Livre Blanc

Règlement Général sur la Protection des Données

L'objectif de ce document est de **fournir la vision de Beijaflore concernant 5 thématiques importantes**, correspondant aux préoccupations premières de la vingtaine de Correspondants Informatiques et Libertés (CIL) que nous avons rencontrés :

1• La cartographie des traitements, étape essentielle pour la mise en conformité
2• L'auditabilité : évaluer son niveau de conformité et être capable de le prouver
3• La construction d'une gouvernance adaptée aux nouveaux enjeux du règlement
4• Les nouveaux droits des individus et comment s'y préparer
5• Le Data Protection Officer : son rôle, son profil, ses objectifs

Beijaflore
CYBER RISK & SECURITY

Février 2017

Le 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, et abrogeant la directive 95/46/CE), inclut de nouvelles dispositions auxquelles les organisations devront se conformer pour le 25 mai 2018. Il introduit notamment de nouveaux droits pour les individus sur leurs données (tels que le droit à l'oubli, le droit à la portabilité ou encore le consentement explicite des individus), des obligations en termes de notification en cas de violation de données à caractère personnel et de nouveaux postes tels que celui de Data Protection Officer.

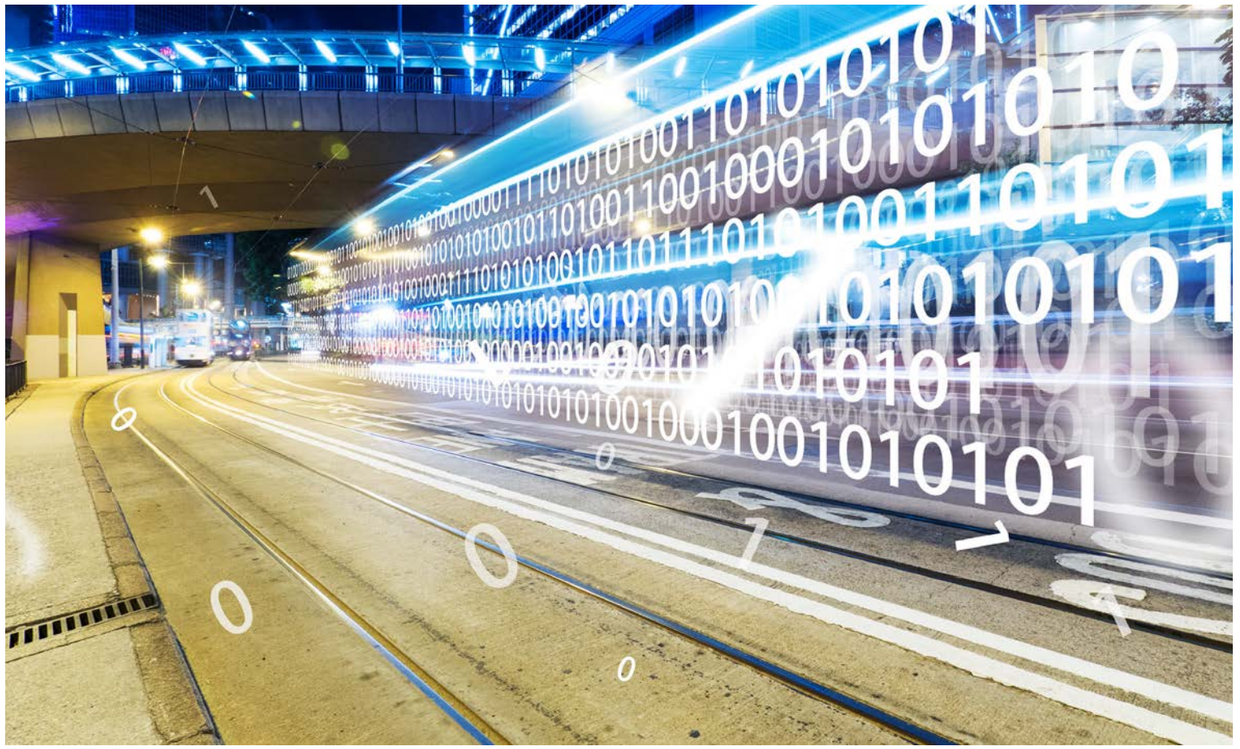
Nous avons interviewé des CILs actuellement en poste dans des entreprises de tailles et de secteurs d'activité divers. Nous avons souhaité percevoir leur vision opérationnelle, connaître leurs préoccupations vis-à-vis de cette nouvelle réglementation, savoir quels sont les chantiers qu'ils ont d'ores et déjà commencés, comment ils ont fixé les priorités et connaître leur perception du rôle de DPO tel que prévu par le règlement.

