GDPR[1]: votre entreprise est concernée!

(Cet article a été publié dans le n°16 de la revue Classe Export Wallonie, Juin-Juillet 2017, p.47-48)

Philippe LAURENT
Avocat - Marx Van Ranst Vermeersch & Partners
Expert marchés à l'international agréé par l'AWEX

Qu'est-ce que le GDPR ?

Le GDPR est le règlement européen adopté l'année passée et établissant les nouvelles règles en matière de protection des données à caractère personnel. Il entrera en vigueur le **25 mai 2018** : à partir de cette date, toute entreprise traitant des données relatives à des personnes physiques devra être conforme au règlement.

En général, le règlement **renforce les obligations** des acteurs impliqués dans les traitements de données personnelles. Il reprend les principes qui étaient déjà consacrés par l'ancienne directive « vie privée », mais ajoute de nouvelles obligations, crée de nouvelles procédures et prévoit des sanctions beaucoup plus dissuasives.

En effet, dès l'entrée en vigueur du GDPR, les autorités de contrôles auront le pouvoir d'imposer des **sanctions administratives** pouvant aller dans certains cas jusqu'à 20 millions d'euros (ou jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu).

Mon entreprise est-elle concernée ?

La réponse est quasi-systématiquement affirmative : le règlement s'applique entre autres aux traitements informatisés (collecte, enregistrement, organisation, consultation, communication, effacement,…) de données se rapportant à des humains identifiés ou identifiables (pensez aux employés et aux collaborateurs indépendants, aux personnes de contact chez les partenaires et les fournisseurs, aux abonnés, clients, consommateurs, internautes, visiteurs, etc.).

Dès l'instant où une entreprise détermine les moyens ou les finalités d'une de ces opérations, elle agit en tant que **responsable** de traitement et doit, à ce titre, respecter une multitude d'obligations prévues par le règlement. Si une entreprise effectue l'une de ces opérations pour le compte d'un tiers, elle agit en tant que **sous-traitant** et doit également respecter certaines obligations.

En pratique, dès qu'une entreprise recourt à l'informatique dans le cadre de ses activités (communication, gestion du personnel, relations clients, gestion des fournisseurs,…), elle entrera généralement dans le champ d'application du règlement.

---

[1]Règlement (UE) 2016/679 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 (le sigle francophone étant « RGPD » pour « règlement général sur la protection des données »).

Assumer ses responsabilités… et pouvoir le démontrer !

La première grande modification apportée par le règlement est la suppression de l'obligation de déclarer les traitements à la commission de la protection de la vie privée. A la place, le règlement instaure un système général de responsabilité et de bonne gestion. L'entreprise doit, à tout moment, **être en mesure de démontrer sa conformité** au règlement et à ses principes. Elle doit dès lors pouvoir prouver qu'elle a les idées claires sur ses traitements de données et que ceux-ci sont bien conçus, gérés et sécurisés. L'exploitation des données doit être faite dans la loyauté et la transparence vis-à-vis des personnes concernées. Les finalités des traitements doivent être prédéfinies et légitimes. Les traitements, les catégories de données traitées et leur conservation doivent être strictement limités à ce qui est nécessaire à ces finalités. Les données doivent par ailleurs être mises à jour et protégées par des mesures de sécurité appropriées contre les accès non autorisés, la perte ou la destruction inopinée.

Afin d'avoir une bonne vue d'ensemble des traitements qui ont lieu en son sein, de prendre les bonnes décisions et de pouvoir documenter sa bonne gestion, l'entreprise doit identifier les différents traitements relevant de sa responsabilité, identifier les bases légales permettant ces traitements et maintenir pour chacun de ceux-ci un **inventaire** des données, de leurs provenances, de leur usage et accès, de leur partage et des mesures prises pour en assurer la sécurisation. Dans certains cas, le règlement impose la tenue d'un **registre formel des activités** de traitement effectuées sous la responsabilité de l'entreprise (cette obligation s'applique d'office aux entreprises ayant plus de 250 employés).

Sécuriser et limiter les traitements à ce qui est strictement nécessaire

Pour assurer une bonne conformité au règlement, les mesures à prendre sont non seulement techniques (**sécurité informatique**), mais également organisationnelles. Elles doivent dès lors comprendre la mise en œuvre de **politiques appropriées (et documentées)**, qui sont communiquées aux employés et aux collaborateurs de l'entreprise et que ceux-ci doivent respecter. Le règlement suggère également l'application de codes de conduite approuvés ou le recours à des mécanismes de certification. Certaines entreprises recourront fréquemment à des audits d'information et de sécurité.

