RGPD :
Approche et Méthode WinDesign

Date dernière révision	21/09/2018
Auteur	Cecima cecima@win-design.com
Versions	V0 : Initialisation du document V01 : Compléments
Document	MSPEC_RGPD APPROCHE ET METHODE WD_NS_31700V01
Renvois	→ Guide de la sécurité des données personnelles (CNIL) → PIA-Outillage (CNIL)

Table des matières

1. INTRODUCTION – SYNTHESE – CONCLUSION - DEFINITION 4

1.1. INTRODUCTION 4
1.2. SYNTHESE 4
1.3. CONCLUSION 5
1.4. DEFINITION D'UN TRAITEMENT DE DCP (DONNEES A CARACTERES PERSONNELLES) 5

2. SYNOPSIS GLOBAL 6

2.1. L'APPROCHE EST DECOMPOSEE EN ACTIVITES 6
2.2. CHAQUE ACTIVITE SE DECOMPOSE EN OPERATION(S) 7

3. DETAILS : ACTIVITE A1 - CARTOGRAPHIER LES INVARIANTS 8

3.1. OPERATION O10 - CARTOGRAPHIER LES PROCESSUS 8
3.2. OPERATION O11 - CARTOGRAPHIER LES BLOCS FONCTIONNELS 8
3.3. OPERATION O12 - CARTOGRAPHIER LES BLOCS APPLICATIFS 8
3.4. OPERATION O13 - CARTOGRAPHIER LES DONNEES MEMORISEES 8
3.5. OPERATION O14 - CARTOGRAPHIER LES FLUX 8
3.6. OPERATION O15 - CARTOGRAPHIER LES BASES DE DONNEES 8
3.7. OPERATION O16 - CARTOGRAPHIER LES SERVEURS 8
3.8. OPERATION O17 - CARTOGRAPHIER LES POSTES DE TRAVAIL 8

4. DETAILS : ACTIVITE A2 - GESTION DES OBJETS CONCERNES PAR LE RGPD 8

4.1. OPERATION O20 - SELECTION DES OBJETS CONCERNES PAR LE RGPD 8
4.2. OPERATION O21 - MARQUAGE DES OBJETS SELECTIONNES 8

5. DETAILS : ACTIVITE A3 - GESTION DES TRAITEMENTS DE DONNEES 9

5.1. OPERATION O30 - MISE EN EVIDENCE DES TRAITEMENTS DE DCP 9

6. DETAILS : ACTIVITE A4 - GESTION DES INFORMATIONS (DONNEES) 9

6.1. OPERATION O40 - ANALYSE DES INFORMATIONS ET GROUPES DE DONNEES 9
6.2. OPERATION O41 - DISTINCTION DES 3 X TYPES DE DCP ET DES GROUPES DCP 9
6.3. OPERATION O42 - PRODUCTION DES FICHES DESCRIPTIVES INDIVIDUELLES DE DONNEES ET DE GROUPES 9

7. DETAILS : ACTIVITE A5 - STRUCTURER LES TRAITEMENTS 10

7.1. OPERATION O50 - REPRESENTATIONS COMPLETES 10

8. DETAILS : ACTIVITE A6 - CONSTITUER LE REGISTRE DES TRAITEMENTS 10

8.1. OPERATION O60 - PRODUCTION DES FICHES DESCRIPTIVES INDIVIDUELLES PAR TRAITEMENT 10
8.2. OPERATION O61 - PRODUCTION DU RAPPORT D'ENSEMBLE == REGISTRE GLOBAL DES TRAITEMENTS 10

9. DETAILS : ACTIVITE A7 - SELECTIONNER LES TRAITEMENTS POUR AIPD 10

9.1. OPERATION O70 - PRIORISATION DES TRAITEMENTS DCP SENSIBLES 10

1. Introduction – Synthèse – Conclusion - Définition

1.1. Introduction

- A travers le module Business Process – Cartographie SI, WINDESIGN vous propose une approche structurée et jalonnée pour appréhender votre « projet RGPD »
  [c.-à-d. la mise en conformité vis à vis du nouveau Règlement de tous vos traitements de Données à Caractères Personnelles (DCP)].

- Soit vous partirez de votre cartographie et modélisation existante ou bien à partir de la mise en œuvre d'un projet nouveau de cartographie (globale ou partielle) de votre Système d'Information.

- Notre proposition de démarche est décomposée en une suite d'activités (nommées : Ai), elles-mêmes structurées en opérations (nommées : Oxx)

1.2. Synthèse

- La démarche consiste à recenser et classer l'ensemble des composants du SI susceptibles de constituer tous les traitements de données, y compris et surtout les Données à Caractères Personnelles (DCP).

- Puis en marquant ces composants, il faudra distinguer, formaliser les traitements de DCP concernés.