1. La cartographie des traitements, étape pour la mise en conformité

Afin d'être en conformité avec les dispositions du RGPD, il est essentiel pour les entreprises de **préparer l'échéance de 2018** et de sécuriser le périmètre de leurs données personnelles et de celles de leurs clients. Par ailleurs, la nouvelle réglementation implique la responsabilité des sous-traitants en matière de protection des données à caractère personnel, qui deviennent donc sanctionnables. Il faudra donc évaluer l'ensemble des contrats existants dans lesquels votre entreprise est responsable du traitement des données ou sous-traitant.

Cet objectif nécessite d'**établir la cartographie globale des données à caractère personnel de l'entreprise**, incluant notamment l'inventaire des traitements, les flux de données et les SI supports, la localisation des données, et les responsabilités en matière de protection de ces données.

Cette cartographie pourra être rapprochée d'une éventuelle cartographie des risques de l'entreprise. Dans le cas des entreprises ayant une cartographie complexe et volumineuse, il pourra être utile de passer par des solutions permettant d'automatiser une grande partie des tâches.



Ainsi, il conviendra de créer le registre, conforme aux exigences du règlement, établissant le suivi et la gestion sécurisée qui permettra de protéger les données personnelles. Rappelons que **ce registre devient obligatoire pour les entreprises de plus de 250 salariés** ou plus généralement pour toute entreprise, sous-traitant compris, traitant des données à caractère personnel et qui est communicable à toute autorité qui en ferait la demande.

La cartographie des traitements doit permettre de préparer les **changements structurant de l'entreprise d'un point de vue organisationnel, opérationnel et procédural**. Et ainsi faciliter les demandes de droit exercées par les personnes concernées (accès, rectification, oubli).

En outre, le règlement renforce les exigences liées au consentement des personnes : chaque responsable de traitement devra ainsi être identifié et s'assurer du respect de ces exigences.

Cette tâche est un élément essentiel pour assurer la mise en conformité de l'entreprise. Elle permettra d'avoir la visibilité sur l'existant, sur le niveau de conformité globale de l'entreprise et de ses traitements.

2. L'auditabilité : évaluer son niveau de conformité et être capable de le prouver

Sur les différentes entreprises rencontrées, la plupart ont déjà réalisé une évaluation de la maturité « protection des données » au niveau du Groupe, leur permettant ainsi d'identifier et de prioriser les chantiers de mise en conformité avec le RGPD.

Un des grands challenges du règlement européen consiste en **la capacité pour les entreprises de donner des preuves de leur niveau de conformité** par rapport aux exigences du RGPD, aux autorités de contrôle. Toute exigence du règlement européen se devra ainsi, en plus d'être respectée, d'être auditable par les autorités.

Ceci implique un besoin de restructuration des processus et de l'organisation pour la gestion de l'information, au sein des entreprises, afin de prendre en compte ce critère d'auditabilité.

A titre d'exemple, il devra être possible pour l'entreprise de prouver qu'elle dispose de moyens pour permettre aux propriétaires des données d'exercer leur droit en matière de vie privée (consentement, oubli, rectification, etc.). Ainsi, tout consentement donné par un titulaire de données à caractère personnel devra être formellement tracé. Lors d'un contrôle des autorités (CNIL en France), une preuve formelle du consentement des personnes pourra être exigée par les auditeurs.

Lorsque pour certaines exigences, des contrats, procédures, ou documents de politiques permettront de rendre des comptes à la CNIL, d'autres nécessiteront d'**intégrer dans les systèmes d'information des mesures de traçabilité** permettant d'enregistrer, archiver, et suivre les différentes demandes de droit exprimées par les propriétaires des données personnelles.

L'organisation et les acteurs clés de la protection des données à caractère personnel de l'entreprise devront être capables d'évaluer le niveau de conformité par

rapport au règlement sur l'auditabilité. En particulier, **l'identification et la cartographie des traitements de données à caractère personnel est nécessaire**, pour permettre l'ajout de traçabilité au niveau des systèmes qui portent ces traitements.

