NOTE TECHNIQUE

Rédaction et implémentation des procédures RGPD

L'un des concepts essentiels dans le cadre de l'implémentation du RGPD est certainement le mot "accountability", qui implique que les entités qui tombent dans le champ d'application de ce règlement doivent pouvoir se justifier lorsqu'elles sont interpellées à ce sujet.

Il est donc important que le cabinet puisse être capable de démontrer qu'il respecte effectivement les dispositions de ce règlement.

Un certain degré de formalisme est donc requis, mais il tombe également sous le sens que ce degré de formalisme et de documentation dépend de la taille du cabinet.

En tout état de cause, il est important que le cabinet rédige des procédures, les implémente et puisse démontrer qu'il applique ces règles écrites.

« Responsabilisation » signifie qu'un cabinet doit pouvoir démontrer qu'il respecte les principes imposés et les règles. Les principes sont énoncés dans le règlement, mais des règles concrètes peuvent également avoir être établies par le cabinet. Ceci, sur la base du profil de risque de l'organisation, lequel doit être évalué selon les exigences spécifiques requises par la protection des données à caractère personnel.

Ces règles internes ne sauraient être à ce point si restrictives qu'aucun incident ne puisse se produire, mais l'organisation doit veiller à ce que le risque d'incidents reste limité et que des mesures appropriées soient prises, le cas échéant.

Passons en revue quelques pistes possibles, des thèmes, des considérations et des préoccupations susceptibles d'être utiles dans la rédaction de ces procédures.

Les cabinets qui ont mis sur pied un cadre de gestion interne de qualité, soit parce que c'est obligatoire, soit dans le cadre d'une démarche volontaire, devront bien entendu y intégrer ces procédures RGPD.

Dès lors que le traitement des données personnelles n'est pas à considérer de façon isolée, il ne suffit pas d'établir une procédure spécifique RGPD : il doit être tenu compte de toutes les autres procédures directement ou indirectement liées à la collecte et la conservation des données personnelles.

Analyse d'impact des données personnelles (l'estimation préliminaire des risques)

Dans le cadre de l'établissement des procédures, chaque cabinet doit au moins établir une évaluation de ses principaux risques et mesurer l'impact des éventuelles infractions au règlement.

Le règlement prévoit les cas dans lesquels une *Data Protection Impact Assessment (DPIA)* est obligatoire. On peut en déduire que cette obligation ne trouve pas à s'appliquer pour la plupart des professionnels économiques.

Sur la base d'une telle analyse préliminaire, il est possible d'évaluer si et quelles procédures devront être établies pour chaque risque identifié.

Exemples

- Les professionnels du chiffre qui sont souvent en relation avec de personnes physiques (par exemple : introduction de la déclaration à l'impôt des personnes physiques) vont encourir un risque plus élevé que ceux en rapport uniquement avec des personnes morales.
- Les professionnels du chiffre qui exercent dans des secteurs sensibles en matière de vie privée (secteur médical, expertises judiciaires, communautés religieuses) devront rehausser leur niveau de risque.
- Les professionnels du chiffre confrontés dans leurs activités avec des 'bigdata" encourent un risque plus élevé que ceux qui traitent des données spécifiques et limitées ;
- Si les mesures de sécurité sont minimes sur les plans de l'intrusion, vol, détournement, fraude le risque de survenance des incidents est plus élevé.
- Les données relatives aux mineurs sont prises en compte de façon particulière dans le règlement, ce qui génère donc une autre estimation du risque.
- Si les activités comportent des échanges de données personnelles avec d'autres pays qui n'appliquent pas une gestion stricte en matière de confidentialité, le risque est plus élevé.
- Si les données à caractère personnel sont collectées pour plusieurs finalités, il s'agit peut-être un risque accru (en ce qui concerne la nouvelle destination des données personnelles)
- Si les données à caractère personnel sont collectées sur la base du consentement plutôt que sur une base légale ou contractuelle, cela implique un risque plus élevé.
- Les professionnels économiques qui recourent fréquemment à des sous-traitants sont exposés à un plus grand risque que ceux qui y recourent moins.
- Si le professionnel dispose déjà d'un contrôle qualité solide, bien défini et appliqué, le risque est, selon toute vraisemblance, plus faible.

