Denis VIROLE
Directeur des services d'Ageris Group
Gérant de Virole Conseil Formation

Les organismes et entreprises doivent être conformes aux exigences du 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 en mai 2018. A un an de l'échéance, un grand nombre d'organisations n'a pas formalisé de démarche, ni initialisé de plans d'actions.

Nous nous intéressons ici à la formalisation d'un plan d'action juridique, organisationnel et technique adapté en soulignant les difficultés inhérentes à un profil de maturité.

Maturité d'entreprise et plan d'action pour la mise en conformité avec le Règlement Général sur la Protection des Données à caractère personnel

Introduction

Un an après la définition du règlement (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 (règlement général sur la protection des données), et à un an de la date d'application, nous allons nous intéresser à la définition d'un plan d'actions concret et pragmatique. Nous illustrerons les étapes de ce plan d'actions par les difficultés potentielles en fonction du profil de maturité de l'entreprise pour la protection de la vie privée.

1. Les trois types de maturité pour la protection de la vie privée et la sécurité des données à caractère personnel

Nous proposons de modéliser trois types de maturité pour la protection de la vie privée et la sécurité des données à caractère personnel :

- **Maturité faible** :

  Le premier marqueur de ce type d'organisme est le très faible niveau de sensibilisation des différents acteurs (responsable du traitement, directions métiers déléguées par le responsable du traitement, sous-traitant, direction Informatique et utilisateurs)

  L'absence de CIL est souvent un marqueur important de ce type d'organisme, la fusion de la fonction CIL avec la fonction de DSI en est un autre. Classiquement dans ces cas, l'organisme se conforme aux différents régimes déclaratoires de conformité, notamment aux normes simplifiées et autorisations uniques, sans réellement contrôler les exigences de la norme simplifiée en termes de types de données, de destinataires et de durées de conservation.

  Les procédures de traitement des demandes d'accès ou de rectification consécutives aux droits des personnes concernées sont inexistantes.

  La sécurité des données à caractère personnel est réalisée dans le meilleur des cas par une approche « sécurité informatique » constituée de règles autojustifiées par la compétence technique des informaticiens. Il n'y a donc pas de relation structurée pour exprimer les besoins et

objectifs de sécurité entre, d'une part les métiers définissant la finalité des traitements, et les informaticiens internes ou externes mettant en œuvre ces traitements.

- **Maturité moyenne** :

Le premier marqueur est clairement la nomination d'un CIL. Très classiquement le DSI ou le RSSI « intègre la fonction ». Il est intéressant de noter que certaines autorités de contrôle, (telle que la Commission Nationale pour la Protection des Données du Luxembourg), refusent ce type de cumul de fonctions.

Le CIL réalise ou tente de réaliser un plan de sensibilisation auprès des différents acteurs (responsable du traitement, directions métiers déléguées par le responsable du traitement, sous-traitant, direction Informatique et utilisateurs).

Il est important de souligner que dans l'intégration de la fonction CIL par le RSSI ou le DSI ne facilite pas la responsabilisation des directions métiers, la problématique est encore comprise comme « informatique ».

Dans le cas où les fonctions et les responsabilités sont bien séparées entre le CIL et le RSSI. La relation n'est pas toujours fluide et le plan de sensibilisation n'a pas permis la mise en œuvre effective de réelles actions structurantes et efficaces pour la sécurité des données à caractère personnel. (Contrôle des accès, des habilitations, des durées de conservation, des procédures d'utilisation des supports de données à caractère personnel, …)

La gouvernance des aspects protection de la vie privée, sécurité des données à caractère personnel, d'une part et sécurité système d'information n'est pas formalisée ou comprise par l'essentiel des acteurs dans l'organisme.

Les directions métiers sont encore peu engagées dans les procédures de mise en conformité des traitements.

L'intégration native de la protection de la vie privée et la sécurité des données à caractère personnel ne sont pas prises en compte dans les méthodes de gestion de projet. Dans le meilleur des cas, pour ce type d'organisme, les procédures permettant aux personnes concernées d'exercer leurs droits sont formalisées. Reste à savoir si elles sont comprises et testées.

- **Maturité forte** :

Le premier marqueur, et clairement le plus important, est la prise de conscience de la responsabilité du responsable du traitement.

La nomination d'un CIL ne cumulant pas des fonctions de CIL ou de RSSI et réalisant de nombreuses campagnes de véritables formations plus que de sensibilisation ou de communication a permis à chacun de comprendre les différentes responsabilités.