- Parmi ces composants, on repèrera les risques, les exigences, les mesures associés et relatifs à chaque traitement
  ✓ 🕮 Cf. Guide de la sécurité des données personnelles le document de référence de la CNIL.

- On précisera notamment pour chaque traitement de DCP les principaux constituants tels que : la finalité ; le(s) responsable(s) ; le(s) destinataire(s) et bien sûr l'ensemble des données mise en jeux (DCP et autres).

- En ce qui concerne les données associées à chaque traitement, il sera nécessaire de les trier par type de DCP puis ensuite de les catégoriser
  ✓ 🕮 Cf. PIA-Outillage.pdf le document de référence de la CNIL.

- Puis chaque traitement ainsi formalisé sera complété d'une partie d'identification et de référencement afin d'alimenter le « Registre » de description et de stockage dédié.

- Enfin la conformité ne sera démontrée que lorsque pour chaque traitement opérant sur des DCP sensibles, les Analyses d'Impacts relatives à la Protection des Données (AIPD) seront effectuées.

- Il sera alors possible de prioriser les traitements de DCP sensibles pour déclencher les actions de mise en conformité nécessaires à leurs maintiens en conditions opérationnelles.

1.3. Conclusion

- Bien sûr l'intégration de la démarche sur le référentiel permanent et unique de WINDESIGN, vous permettra d'assurer la pertinence dans le temps de votre référentiel (« le Registre ») de traitements ainsi que leur conformité au RGPD.

- La maintenance (ajouts, mises à jour, suppressions, archivages, etc.) du catalogue des traitements (« Registre ») ainsi que celle de leurs composants est un pilier de la démarche de mise en conformité.

1.4. Définition d'un Traitement de DCP (Données à Caractères Personnelles)

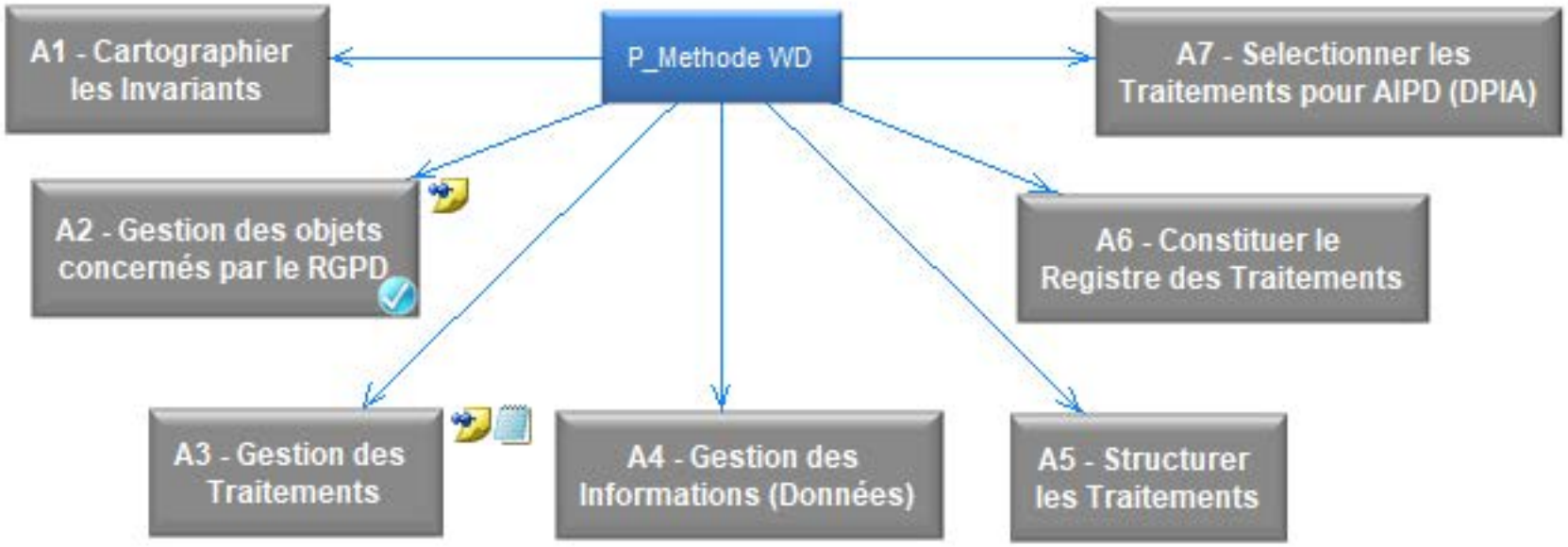
- La Loi Informatique & Liberté (I & L) est le support de toute notre démarche.