Procédure d'établissement et de mise à jour périodique du registre des activités de traitement

Etablir une procédure pour le développement d'un registre des activités de traitement n'a pas beaucoup de sens. Il s'agit, en effet, d'une opération unique. Mais il n'en reste pas moins important de vérifier si le registre est complet et qu'il contient bien les données qui doivent s'y trouver.

Il est donc conseillé de déterminer les modalités de mises à jour du registre.

En effet, avec le temps il est parfaitement possible que la nature, le sujet ou la finalité des données personnelles conservées évoluent, tout comme il est possible que l'on fasse usage des nouvelles techniques de communication pour le traitement des données.

Il est préférable de formaliser et de documenter une telle mise à jour périodique à l'aide d'une procédure spécifique qui doit au moins comprendre les éléments suivants :

- Qui se charge de cette révision périodique ? (à priori, la personne ad hoc désignée)
- Quelle est la fréquence des mises à jour ? par exemple, annuellement, à moins qu'il y ait des changements structurels exigeant des adaptations plus rapides.
- Selon quelles modalités ?
- Quel est le mode de communication de la mise à jour : comment et à qui ?

Dans le cadre de la mise à jour périodique du registre, il est utile de conserver un historique des différentes versions (références et archives des versions précédentes), afin de pouvoir établir précisément que telle version correspond à telle année.

Procédure en matière d'accès, de sécurité et de conservation des données

Il tombe sous le sens que cette procédure forme une partie substantielle de la politique de prévention et qu'elle mérite donc toute notre attention.

Lorsqu'ils ont intégré un système interne de gestion de la qualité, les cabinets disposent à priori, d'une procédure dans laquelle la sécurité et la conservation des données et réglée, comme mentionné au point 46 du ISQC1 : "*Le cabinet doit définir des politiques et des procédures destinées à assurer la confidentialité, l'archivage sécurisé, l'intégrité, l'accessibilité et la facilité de recherche de la documentation d'une mission",* avec des notes explicatives dans les paragraphes A56 – A59 de ISQC-1.

La conservation préservation des documents est réglementée au paragraphe 47. "*Le cabinet doit définir des politiques et des procédures pour la conservation de la documentation des missions pendant une période de temps suffisante pour répondre à ses besoins ou aux exigences de la loi ou de la réglementation",* avec des notes explicatives dans les paragraphes A60 – A63.

Le cas échéant, il est souhaitable de compléter l'ISQC1 par des passages spécifiques relatifs à la conservation et protection des données à caractère personnel traitées. Dans ce cadre, vous consulterez utilement les exemples de procédure, disponibles sur le site de l'ICCI.

S'agissant de conservation des données, ne perdez pas de vue que la protection des données personnelles ne concerne pas uniquement les données électroniques, mais également les données physiques.

Cette distinction gagne également à être formulée dans le manuel des procédures, ce qui signifie qu'il y a lieu de se poser à l'avance la question suivante :

- Comment les données personnelles sont-elles stockées (papier, électronique, numérique) ?
- Lieu de conservation des données physiques (physiquement dans des locaux ou externalisés, comme les archives, de manière sécurisées ou accès aisé) ?
- Lieu de stockage des données électroniques : PC, ordinateur local, serveur, dans le "Cloud".

  Notez que le responsable du traitement des données est le responsable et que le cloud service provider est un sous-traitant. Il appartient au responsable de choisir un sous-traitant qui garantit de manière appropriée que les obligations du RGPD sont respectées ;

- Quels supports de données numériques sont utilisés (USB, CD, DVD, ...) ?
- Qui a accès à ces données ?

Dans ce contexte, les thèmes, risques et mesures de sécurité suivants gagnent à être examinés :

- Limitations aux accès à la plateforme informatique (techniques et procédures d'authentification mots de passe, détection des empreintes).
- Cryptage des données stockées (en particulier, en cas d'usage de pc portables)
- Restriction d'accès aux seules données nécessaires pour les activités
- Modification périodique obligatoire du mot de passe
- Sécurisation physique des ordinateurs, en ce compris mise en place d'une politique sur la surveillance des PC dans le cadre des déplacements, travail à la maison, utilisation lors des déplacements
- Intrusions et test de hackings externalisés à des experts externes
- Service level agreement avec des fournisseurs externes, prestataires de services et autres partenaires organisés dans des procédures sur l'usage et la conservation des données personnelles
- Pour les données conservées dans le cloud, vérification que le prestataire de service (de *cloud service provider)* respecte le RGPD et la directive européenne sur les réseaux et la sécurisation des informations (NIS directive) du 6 juillet 2016 - Disponible ici

Si les exemples de textes de l'ICCI s'avèrent insuffisants ou ne peuvent être appliqués pleinement, une série de recommandations de sécurité peuvent également être extraites des polices d'assurances, qui couvrent plus spécifiquement les risques spécifiques en matière de sécurité informatique, *computercrime*, hacking, et autres problématiques de même type.