Le deuxième marqueur est 'intégration de la fonction CIL dans une gouvernance globale pour la protection de l'information formalisant les relations avec les maitres d'œuvre internes ou externes permet de structurer les projets comprenant des données à caractère personnel. La définition de voies fonctionnelles articulées autour d'un comité de pilotage, arbitrage et homologation : (protection de la vie privée et sécurité des données à caractère personnel, conservation des documents, sécurité système d'information, protection des personnes et des installations, …)

La définition de référentiels cohérents, complémentaires appliqués par les parties prenantes, comprenant les aspects de la protection de la vie privée (incluant les procédures pour permettre aux personnes concernées d'exercer leurs droits), de la protection de l'information et la sécurité des systèmes, constitue un autre marqueur décisif.

2. La cible à atteindre

Nous proposons ici de synthétiser ici la cible ultime que le plan d'action devra atteindre.

En effet la conformité avec le règlement général sur la protection des données à caractère personnel peut être structurée en quatre axes principaux :

1. Un renforcement majeur des droits des personnes concernées,
2. Un renforcement majeur des obligations de sécurité des données à caractère personnel et de protection de la vie privée,
3. Un renforcement des responsabilités du responsable du traitement et surtout la définition de nouvelles responsabilités pour le sous-traitant,
4. L'obligation d'être en mesure de fournir des preuves de la conformité.

3. Les étapes du plan d'action

La figure 1 illustre la cible et les différentes étapes :

La cible pour les organismes est très claire, il s'agit d'être en mesure pour mai 2018 de démontrer la conformité au Règlement.

Dans un deuxième temps nous identifierons les difficultés à surmonter en fonction du profil de maturité de l'organisme.

Cette cible ne peut être atteinte sans réaliser les actions consécutives aux 5 types d'étapes :

1. La formation du responsable du traitement, des directions métiers, de l'encadrement intermédiaire, des directions supports (DSI, sûreté des installations, …) et de l'ensemble des utilisateurs manipulant des données à caractère personnel.

   Cette campagne de formation a conduit à

   - La nomination d'un chef de projet pour la mise en conformité,
   - La nomination éventuelle du DPO.

   Il est important de noter que la formation devra être reproduite et adaptée aux différents acteurs en fonction des étapes.

2. La cartographie de l'ensemble des traitements, la définition du registre puis la formalisation de politiques de protection de la vie privée destinée aux clients ou aux usagers et une particulière à usage interne.

   Ces politiques doivent être mises en cohérence avec l'ensemble du référentiel protection de l'information, sécurité des systèmes d'information.

   La mise en place d'une gouvernance identifiant les acteurs et les responsabilités ainsi que les articulations avec l'organisation hiérarchique, les fonctions de contrôle interne d'une part et l'autorité de contrôle CNIL d'autre part.

3. La formalisation des procédures permettant aux personnes concernées d'exercer leurs droits. Ces procédures doivent être enseignées aux différents acteurs de l'organisme, puis testées.

   Les mentions légales doivent être mises à jour. Les contrats avec les sous-traitants doivent intégrer les nouvelles obligations. Ces contrats doivent faire l'objet de Plans d'Assurance Sécurité permettant au responsable du traitement d'avoir l'engagement du sous-traitant à respecter les règles fonctionnelles de sécurité définies dans les politiques de l'organisme. Le

Plan d'Assurance Sécurité devra démontrer la transcription effective de l'application des règles fonctionnelles de sécurité des données à caractère personnel.

La sécurisation des systèmes hébergeant des données à caractère personnel est essentiellement réalisée par l'adjonction d'outils extérieurs pour protéger des systèmes ou des applications n'ayant pas intégré une démarche native de sécurité pendant tous les cycles de vie du projet.

4. L'étape quatre doit conduire à systématiser pour tout projet traitant des données à caractère personnel, la démarche de sécurité dès la phase de conception jusqu'à la phase de mise en production.

5. La dernière étape doit permettre non seulement de fournir la preuve à l'autorité de contrôle, voire à la personne concernée que les traitements sont conformes aux principes du règlement, mais aussi de contrôler l'efficacité de l'ensemble des mesures pour la protection de la vie privée.