Pour finir, il devient important pour l'entreprise de définir une organisation et une procédure de réaction à un contrôle des autorités, qui soit communiquée et régulièrement testée par l'ensemble des parties prenantes. En particulier, une sensibilisation forte doit être effectuée pour les personnels d'accueil, responsables de la sécurité, et responsables des locaux. Ceci permettra de **diminuer les risques** (manque de documentation, communication erronée, comportement inadapté) **liés à un manque de préparation en cas de contrôle**, et d'être en mesure de donner les éléments de preuve demandés sur les points contrôlés.

3. Construction d'une gouvernance adaptée aux nouveaux enjeux du règlement

Une fois l'évaluation du niveau de conformité établi, il est important de profiter du changement de réglementation pour challenger et restructurer la gouvernance dans l'entreprise.

En particulier, toute organisation se doit de formaliser une **politique de protection des données personnelles** incluant les principes de traitement des données personnelles, les garanties relatives à leur sécurisation et à leur confidentialité et les moyens dont disposent les personnes concernées pour contrôler leurs données. Une politique de protection des données personnelles ne doit pas être figée, elle doit être revue régulièrement et notamment lors de changements majeurs (loi et réglementations, cadre d'application…).

La politique de protection des données personnelles doit donc être révisée en matière de vie privée pour inclure les nouvelles dispositions apportées par le RGPD.

Par ailleurs, la gouvernance et méthodologie projet de l'entreprise doit être adaptée. Une des obligations introduite par le règlement européen est la notion de « **privacy by design** » (ou « protection des données dès la conception »): elle impose aux organisations de mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles **dès la conception** des produits et services et par défaut. L'approche doit être proactive et non réactive afin d'anticiper et de prévenir les violations de données avant qu'elles ne surviennent.

Des exemples de mesures à implémenter sont :

- La « minimisation » des données, ou la limitation au strict nécessaire de la quantité de données récupérées et traitées et leur suppression dès qu'elles ne sont plus nécessaires.
- La « pseudonymisation » des données, et le chiffrement en stockage.
- La transparence vis-à-vis des personnes concernées quant au traitement de leurs données.
- La mise en place d'une analyse des risques relatifs à la vie privée pour prendre conscience de son degré d'exposition aux risques et pour identifier les mesures à mettre en place pour y remédier.

délais », si la violation est susceptible d'engendrer un risque élevé pour ses droits et libertés.

La majorité des entreprises rencontrées n'ont pas à ce jour de processus défini concernant ce point.

4. Les nouveaux droits des individus et comment s'y préparer

Le règlement renforce de manière significative le droit des personnes vis-à-vis des traitements opérés par les organisations. Notamment, le droit à la portabilité ou le droit à l'oubli sont deux exemples qui impacteront significativement l'organisation et les SI des entreprises. Le premier doit permettre à une personne de récupérer l'ensemble des données personnelles fournies auprès du responsable de traitement, dans un format structuré, et/ou de les transmettre à un Tiers. Le second permet à la personne de demander au responsable du traitement la suppression de la totalité de ses données (y compris dans les données archivées).

L'ajout de **ces nouveaux droits implique la mise en place de nouveaux processus** au sein de l'organisation : la gestion et le suivi des demandes via la création de workflows, la revue de la politique d'archivage des preuves, ou la redéfinition des périmètres de responsabilité dans les contrats avec les sous-traitants sont quelques-uns des impacts directs de l'ajout de ces droits.

Ces impacts organisationnels touchent l'entreprise à plusieurs niveaux : le département juridique par transposition des clauses dans les contrats avec les sous-traitants, le département des achats par le respect du règlement par les futurs sous-traitants lors des réponses à appels d'offre, les ressources humaines, le département informatique,…

D'autre part, les nouveaux droits impacteront fortement les systèmes d'information de l'entreprise (définition de workflow des traitement des droits des personnes concernées, architecture et politique de sauve-

Le nouveau règlement évoque aussi l'intérêt des PIA (Privacy Impact Assessment), faisant partie intégrante de l'approche « privacy by design », et qui permettent aux organisations de démontrer qu'elles ont étudié les risques associés aux traitements de données personnelles, ont évalué leur impact sur les droits des personnes et ont mis en place des actions appropriées. Toute organisation doit donc de Privacy Impact Assessment. Cette étude d'impact est comparable à une analyse de risque et peut être intégrée dans l'approche de gestion des risques déjà existante dans les organisations.

Il conviendra d'impliquer les métiers lors des analyses pour assurer une bonne compréhension et maitrise des impacts sur les données.