Désignation et tâches d'un responsable ad hoc du traitement des données personnelles

Le règlement prévoit explicitement [1] dans un certain nombre de circonstances l'obligation de désigner un dénommé « *data protection officer* » ou DPO (en français "délégué à la protection des données "[2]). Les seuils étant principalement liés à l'activité[3], un professionnel dans le secteur économique ne devrait pas, à priori, être soumis à cette obligation.

Retenons, en ordre principal, qu'aucun critère mathématique n'a été avancé quant au fait de savoir si un DPO doit ou non être désigné, mais la question de savoir si l'activité exercée génère ou non un haut risque pour les droits et les libertés des personnes concernées devra être posée.

En principe, ce n'est pas le cas pour les professionnels économiques[4].

Il est cependant possible que les professionnels économiques soient indirectement invités à désigner un DPO. Tel peut par exemple être le cas si un professionnel économique agit comme sous-traitant d'une autre entité, telle qu'une autorité publique ou un organisme public, tenu(e) de désigner un DPO.

Cette observation n'ôte rien au fait que les cabinets peuvent désigner un responsable ad hoc. Les trois Instituts recommandent d'ailleurs qu'une telle désignation soit effective, en ce compris dans les cabinets de plus petite taille.

Cette fonction peut également être externalisée à un tiers. Si tel est le cas, il importe que cet expert externe dispose des compétences appropriées et du temps nécessaire mais aussi qu'il puisse communiquer rapidement et aisément avec le cabinet.

Dans le cadre de la désignation d'un responsable ad hoc, ne perdez pas de vue que la fonction de *data protection officer* est explicitement réglée dans le règlement, ce qui signifie que le dispositif légal, tel que décrit dans ce règlement, est également d'application à la personne désignée comme *data protection officer*.

Ceci n'est pas toujours souhaitable[5]. Le cabinet peut éventuellement choisir un autre titre pour qualifier cette fonction (par exemple, privacy officer, GDPR-officer, ...) de sorte qu'il ne puisse y avoir de malentendus, les devoirs et les droits découlant du règlement n'étant dès lors pas d'application à la personne ad hoc ainsi désignée.

Si un DPO est effectivement désigné, il faut prêter attention à ce qu'un certain nombre de formalités soient respectées, comme :

---

1 Chapitre IV, section 4, articles 37 à 39

2 Dans la directive 95/46/EG, il est fait mention de la dénomination "détaché à la protection des données"

3 L'ancienne directive retenait un seuil de 250 travailleurs comme référence. L'exception pour les PME a disparu dans la nouvelle directive. A la lecture du règlement, il ressort en ordre principal que cette obligation ne s'applique que lorsqu'il est question d'un traitement dont la principale composante est une observation régulière et systématique à grande échelle, ou un traitement à grande échelle de catégories spéciales de données.

4 La non désignation d'un DPO quand c'était effectivement nécessaire peut conduire à une sanction administrative.

5 Le DPO bénéfice par exemple d'une protection contre le renvoi.

- La mention de l'identité et des coordonnées du DPO dans l'information que le responsable du traitement communique à la personne concernée (article 13) ;
- La communication des coordonnées du DPO (article 14) ;
- La mention des coordonnées du DPO dans le registre du responsable du traitement et du sous-traitant. (article 30);
- La communication d'une violation de données à caractère personnel à l'autorité de contrôle (article 33) et à la personne concernée (article 34) ;
- L'intervention du DPO dans l'analyse d'impact relative à la protection des données (article 35)

Quelle que soit la manière et le titre sous lequel la fonction est remplie, il parait évident que la personne désignée doit prendre « sa tâche à cœur » et l'exécuter dans l'esprit du règlement.

La désignation en qualité de DPO intervient aussi dans le cadre d'une obligation règlementaire. Ses taches englobent la délivrance d'informations (ce qui suppose une connaissance du cadre légal), la consultation (par exemple, l'analyse d'impact) et l'exercice d'un contrôle sur la conformité au règlement. En ce qui concerne ce dernier point, il est donc dans une certaine mesure également en charge de la partie *"compliance".*

Le responsable désigné a incontestablement un rôle de sensibilisation et une mission de formation : il doit conscientiser son environnement de travail et rester en alerte par rapport à tout ce qui touche aux données à caractère personnel.