Figure 1 : les étapes

<table>
<tr><td rowspan="2">Maturité</td><td colspan="2">Faible</td><td>Moyenne</td><td colspan="2">Forte</td></tr>
<tr><td>Pratique inexistante</td><td>Pratiques de base mises en œuvre de manière informelle</td><td>Pratiques de base mises en œuvre, avec un engagement de l'organisme vis-à-vis des PC</td><td>Processus défini, décrit, adapté à l'organisme, généralisé et bien compris par le management et par les exécutants</td><td>Processus coordonné et contrôlé à l'aide d'indicateurs permettant de corriger les défauts constatés</td></tr>
<tr><td colspan="2" rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="3">Preuve
+
Contrôle des mesures juridiques et techniques
+
Labellisation
Protection de la vie privée
+
Codes de conduite
+
Certification</td></tr>
<tr><td rowspan="2">Intégration de la sécurité des DCP dans les projets
+
EIVP
+
Security by design</td></tr>
<tr><td colspan="2">Registre des traitements

Politiques et référentiels
Gouvernance</td><td>Respect des droits de la PC
+
Contrats
+
Plan d’Assurance sécurité
+
Adjonction d’outils SSI
Security by default</td></tr>
<tr><td></td><td colspan="5">Sensibilisation
Formation
Directions
Métiers
+
Utilisateurs
Nomination du Chef de projet / DPO</td></tr>
<tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td></td><td colspan="4">Temps</td><td>Mai 2018</td></tr>
</table>

4. Les difficultés de chaque étape en fonction du niveau de maturité

Il est important de noter que l'évolution du niveau de maturité à l'intérieur de chaque étape constitue aussi des paliers progressifs pour la mise en conformité.

4.1. Etape 1 : La sensibilisation et la Formation

4.1.1. Etape 1 : Les organismes à faible maturité

La sensibilisation du responsable du traitement constitue une étape fondamentale ; de son succès dépend les autres étapes.

Le responsable du traitement doit clairement comprendre quelles sont ses responsabilités. Le montant des nouvelles sanctions administratives (jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial) constitue évidemment un vrai levier juridique.

Il est néanmoins dommage de mettre pédagogiquement en avant les sanctions quand l'on sait que l'objectif du règlement est : « *de respecter tous les droits fondamentaux et d'observer les libertés et les principes reconnus par la* ***Charte des droits fondamentaux de l'Union Européenne****, consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des données à caractère personnel, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et accéder à un tribunal impartial, et la diversité culturelle et religieuse* ».

Cette sensibilisation auprès du responsable du traitement devrait permettre de définir un chef de projet pour la mise en conformité puis de nommer un DPO (externe ou interne), même dans les cas où ce n'est pas obligatoire. La nomination d'un DPO constituant un véritable acte citoyen facilitant notamment le respect des droits de la personne concernée.

Il est clair que ce profil d'entreprises ou organismes est très peu préparé aux étapes suivantes.

Le responsable des traitements doit par conséquent allouer les budgets et les ressources nécessaires pour permettre à l'éventuel DPO de réaliser ses missions et pour le suivi du plan d'action.

Cette sensibilisation comme pour les autres types d'organisme devra être complétée de véritables formations notamment auprès de l'encadrement intermédiaire et des acteurs techniques chargés de la mise en œuvre effective des traitements.

4.1.2. Etape 1 : Les organismes à maturité moyenne et forte

Comme nous l'avons évoqué plus haut, ce type d'organisations se caractérise par une compréhension plus forte du responsable du traitement sur la problématique de la protection de la vie privée et la sécurité des données à caractère personnel. Aussi la sensibilisation devra se concentrer sur les nouveautés et leurs impacts en termes de responsabilités et de gouvernance.

4.2. Etape 2 : La constitution du Registre, la définition des référentiels et la mise en œuvre de la gouvernance

4.2.1. Etape 2 : Les organismes à faible maturité

Les organisations à faible maturité au regard de la protection de la vie privée ont rarement nommé un CIL ; aussi la constitution du registre représente une nouveauté.

La constitution du registre (obligatoire) doit permettre de réaliser une véritable cartographie des traitements, des finalités, des durées de conservation des données à caractère personnel, des destinataires et des personnes chargées de la mise en œuvre effective des traitements.

Il est important de noter que la constitution d'un registre ne pourra se faire qu'après avoir formé des relais dans les directions métiers, organisés grâce à une gouvernance structurée dans un véritable référentiel.

