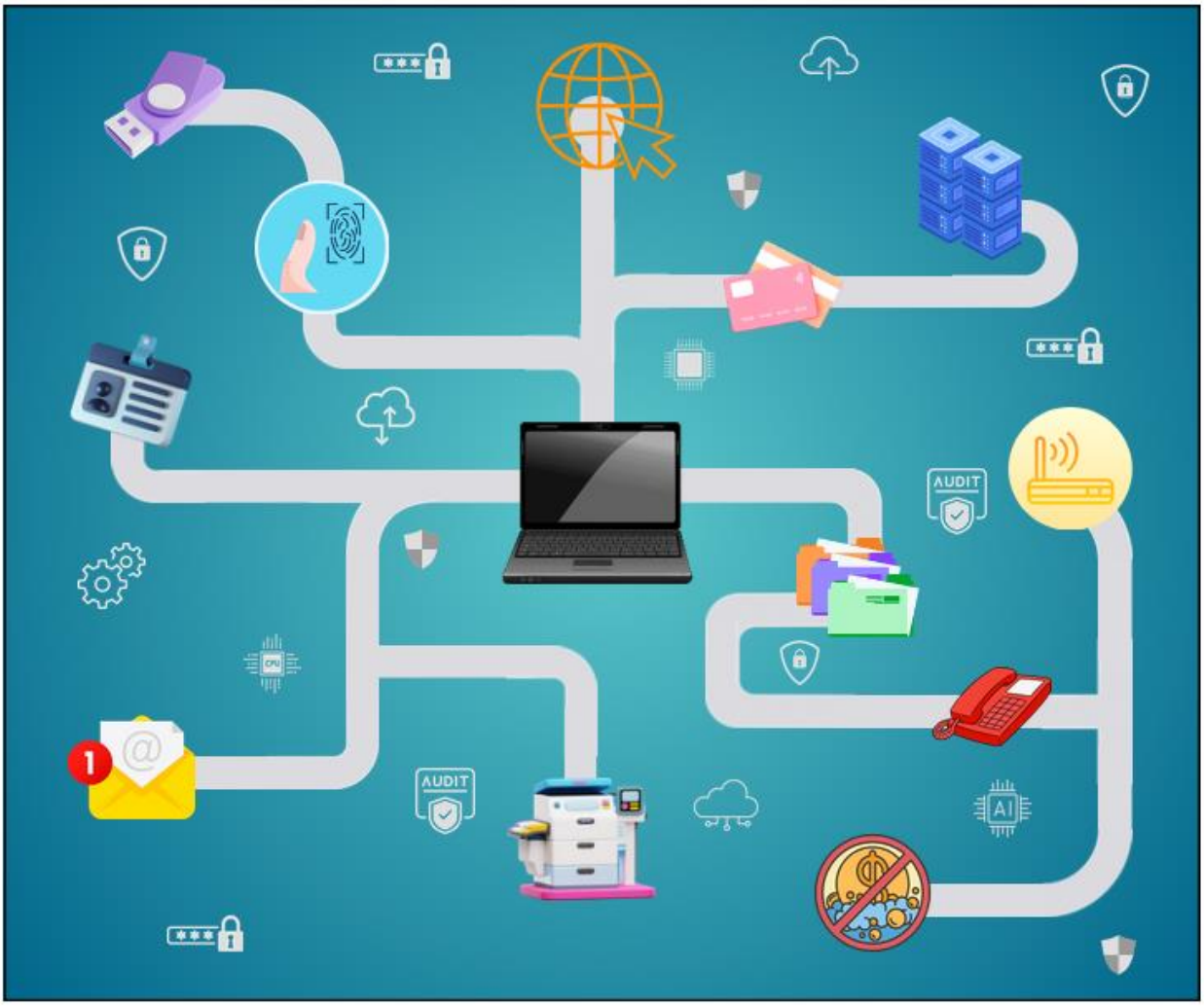
Cartographie : Comment recenser vos traitements de données personnelles ?

Etape désormais incontournable pour la mise en conformité avec la Loi n° 1.565 du 3 décembre 2024, une cartographie de l'ensemble des opérations ou ensemble d'opérations appliquées à des données personnelles (à savoir les traitements) permet de produire une vue exhaustive des données personnelles traitées par une entité, et ce depuis la collecte de ces données jusqu'à leur suppression.

Une telle démarche de recensement semble ainsi nécessaire pour toute entité monégasque désireuse d'assurer la protection des données à caractère personnel qu'elle détient.



Cette fiche a donc pour objectif de guider les responsables du traitement dans la cartographie de leurs traitements ; cartographie comportant 6 éléments clés qui peut être réalisée en utilisant une approché métier ou technique, voire même une combinaison des deux, et qui surtout doit faire face à de nombreux défis.