  Son article 2 explicite notamment :

  « Traitement de DCP = toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment
  - la collecte,
  - l'enregistrement,
  - l'organisation,
  - la conservation,
  - l'adaptation ou la modification,
  - l'extraction,
  - la consultation,
  - l'utilisation,
  - la communication par transmission,
  - diffusion ou toute autre forme de mise à disposition,
  - le rapprochement ou l'interconnexion,
  - ainsi que le verrouillage,
  - l'effacement
  - ou la destruction»

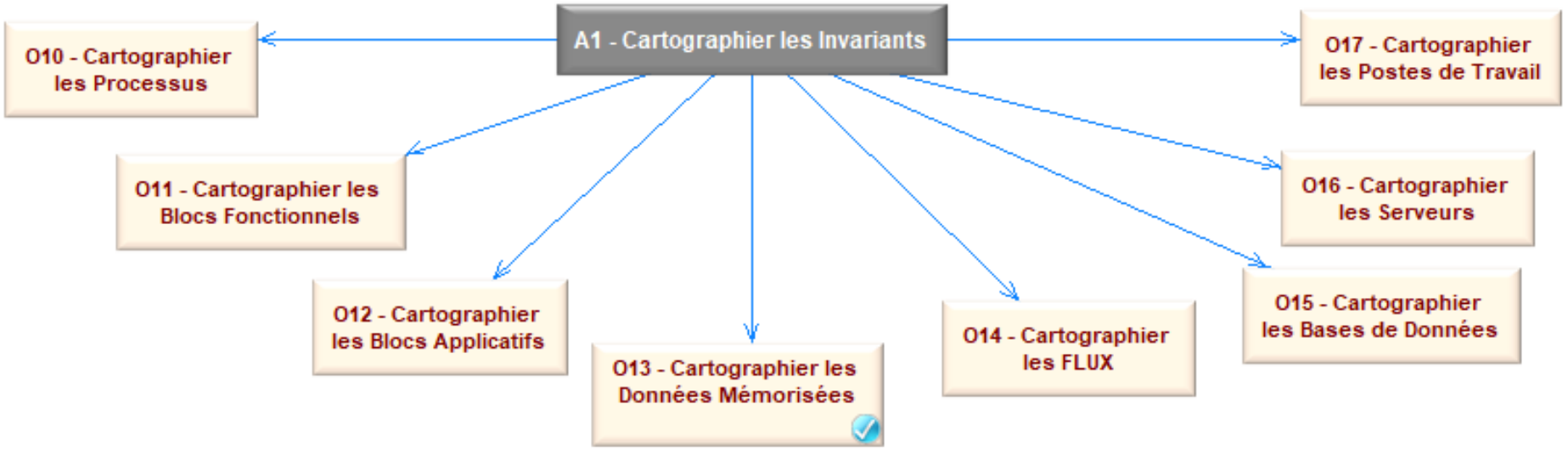
2. Synopsis global

2.1. L'approche est décomposée en Activités

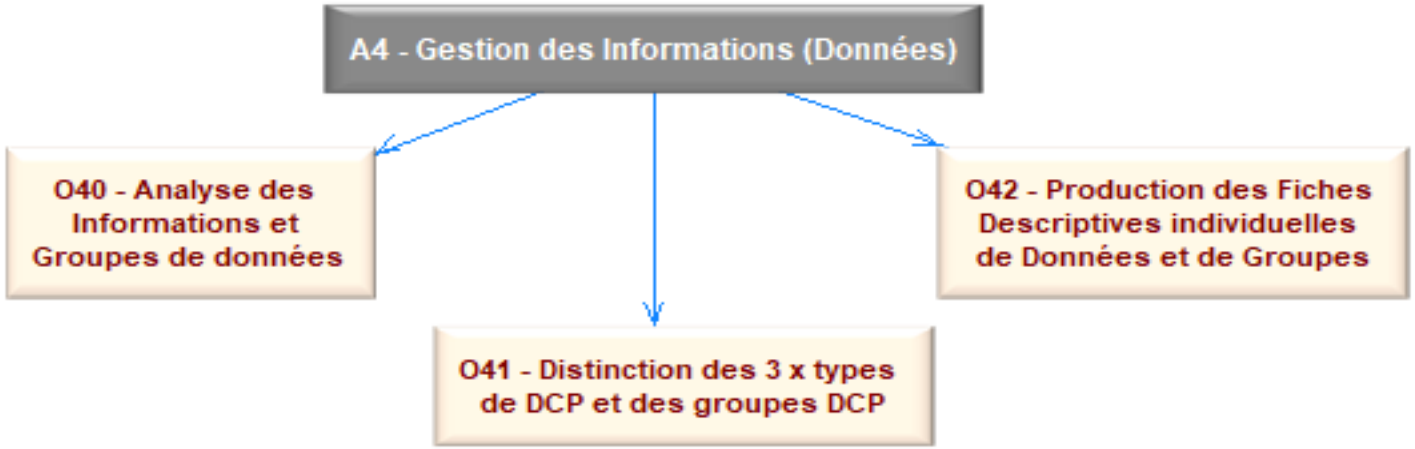


2.2. Chaque activité se décompose en Opération(s)

Exemple Activité A1 :



Exemple Activité A4 :



3. Détails : Activité A1 - Cartographier les Invariants

3.1. Opération O10 - Cartographier les Processus

Livrable = Catalogue des Macro Processus, Processus, Sous Processus et Activités modélisés dans le SI.