Cette étape devra être complétée par la définition de politiques puis par la mise en place d'une véritable gouvernance.

4.2.2. Etape 2 : Les organismes à maturité moyenne

C'est sur ce dernier point que se concentreront les organismes à maturité moyenne, dans le cas où le Registre des traitements est déjà constitué.

La formalisation de politiques de protection de la vie privée et de sécurité des données à caractère personnel doit non seulement être mise en cohérence avec la politique de sécurité système d'information, mais aussi « chapeautée » par une véritable lettre d'engagement du responsable du traitement, démontrant son engagement de responsabilité et sa volonté de fournir les moyens budgétaires, humains et techniques pour se mettre en conformité.

Ainsi trois niveaux de textes devraient constituer ce référentiel :

1. Stratégique : La lettre d'engagement du responsable du traitement.

   Deux écoles se profilent : la première est de définir ce texte en parallèle de la lettre d'engagement pour la protection de l'information et la sécurité des systèmes d'information. La deuxième école est plutôt de fusionner les deux thématiques et de monter la cohérence de l'approche.

2. Tactique et fonctionnel : La politique générale pour la protection de la vie privée ou plutôt les politiques de protection de la vie privée, l'une devant être formalisée à destination des clients ou des usagers.

   Elle présente les règles fonctionnelles consécutives aux principes du règlement respectées par le Responsable du Traitement à l'égard des personnes concernées clientes ou usagers.

   L'autre à usage interne destinée aux directions métiers présente la démarche, les responsabilités respectives internes et les règles fonctionnelles à usage interne.

   La politique générale de protection de la vie privée devrait faire appel aux règles de sécurité de la politique sécurité système d'Information, supposée exister dans les organismes à maturité moyenne.

3. Opérationnel : ce niveau de texte constitué de guides, manuels et chartes présente les règles opérationnelles et pratiques de protection de la vie privée.

Comme pour les organismes à fable maturité, le défi majeur est dans la mise en œuvre opérationnelle de la gouvernance et de la supervision.

4.2.3. Etape 2 : Les organismes à maturité forte

Les organismes à forte maturité sont censés avoir déjà réalisé la phase de définitions des politiques, aussi ils ne réaliseront qu'une adaptation pour intégrer les nouveaux droits des personnes concernées et les nouveaux devoirs du Responsable de Traitement (nouvelles informations à fournir, sécurité et notification de violations de données à caractère personnel à l'autorité de contrôle, voire à la personne concernée).

Aussi, c'est bien dans la mise en place d'une nouvelle gouvernance que se caractérise cette étape pour les entreprises ou organisations en maturité effective.

La nomination du DPO dans le DSI n'est pas dans l'esprit du règlement, nous rappelons que certaines autorités de contrôle le refusent. La fonction de contrôle du DPO exige une séparation avec la fonction de mise en œuvre. Nous avons aussi souvent constaté que le cumul de la fonction CIL avec celle de DSI, voire de RSSI ne facilite pas la responsabilisation des directions métiers qui ressente encore la problématique comme technique.

Dans ces organismes à forte maturité, le DPO sera nommé à la direction de l'Audit, de la conformité ou à la direction juridique.

Il est important de souligner que souvent les directions juridiques ne se sentent pas à l'aise avec les aspects sécurité « techniques » obligatoires pour garantir une protection réelle de la vie privée. Ils ne viennent pas participer aux Eudes d'Impact sur la Vie Privé que nous aborderons dans l'étape 4. Une autre question se pose : sur le contrôle de la conformité présentée dans la dernière étape, les profils juridiques sont-ils les plus adéquats pour réaliser ce contrôle ?

La gouvernance pour la protection de la vie privée devra s'articuler autour de deux voies fonctionnelles non hiérarchiques en parallèle de la voie hiérarchique et pilotées par un comité de pilotage, arbitrage et suivi chargé notamment de la validation des traitements. Cette validation devant être considéré comme une véritable homologation :

1. La voie fonctionnelle pour la protection de la vie privée, animée par le DPO, constituée de relais dans les directions métiers, elle doit permettre l'intégration des exigences du règlement dans chaque direction.

   Elle doit faciliter la remontée d'incidents en évitant les ressentis éventuels de culpabilité ou de délation. A ce titre, il est important de noter que le DPO n'a pas de pouvoir hiérarchique dans lesdites directions métiers. C'est au DPO de décider, en fonction de la gravité, de la nécessité de remonter l'incident au responsable du traitement, à l'autorité de contrôle, voire à la personne concernée.