En plus, des solutions techniques implémentées pour détecter les failles de sécurité (DLP, SOC/SIEM, etc.), les organisations devront **mettre en place un processus efficace et une organisation éprouvée** pour répondre à la nouvelle exigence de notification des failles de sécurité : obligation de notifier les autorités en charge de la protection des données en cas de violation de données à caractère personnel, dans les 72h suivant la faille, et la personne concernée dans les « meilleurs

garde et d'archivage, processus d'identification et de suppression des données à caractère personnel dans les différents actifs du SI.

5. Le Data Protection Officer : son rôle, son profil, ses objectifs

Le DPO, devient, avec l'arrivée du RGPD, un élément essentiel et central du dispositif lié à la protection des données. **Il devra aider l'organisation à contrôler la conformité interne au règlement européen**. Il appartient donc aux entreprises de réfléchir aux qualités, à l'expertise, au profil et au rôle du DPO.

Nombre de CILs actuellement en place deviendront DPO. Le niveau d'expertise (et de soutien dont ils auront besoin) ne sont pas strictement définis, mais ils doivent correspondre à la sensibilité, à la complexité et à la quantité de données traitées par une organisation. Le DPO devra donc être soigneusement choisi, en tenant compte du contexte de l'entreprise et de l'importance de la protection des données au sein de l'organisation.

Bien que le règlement ne spécifie pas les qualités professionnelles à prendre en considération lors de la désignation du DPO, il est pertinent qu'il ait une expertise dans les lois et pratiques nationales et européennes en matière de protection des données et une compréhension approfondie du RGPD. Il doit également **être en mesure de comprendre les opérations de traitement effectuées**, les systèmes d'information, ainsi que les besoins en matière de sécurité et de protection des données de l'entreprise.

Si la principale préoccupation du DPO doit être de **s'assurer de la conformité avec le RGPD**, il doit jouer un rôle clé dans la promotion de la culture de la protection des données.
Le RGPD stipule que le DPO « tient dûment compte du risque lié aux opérations de traitement en tenant compte de la nature, de la portée, du contexte et des finalités de la transformation ».

A ce titre, les DPO doivent avoir une approche pragmatique et une connaissance poussée de l'analyse de risques, et concentrer leurs efforts sur les questions qui présentent des niveaux risques plus élevés en matière de protection des données.

Nous avons évoqué précédemment les PIA. Sur ce sujet, le DPO doit être consulté sur toutes les problématiques liées aux DPIA :

- effectuer ou non un DPIA ?
- quelle méthodologie suivre ?
- quelles garanties (et solutions) à appliquer pour atténuer les risques pour les droits des personnes concernées
- l'évaluation de l'impact de la protection des données a-t-elle été correctement effectuée ? Ses conclusions sont-elles conformes au RGPD ?

Le DPO pressenti est donc juriste, expert sécurité, risk manager, communicant, autonome, charismatique, et bien entouré.

Les nouvelles règles apparues avec le RGPD complexifient le rôle de DPO. Afin de l'accompagner et lui permettre d'appréhender pleinement la responsabilité qui est la sienne, il peut être envisageable de faire appel à du coaching.

Allant de la simple rédaction de procédure, de politique, au suivi de projet en passant par le reporting, ou la sensibilisation, le coaching permettra d'élever graduellement et progressivement le niveau de conformité et de sécurité des données personnelles tout en accompagnant la montée en compétence du DPO en place.

Permettant à la fois de disposer d'une expertise pointue, d'une grande souplesse de fonctionnement, cette démarche permet de répondre tant aux besoins des TPE que des grandes structures.

6. Conclusion

Compte tenu des échéances courtes avant la mise en application du règlement, les organisations doivent considérer le RGPD et ses impacts comme un projet à part entière. Le cadrage, la définition des grands chantiers et leur priorisation, et l'établissement du planning jusqu'à 2018 sont les premières étapes à lancer, afin d'**assurer une mise en conformité dans les délais**.

Pour les entreprises que nous avons rencontrées, les travaux se concentreront tout d'abord sur les briques de base : cartographie des traitements, prise en compte de l'auditabilité, construction d'une gouvernance DCP et préparation aux nouveaux droits des personnes, impliquant une réelle transformation aux niveaux organisationnel et SI.

Le suivi régulier et le pilotage efficace de cette transformation permettra d'assurer la prise en compte des exigences du RGPD d'ici la mise en application du règlement.

Paris - Head Office : 11-13 avenue du Recteur Poincaré 75016 PARIS - www.beijaflore.com
Maxime de Jabrun, Head of Cyber Risk & Security mdejabrun410@beijaflore.com