - Pour la mise en œuvre de la Politique de Protection des Données
  - Nécessité de se faire accompagner par:
    - Des experts juridiques
    - Des experts cybersécurité
    - Des RSSI et DPO à temps partagé

Questions

Didier SAVALLE
Correspondant régional
Club 27001 Lyon
didier.savalle@fidens.fr
+33 (6) 84 76 42 92