   Elle doit permettre de solliciter le comité de pilotage, arbitrage et suivi pour arbitrage, car les divergences d'estimation ne seront pas rares à l'intérieur des directions métiers et bien sûr avec la direction système d'information ou le sous-traitant.

   De plus, seule la voie fonctionnelle pour la protection de la vie privée serait apte à gérer les éventuelles demandes de dérogations.

   Le principe étant que seule l'équipe formalisant les règles peuvent fournir des dérogations. Dans ce cas le comité de pilotage, arbitrage et suivi devra être consulté.

Il est intéressant que les grands groupes à très forte maturité aient déjà initialisé une voie fonctionnelle pour la protection des informations (et non pas pour la protection des systèmes). Aussi il n'est pas rare que cette voie fonctionnelle fusionne avec la voie fonctionnelle protection de la vie privée.

2. La voie fonctionnelle SSI, animée par le RSSI, chapeautée par le comité de pilotage, arbitrage et suivi a les mêmes objectifs que la voie fonctionnelle pour la protection de la vie privée mais sur le périmètre de la sécurité système d'information.

Il est important de noter la nécessité de formaliser dans une méthode adaptée une relation structurée entre les métiers chargés de formaliser les besoins et les événements redoutés et les maitres d'œuvre chargés de la réalisation des objectifs de sécurité.

4.3. Etape 3 : Le respect des droits de la personne concernée, la formalisation des contrats et la sécurité par adjonction d'outils

4.3.1. Etape 3 : Les organismes à faible maturité ou moyenne

L'étape est ici fondamentale pour les deux profils d'organisations :

Le responsable du traitement doit fournir treize informations à la personne concernée lorsque les données sont collectées directement, quatorze lorsqu'elles sont collectées indirectement.

1. L'identité et les coordonnées du responsable du traitement,
2. Les coordonnées du DPO,
3. Les finalités du traitement,
4. Les intérêts légitimes poursuivis par le responsable du traitement lorsque le traitement est fondé sur l'art. 6§1,
5. Les destinataires ou catégories de destinataires des données à caractère personnel,
6. L'intention d'effectuer un transfert de données à caractère personnel hors Union Européenne,
7. La durée de conservation des données à caractère personnel,
8. Les droits d'accès, de rectification ou l'effacement de celles-ci, de limitation du traitement et le droit à la portabilité,
9. L'existence du droit de retirer son consentement à tout moment lorsque le traitement est fondé sur l'art. 6§1 point a) ou sur l'art. 9§2 point a),
10. Le droit d'introduire une réclamation auprès d'une autorité de contrôle,
11. Des informations sur la question de savoir si l'existence de la fourniture des données à caractère personnel a un caractère réglementaire ou contractuel,
12. L'existence d'une prise de décision automatisée, y compris d'un profilage
13. Si modification de la finalité lors d'un traitement ultérieur, le responsable du traitement doit informer la personne concernée,
14. Le responsable du traitement doit fournir la source d'où proviennent les données à caractère personnel et une mention indiquant qu'elles sont issues ou non de sources accessibles au public, lorsque les informations n'ont pas été collectées directement auprès de la personne concernée.

Ceci représente une véritable nouveauté. Les autorités de contrôle seront particulièrement vigilantes puisque l'information de la personne concernée constitue le préambule au respect de ces droits.

Les informations légales devront permettre d'acquérir, quand c'est nécessaire, le consentement éclairé et univoque de la personne concernée. Le responsable du traitement devra recueillir les éléments pour en fournir la preuve. Le consentement devra pouvoir être retiré aussi facilement que sa fourniture.

Une part importante du chantier de cette étape est de formaliser un ensemble important de procédures permettant aux personnes concernées d'exercer leurs droits en face à face, en utilisant un mandataire, par courrier postal, par mail, en interne, externe ….

Il est important de rappeler que les délais de réponse ont changé et que le premier délai est fixé à un mois au lieu de deux dans la loi I &L.

Nous soulignons ici que ceci constitue la partie la plus visible de la conformité et qu'elle est particulièrement sensible puisqu'elle détermine clairement le respect de la vie privée et des libertés fondamentales.

Le lecteur doit savoir que les autorités de contrôle peuvent surveiller les organismes en ligne.