3.2. Opération O11 - Cartographier les Blocs Fonctionnels

Livrable = Catalogue des Fonctionnalités réalisées par le SI : Fonctions Principales, Secondaires, Elémentaires ou autres.

3.3. Opération O12 - Cartographier les Blocs Applicatifs

Livrable = Catalogue du patrimoine Applicatif : incluant les modules, les IHM, composants d'architecture, etc.

3.4. Opération O13 - Cartographier les Données Mémorisées

[HORS BdD]
Livrable = Recenser toutes les structures de données : Fichiers de tous types, Informations isolées, etc.

3.5. Opération O14 - Cartographier les Flux

Livrable = Catalogue de tous les Flux d'échanges de données intra et extra SI.

3.6. Opération O15 - Cartographier les Bases de Données

Il s'agit d'identifier TOUS les gisements d'Information (formels ou informels) [cf. Prévention des fuites de données « Data Breach »].

3.7. Opération O16 - Cartographier les Serveurs

Livrable = Catalogue des serveurs Physiques, Hyperviseurs et Virtuels présents dans les infrastructures Internes / Externes (y compris Sous Traitants).

3.8. Opération O17 - Cartographier les Postes de Travail

Livrable = Catalogue de tous les postes de travail : Virtuels ET physiques (Fixes, Portables, tablettes, Mobiles).

4. Détails : Activité A2 - Gestion des objets concernés par le RGPD

4.1. Opération O20 - Sélection des objets concernés par le RGPD

A travers le référentiel unique, il conviendra de définir puis exécuter des requêtes de sélection – extraction des objets « marqués » RGPD.

4.2. Opération O21 - Marquage des objets sélectionnés

Mise à jour des caractéristiques étendues et des liens inter-objets.

5. Détails : Activité A3 - Gestion des Traitements de Données

5.1. Opération O30 - Mise en évidence des Traitements de DCP

Il faut lister les traitements (puis créer l'objet éponyme) qui surgissent de l'ensemble des objets marqués.
Qu'est-ce qu'un traitement ? cf. la définition, ci-dessous, des procédés qui le constituerait !

Rappel :
(cf. Art 2 de la Loi I & L)

« Traitement de DCP = toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment
- la collecte,
- l'enregistrement,
- l'organisation,
- la conservation,
- l'adaptation ou la modification,
- l'extraction,
- la consultation,
- l'utilisation,
- la communication par transmission,
- diffusion ou toute autre forme de mise à disposition,
- le rapprochement ou l'interconnexion,
- ainsi que le verrouillage,
- l'effacement
- ou la destruction»

6. Détails : Activité A4 - Gestion des Informations (Données)

6.1. Opération O40 - Analyse des Informations et Groupes de données

Pour chaque traitement mis en évidence, détecté : il faut considérer les données ET-OU les groupes de données associés.
Sont elles des DCP ou des informations standard ?

6.2. Opération O41 - Distinction des 3 x types de DCP et des groupes DCP

Classification (types + catégories) des DCP et des groupes DCP associés.

6.3. Opération O42 - Production des Fiches Descriptives individuelles de Données et de Groupes

Pour chacun des 3 x types de DCP et chaque groupe DCP, il faut constituer la fiche descriptive rapide.

7. Détails : Activité A5 - Structurer les Traitements

7.1. Opération O50 - Représentations complètes

Visualiser intégralement les Données et les composants de contextes selon les points de vues recherchés (Vue détaillée, Vue synthétique, Vue identitaire, ...)

8. Détails : Activité A6 - Constituer le Registre des Traitements

8.1. Opération O60 - Production des Fiches Descriptives individuelles par Traitement

Utilisation de la documentation rapide.

8.2. Opération O61 - Production du rapport d'ensemble == Registre global des Traitements

Utilisation du rapport d'ensemble selon la maquette dédiée.

9. Détails : Activité A7 - Sélectionner les Traitements pour AIPD

9.1. Opération O70 - Priorisation des Traitements DCP sensibles

Rappel : AIPD = DPIA.

Afin de d'analyser les impacts sur les informations (DCP) sensibles mises en jeu par ces traitements prioritaires.

win-design.com

Tel : +33(0)4 42 96 51 67