Qu'est-ce qu'une cartographie?
La cartographie des traitements de données personnelles consiste à identifier et répertorier tous les traitements au sein d'une entité (entreprise, administration, association, etc). Concrètement, elle permet à chaque responsable du traitement de déterminer, pour chaque traitement, le nom et les coordonnées du responsable du traitement, la finalité (à savoir l'objectif) dudit traitement (relation commerciale, gestion RH,…), les catégories de personnes concernées (clients, salariés, candidats,…), les acteurs, internes ou externes, amenés à gérer ces données, le parcours des flux de données en cas de transferts hors de la Principauté, les délais prévus pour l'effacement des données et, enfin, une description des mesures de sécurité techniques et organisationnelles prises pour en assurer leur protection. Bien menée, elle illustre une réalité qui peut être à la fois dense et complexe et permet de mettre en évidence les imbrications et les interdépendances entre les multiples composants du Système d'Information (SI) et ses différentes couches.

Les 6 éléments clés pour réussir sa cartographie

Ces 6 éléments clés s'articulent autour de 6 questions principales.

1 – QUI gère le traitement ?

Il est nécessaire de savoir avant toute chose qui sont les acteurs qui, en interne ou en externe, sont susceptibles de manipuler les données. Ainsi, il convient de noter le nom et les coordonnées du responsable du traitement (et lorsque cela est le cas, de son représentant et/ou de son délégué à la protection des données), d'identifier les responsables des services opérationnels traitant les données au sein de l'entité et d'établir la liste des sous-traitants. Concernant ces derniers, une liste à jour permettra notamment de vérifier et de modifier, si besoin, les clauses de confidentialité contenues dans leurs contrats.

2 – QUOI est collecté ?

La deuxième étape importante de la cartographie est de déterminer quelles sont les données à caractère personnel traitées pour chaque acteur. Pour cela il convient d'identifier les différentes catégories de données traitées mais également les données susceptibles de soulever, en raison de leur sensibilité, des risques particuliers, telles que, par exemple, les données relatives à la santé.

3 - POURQUOI ces données sont-elles traitées ?

Une fois ces deux 1ères étapes passées, il est nécessaire de déterminer les objectifs poursuivis par ces opérations de traitement de données, à savoir leur finalité ; celle-ci pouvant

par exemple être la gestion des ressources humaines, la gestion du contentieux ou bien encore la gestion de la messagerie professionnelle.

4 - OU sont hébergées les données ?

Une autre étape essentielle est de déterminer les lieux physiques où sont hébergées les données personnelles mais aussi le ou les pays vers le(s)quel(s) ces données peuvent ensuite être transférés. Cette question est particulièrement importante pour les données situées dans le *cloud*. En effet, ces données peuvent déménager très facilement et il peut alors devenir ardu de suivre leurs transferts successifs.

5 - COMBIEN de temps sont stockées les données ?

La question de la conservation des données est une autre interrogation essentielle. Pour chaque catégorie de données à caractère personnel, il faut donc préciser combien de temps il est nécessaire de les garder. Cela peut être par exemple 30 jours pour les images de vidéosurveillance ou bien encore jusqu'au règlement amiable d'un litige dans le cadre de la gestion d'un précontentieux.

6 - COMMENT la sécurité des données est-elle assurée ?

Enfin, il est indispensable de mettre en lumière les différentes mesures de sécurité qui ont été mises en œuvre pour minimiser les risques d'accès non autorisés aux données, le but étant de limiter le plus possible l'impact sur la vie privée des personnes concernées. Une des premières mesures de sécurité consiste par exemple à mettre en place des mots de passe nominatifs « *forts* » et régulièrement renouvelables pour accéder aux ordinateurs.

Les différentes approches permettant de cartographier les traitements

Deux approches, souvent complémentaires, peuvent être retenues pour réaliser une cartographie et s'assurer que tous les opérations portant sur des données personnelles ont bien été recensées : une approche métier (qui part de l'individu concerné par le traitement des données) et une approche technique (qui part du processus de gestion des données).

1 – L'approche métier

Cette approche revient à suivre les 4 étapes suivantes :