Les responsabilités des sous-traitants devront être définies dans les contrats. Elles devront aborder non seulement les aspects juridiques et contractuels mais aussi techniques de sécurité. Ce profil d'organisme a rarement formalisé les exigences techniques de sécurité dans un document annexe au contrat : le Plan d'Assurance Sécurité. L'ANSSI a constitué un outil intéressant dans un PAS type à faire compléter par le sous-traitant.

Cette étape doit être complétée par la sécurisation des systèmes informatiques, dite « by default » dans le règlement.

Les entreprises à faible ou moyenne maturité ne possèdent que rarement des politiques de sécurité et devront appliquer des bonnes pratiques de sécurité.

La formalisation d'une PSSI structurée selon la norme ISO 27002 ou inspirée de la PSSI E (de l'Etat pour le non confidentiel défense) est clairement ressentie comme lourde ; aussi l'application des mesures issues du guide d'hygiène de sécurité informatique, en complément des recommandations CNIL, est perçue comme pragmatique et adaptée à la taille et aux enjeux de ce type d'entreprise.

Pour ce profil d'entreprises ou d'organisations, il n'est pas rare de se contenter d'une minimisation des données à caractère personnel complété d'une approche de sécurisation constituée d''ajouts de produits de sécurité additionnels sensés sécuriser à la fois les données et protéger la vie privée des personnes concernées.

La minimisation des données à caractère personnel a pour objectif de s'assurer que seules les données à caractère personnel adéquates, pertinentes et non excessives au regard de la finalité poursuivie, sont collectées.

La recommandation est claire : seuls les champs relatifs aux données à caractère personnel déterminés sont créés et peuvent être renseignés dans une base de données et aucun autre champ ne peut être ajouté (ne pas prévoir de champ « texte libre ») et de bien vérifier régulièrement qu'aucune DCP supplémentaire n'a été collectée par rapport à ce qui était initialement prévu…

Cette approche est possible si l'expression des besoins et exigences juridiques est réellement exprimée par les directions métiers et arbitrée par une structure collégiale, (rarement mis en place dans ce type d'organisme) pour être en relation avec ces bonnes pratiques.

Sinon cette sécurité restera constituée de règles auto justifiées par l'informatique et la sécurité et leurs adéquations avec les besoins des directions métiers ne saurait être garantie.

L'application du premier alinéa de l'article 32 du règlement mentionne : « *compte tenu de l'état des connaissances, des couts de mis en œuvre et de la natures, de la portée du contexte et des finalités des traitements ainsi que des risques, dont le degré de probabilité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque y compris entre autres selon les besoins :*

a) La pseudonymisation et le chiffrement des données à caractère personnel »

On voit bien ici la nécessité d'une concertation forte en les directions métiers déléguées par le responsable du traitement et les équipes de mise en œuvre, direction des systèmes d'information ou sous-traitants.

La DSI ou le sous-traitant ne peuvent, sans instruction des directions métiers, identifier la sensibilité des données à caractère personnel et la finalité des traitements. L'expression des besoins nécessite leur implication, l'identification des évènements redoutés ne peut se faire sans elles et la validation des risques résiduels juridiques et techniques relève de leurs responsabilités.

La mise en œuvre des dispositifs de pseudonymisation et de chiffrement doit être mise en œuvre en corrélation avec la sensibilité des données à caractère personnel, la finalité du traitement et l'impact potentiel pour la vie privée.

L’idée est de protéger au maximum la vie privée de la personne concernée.

La première possibilité est donc de faire perdre définitivement le caractère identifiant des données à caractère personnel. Une « véritable » anonymisation implique nécessairement une perte (irréversible) d’information. Dans certains cas, le simple fait d’effacer ou de noircir une partie des données peut suffire à atteindre l’objectif souhaité.

La « pseudonymisation » est donc plus adaptée à un grand nombre de traitements. Elle peut être définie comme le remplacement d'un nom par un pseudonyme. C’est le processus par lequel les données perdent leur caractère identifiant (de manière directe). Les données restent liées à la même personne dans tous les dossiers et systèmes informatiques sans que l’identité ne soit révélée. Elle est opérée avec la possibilité de retour vers les noms ou identités.

Il convient de garder à l’esprit que la corrélation de données à caractère personnel pseudonymisées reste possible et qu’une ré-identification peut intervenir à partir d’informations partielles dès lors qu’une donnée à caractère personnel est pseudonymisée et non purement supprimée. En effet, il est possible d’associer la donnée originale à la donnée pseudonymisée dès lors que le secret est compromis et que la complexité de la donnée originale n’est pas suffisante.