Dans la mesure où cela semble opportun, le responsable ad hoc du traitement des données dresse un rapport (périodique) au plus haut organe de gestion, à l'instar de ce qui est attendu d'autres fonctions analogues comme l'audit interne, la compliance, le risk management, etc.

Procédure de reporting des incidents

Si un incident se produit, le responsable du traitement des données doit en principe le notifier dans un délai de 72 heures après en avoir pris connaissance[6], à l'autorité de contrôle et dans certains cas, aux personnes concernées.

Les règles sont plus souples pour les sous-traitants[7], ce qui peut générer de l'insécurité juridique.

II est par conséquent recommandé de convenir d'un délai concernant le reporting d'éventuels incidents dans les contrats entre le responsable du traitement des données et le sous-traitant.

La procédure de réaction aux incidents peut être concise et simple, et pourrait, par exemple, reprendre les éléments suivants :

- Formation et sensibilisation des collaborateurs en matière d'incidents et procédures applicables.
- Politique avec les sous-traitants en ce qui concerne l'obligation de notification ;
- Directives écrites pour les collaborateurs confrontés à un incident ;

[6] Article 33, premier paragraphe ;
[7] Article 33, deuxième paragraphe ;

- Directives écrites pour le responsable ad hoc confronté à un incident, en ce compris la notification obligatoire aux autorités de contrôle et à la personne concernée ;
- Principes, règles et directives en matière de notification et d'assistance dans le cadre d'une violation des données à caractère personnel ;
- Feuille de route et scénarios envisageables pour limiter le plus possible les conséquences négatives de l'incident ;
- Adresses utiles et données de contact des personnes susceptibles de délivrer une assistance ;
- Modèle d'une notification d'incident.

Procédure en ce qui concerne le recrutement et la formation du personnel

La sensibilisation du personnel en matière de protection des données personnelles n'est certes pas à négliger, mais elle ne doit pas nécessairement s'inscrire dans une périodicité ou faire l'objet d'une formation spécifique, en sorte qu'une procédure spécifique n'est pas opportune.

Il est par contre d'un réel intérêt que cette thématique soit abordée lors du recrutement du personnel, mais aussi dans le cadre du recrutement d'intérimaires.

Il apparaît indiqué d'inclure cette sensibilisation ainsi qu'une courte présentation du cadre légal dans la procédure applicable au recrutement du personnel, au cours de laquelle d'autres procédures du cabinet sont également présentées.

Codes de conduite sectoriels

L'article 40 du RGPD encourage les États membres, les autorités de contrôle, le comité et la Commission à élaborer des codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises.

Les trois Instituts ont l'intention d'établir ensemble un tel code de conduite, étant entendu qu'il n'est pas encore déterminé de quelle façon ce code pourra être intégré au cadre normatif.

Ce document sera soumis, comme le prévoit le règlement, à l'approbation de l'Autorité de protection des données.

Certification

La politique interne de gestion de la qualité peut parfois être imposée par une contrepartie comme des clients ou des fournisseurs qui ne souhaitent travailler qu'avec des entreprises disposant d'une bonne gouvernance, respectant les règles en matière de protection des données à caractère personnel.

Il n'est donc pas exclu que des contreparties ne veuillent plus travailler avec des professionnels si ceux-ci ne sont pas en mesure d'apporter la preuve qu'ils disposent d'une politique et d'un système de gestion adéquats.

Dans une telle circonstance, les reviseurs d'entreprises peuvent faire référence à la norme ISQC-1. Les autres professionnels peuvent recourir à cette norme sur une base volontaire.

Une alternative possible, qui pourrait être satisfaisante pour les contreparties, consiste en l'obtention d'un certificat externe (par exemple, ISO 27001).

Quelques trucs et astuces complémentaires

Si le cabinet ou un certain nombre de ses membres exercent une activité relativement atypique ou ont une clientèle atypique, nous recommandons de lire le règlement en détail.

Le règlement contient en effet, une série de règles plus sévères offrant une protection complémentaire à des personnes (groupes) cibles.

Dans ce cas, il est important de savoir si ces règles plus sévères trouvent ou non à s'appliquer.