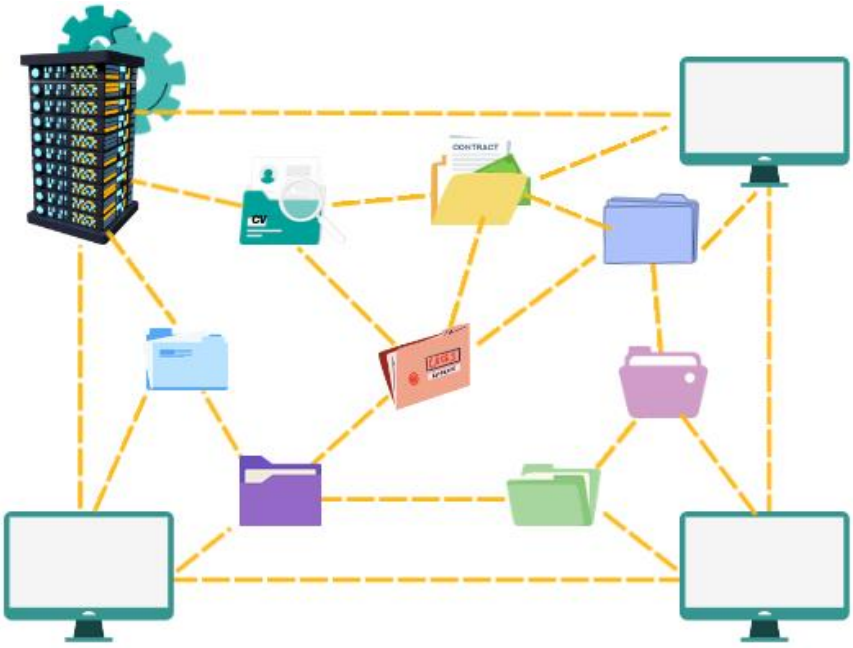
- **IDENTIFIER les catégories de personnes physiques** qui sont en interaction avec l'entité**.** Il peut ainsi s'agir des employés, des clients, des prospects, des utilisateurs, des fournisseurs, etc.
- **RECENSER**, pour chaque catégorie de personnes, **la nature des données personnelles** collectées par l'entité concernée
- **SUIVRE les flux de données,** à savoir leurs points d'entrée et de transfert
- **IDENTIFIER les traitements** effectués sur ces données

Exemple : Partons des employés. Pour ces derniers, des catégories de données telles que leurs salaires, leurs situations familiales, leurs avantages sociaux et/ou leurs problèmes de santé peuvent être collectées.

Une fois toutes ces catégories de données bien répertoriées, il devient plus aisé de définir quel service au sein de l'entité est responsable par exemple du suivi des performances et quel autre est responsable du suivi des données médicales.

A charge alors à ces services de mettre en place une politique de gestion des données en portant une attention particulière aux données critiques (numéro de compte bancaire par exemple) et de déterminer une stratégie de rétention de ces données.

2 – L’approche technique



Cette approche repose sur la procédure suivante :

- **DEFINIR les processus** internes et externes en interaction avec les personnes concernées
- **RECENSER les systèmes d’information** sur lesquels reposent directement ces processus
- **IDENTIFIER les flux et traitements** de données personnelles supportés par ces systèmes
- **REMONTER les flux et traitements** de données personnelles

Exemple : Partons cette fois du système physique qui gère les données d’identité. Ces données peuvent provenir du système de recrutement puisque l’employé en question a été un candidat avant d’être recruté, du système de gestion de la paie ou encore du système de gestion des frais professionnels et de déplacement qui peut contenir des informations sensibles, telles que des numéros de cartes de crédit.

Là encore, une fois que tous ces systèmes auront été identifiés, il deviendra plus facile pour l’entité d’avoir une vision complète du cycle de vie des données de ses employés, de leur arrivée au sein de l’entité à leur départ.

La cartographie dans le temps : défis et bonnes pratiques

Au-delà de sa création, une cartographie doit vivre et évoluer dans le temps. Cet inventaire qui se veut exhaustif, doit en effet impérativement être régulièrement tenu à jour afin de devenir le document de référence incontournable permettant à toute entité de s'assurer de sa conformité en matière de protection des données personnelles.

Face aux défis d'une matière en perpétuelle évolution, il est donc important pour les entités concernées d'adopter certaines bonnes pratiques.

1 - Une méthodologie d'investigation rigoureuse

Une cartographie incomplète expose l'entité à un risque important de vulnérabilité en matière de protection des données et peut entraîner la mise en place d'actions correctives mal proportionnées (coût de ressources engagés trop élevé par exemple).

Il est donc important de mettre en place une méthodologie d'investigation rigoureuse, notamment lorsque le SI est complexe, notamment en cas de

- traitement massif de données (solutions *big data*) ;
- recours à la **virtualisation** ;
- multiples **périmètres IT ou métier externalisés**, notamment *via* le *cloud*.

2 – Une cartographie pragmatique et réactive

Comme mentionné précédemment, la cartographie doit représenter à tout instant la réalité du SI, que cette réalité soit celle de l'existant ou bien une projection sur l'avenir (cibles).

3 – Une cartographie en perpétuelle évolution

Trop figée, une cartographie peut vite devenir inutile et coûteuse. C'est donc un chantier permanent qui doit accompagner la vie de l'entité, de manière progressive, en mettant en concordance les visions métier et technique.

4 – Une cartographie compréhensible

La cartographie enfin doit favoriser le dialogue et la compréhension du futur par tous les acteurs concernés. Elle doit ainsi être compréhensible par tous et expliquer clairement les changements qui pourraient être à réaliser.

En conclusion, une cartographie réussie est un outil qui permet à un responsable du traitement d'identifier aisément tous les traitements (par finalité) contenant des données personnelles qu'il a mis en oeuvre.