Les autorités de contrôle conseillent que de pratiquer une véritable suppression de données, ou de réaliser une « pseudonymisation » accompagnée de garanties organisationnelles et techniques fortes, notamment par l’utilisation de fonctions de hachage à clé secrète.

Elles recommandent de supprimer une partie suffisante des données (ex. : ne garder qu’une année de naissance et non la date de naissance complète pour éviter qu’on retrouve l’identité d’une personne en connaissant en plus son lieu de naissance et son sexe, supprimer les deux derniers octets d’une adresse IPv4), appliquer une fonction de hachage à clé secrète et supprimer la ou les clés secrètes, ou encore remplacer les DCP qui permettent d’identifier les personnes par un texte neutre (étoiles, quelques lettres identiques, identifiant séquentiel…)…

S’il est nécessaire que des personnes habilitées puissent vérifier que des données anonymisées correspondent à des données originales qu’ils ont en leur possession, il est conseiller d’utiliser une fonction de hachage SHA-256 avec une clé secrète, voire pratiquer une double pseudonymisation avec deux clés secrètes détenues par deux organismes différents ;

S’il est nécessaire à des personnes habilitées de pouvoir retrouver les données originales (levée de pseudo), utiliser une fonction de chiffrement, éventuellement en partageant une clé en trois parties confiées à trois personnes différentes (par exemple sur un CD ou une carte à puce) avec l’obligation qu’au moins deux des trois personnes se réunissent pour reconstituer la clé, afin de protéger la confidentialité du secret…

L’organisation de protection des secrets (clés, tables de correspondance…), permet si nécessaire de lever le pseudo et doit garantir que cela ne puisse être fait que par le détenteur des secrets (séparation et stockage des clés dans des coffres ignifugés, journalisation des accès…).

L’application de l’alinéa a de l’article 32 soulève deux grandes questions. La première l’organisation, la gouvernance, l’implication des directions métiers, la deuxième concerne la disponibilité des outils et produits. L’Association Française des Correspondants pour la protection des Données à caractère Personnel a constitué un référentiel d’outils mais la liste est encore limitée.

La difficulté est donc double : organisationnelle et méthodologique nécessitant de réelles concertations dans les équipes d’une part et dans la faible disponibilité des outils et produits.

La solution consiste clairement à intégrer ce type de fonction nativement dans le système d’information traitant les données à caractère personnel selon la démarche « *by design* », (voir plus bas).

4.3.2. Etape 3 : Les organismes à forte maturité

Les organismes à forte maturité sont équipés depuis longtemps d'une PSSI et de contrats complétés de PAS, aussi ils se concentreront sur la mise à niveau des procédures permettant aux personnes concernées d'exercer leurs droits, les mentions légales et les contrôles auprès des sous-traitants.

C'est pourquoi il est fondamental d'avoir formalisé un PAS avec le sous-traitant pour réaliser les contrôles prévus dans la clause d'audibilité du contrat formalisant les périmètres et les délais de prévenance.

Il nous semble important de souligner la composante humaine du sous-traitant, il doit s'engager à former ses collaborateurs, non seulement aux exigences juridiques mais aussi et surtout aux règles formalisées dans les politiques de protection de la vie privée et de sécurité des données à caractère personnel de son client.

4.4. Etape 4 : Intégration de la sécurité des données à caractère personnel dans les projets

4.4.1. Etape 4 : Les organismes à faible maturité ou moyenne

L'intégration native de la sécurité des données à caractère personnel pour garantir la protection de la vie privée EIVP, dite dans le Règlement « security by design » constitue une véritable difficulté pour ce profil d'entreprises ou organisations.

L'application littérale des normes ISO 3100 et ISO 27005, l'intégration de la méthode ANSSI EBIOS ne saurait être une réponse facile et adaptée au contexte de ces profils de maturité.

En effet les DPO à culture non technique se sentent un peu effrayés par la complexité de la méthode et tentant trop souvent une application littérale et orthodoxe. Ils manquent de recul et ont clairement besoin du RSSI pour réaliser les différentes étapes. Attention de bien comprendre que les objectifs ne sont pas les mêmes, l'un est réalisé pour protéger la vie privée de la personne concernée, l'autre pour répondre aux besoins des métiers identifiés par les évènements redoutés pour l'organisme.

La CNIL, identifiée par le G29 comme la plus avancée sur le sujet, a donc adapté la méthode EBIOS au contexte de la protection de la vie privée. La CNIL ayant bien conscience des difficultés pour ces profils a déjà formalisé deux versions de la méthode. Il est probable qu'il y en aura une troisième version.

Le succès pour ces profils d'organismes passe notamment encore une fois par de véritables formations destinées aux représentants des maitrises d'ouvrage et aux chefs de projet informatique mais aussi sans doute par des outils simples permettant de suivre de manière fluide et quasi automatisée les étapes de la méthode.

Un effort réel devra être fourni pour formaliser le processus de validation des risques résiduels par le responsable du traitement qui se sent souvent très loin de ce type de préoccupation.

4.4.2. Etape 4 : Les organismes à forte maturité

L'intégration native de la sécurité dans les projets est censée être appropriée par tous les acteurs concernés dans ce type d'organisation.

Les méthodes institutionnelles MEHARI, EBIOS ou « maison » sont donc adaptées afin de prendre en compte les spécificités des nouvelles exigences juridiques et les dommages redoutés.

L'intégration de la protection de la vie privée dans tous les projets, au même titre que l'intégration de la sécurité de l'information, n'aura pu se faire qu'à l'aide des référentiels documentaires cohérents et complémentaires diffusés et supportés par les voies fonctionnelles et leurs articulations : SSI, Protection de la vie privée, sureté des installations, combinées à un engagement fort du management.
…

4.5. Etape 5 : Contrôle des mesures juridiques et techniques

Nous rappelons ici le devoir du responsable du traitement de fournir des preuves de la conformité des traitements qu'il a fait mettre en œuvre.

A par les grands groupes qui sont habitués à mettre en œuvre des fonctions transverses de contrôle, (direction de l'audit interne ou direction de la conformité), ceci constitue une véritable nouveauté et aucun profil d'entreprise ou organisme ne se détache particulièrement. En effet certains organismes en réflexion, envisagent de nommer le DPO dans une direction orientée maitrise d'œuvre, dans ce cas ils sont vite confrontés à la difficulté de l'autocontrôle.

Un grand nombre d'organismes ou entreprises de toutes tailles identifient le label gouvernance formalisé par la CNIL comme étant une voie importante et relativement facile à suivre sur le plan méthodologique pour démontrer la conformité aux aspects organisationnels et juridiques.

Un grand nombre d'entreprises envisageront les tests intrusifs pour qualifier la sécurité informatique des traitements.

La certification de sécurité de premier niveau (CSPN) de certains produits par l'ANSSI peut être intéressante pour fournir une preuve. Ces produits peuvent poser des problèmes d'exploitation car ils ne constituent pas les standards de fait du marché et nécessitent encore une fois des plans de formation adaptés.

Une question se pose : les grands groupes, en attendant que les autorités de contrôle mettent à disposition des mécanismes de certification du respect de codes de conduite, se lanceront ils dans une démarche de type ISO 27001 pour la réalisation d'un système de management pour la protection de l'information sur le périmètre restreint du traitement des données à caractère personnel ?

Les hébergeurs de données à caractère personnel sensible vont clairement dans cette voie. La certification ajoutée à l'agrément d'hébergeurs de données de santé rassure fortement les clients. Elle nécessite un engagement fort de la direction générale et suppose un niveau de maturité toujours plus grandissant.

Conclusion

Le plan de mise en conformité avec le règlement ne saurait être plaqué sur une organisation sans prendre en compte son « histoire », sa culture, son organisation et son niveau de maturité, à la fois pour la protection de la vie privée et la sécurité des systèmes hébergeant ces données.

Nous soulignons ici qu'il nous parait fondamental de s'appuyer non seulement sur la direction juridique et les directions métiers mais aussi sur l'équipe sécurité pour se mettre en conformité. Pourtant, il n'est pas rare que celui-ci ne soit pas intégré par réflexe dans l'équipe pour le plan de mise en conformité. Or le RSSI voit toujours le règlement comme un « magnifique » levier pour pousser le responsable des traitements à toujours continuer le processus de sécurisation. Les entreprises soumises au Sarbanes Oaxley Act ont vécu le même processus : la réglementation pousse les entreprises et organismes à toujours plus intégrer les exigences de sécurité.