L'entreprise doit également s'assurer que ses **sous-traitants** respectent les règles et agissent sous son contrôle et conformément à ses instructions. Le règlement renforce également les obligations à cet égard, ce qui implique l'adoption de contrats de sous-traitance adéquats ou la révision des contrats déjà en place.

Prendre en compte le respect de la vie privée dès la conception des systèmes, produits et services

Le règlement instaure deux nouveaux principes : « privacy by design » et « privacy by default ».

La protection des données personnelles doit être prise en compte et mise en œuvre dès la conception des traitements. Des mesures appropriées (telles que la pseudonymisation et la minimisation des données et des traitements) doivent être adoptées et intégrées dans la réalisation de tout projet impliquant l'utilisation de données personnelles. Par exemple, une entreprise produisant des objets

connectés devra les développer en limitant les collectes et les communications de données des utilisateurs à ce qui est strictement nécessaire afin de fournir les fonctionnalités et services proposés.

Par ailleurs, au cas où un produit ou un service offre des possibilités de paramétrage, les choix par défaut devront également être les moins intrusifs par rapport à la vie privée des personnes concernées.

Renforcement du principe de transparence et des droits des personnes concernées

Le règlement renforce les obligations de transparence vis-à-vis des personnes concernées. L'entreprise doit adopter des **déclarations de respect de la vie privée** (ou « déclarations de confidentialité ») adéquates, ou mettre à jour les documents existants en fonction des nouveaux prescrits du GDPR. Si l'entreprise se base sur le **consentement** des personnes concernées pour procéder au traitement de leurs données, l'entreprise doit également adapter aux nouvelles normes ses formulaires de consentement et les techniques utilisées afin de recueillir pareil consentement. Attention également au fait que le GDPR prévoit de nouvelles mesures particulièrement protectrices lorsque les données ont trait à des mineurs de moins de 16 ans.

Le GDPR octroie également de **nouveaux droits aux personnes concernées**. Outre leurs droits d'accès, de rectification et d'opposition qui existaient déjà sous le régime de la directive, le Règlement leur reconnait aussi, dans certains cas, des droits de suppression, d'objection (par exemple en cas de décision individuelle automatisée ou profilage) et de portabilité. L'entreprise doit dès lors adopter des procédures, ou mettre ses procédures à jour, afin de pouvoir adopter un comportement adéquat vis-à-vis des personnes concernées et de réagir à toute requête de manière appropriée.

Obligations complémentaires ou circonstancielles

Outre ces règles générales, les entreprises doivent encore remplir des obligations additionnelles dans certains cas ou dans le cadre de circonstances déterminées.

L'entreprise est obligée de désigner un **délégué à la protection des données** (ou « DPO » pour « data protection officier ») dans trois hypothèses particulières, à savoir lorsque le traitement est effectué par une autorité publique, s'il implique un suivi régulier et systématique à grande échelle des personnes concernées ou s'il porte sur des données sensibles. Le DPO est un conseiller spécialisé chargé, entre autres, de contrôler la légalité des traitements effectués à tous les niveaux de l'organisation et de coopérer avec l'autorité de contrôle.

L'entreprise devra procéder à une **analyse d'impact** des opérations de traitement qu'elle envisage d'effectuer dès que celles-ci sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Par exemple, des activités de profilage donnant lieu à des décisions automatisées ou des traitements à grande échelle de données sensibles déclencheront l'application de cette mesure. Cette analyse d'impact pourra déboucher sur une obligation de consultation préalable de la commission de la protection de la vie privée.

Notons encore que l'entreprise est tenue de **notifier toute violation de données à caractère personnel** (ce qui inclut la perte, l'altération ou la divulgation non autorisée) à la commission de la

protection de la vie privée, lorsque pareil incident engendre des risques pour les personnes concernées. En cas de risque élevé, les personnes concernées devront également être averties.

Aspects internationaux

Tout comme sous le régime de la directive, le GDPR interdit le transfert de données en dehors de l'Union Européenne lorsque les données transférées ne bénéficient pas d'un **niveau de protection adéquat** dans le pays cible. Différents mécanismes (déjà prévus par la Directive) permettent de créer les passerelles juridiques nécessaires.

Le GDPR introduit par ailleurs la notion de «**traitement transfrontalier**», qui vise le traitement d'un responsable ou d'un sous-traitant qui a lieu dans le cadre des activités de plusieurs de ses établissements situés dans différents pays de l'Union ou qui affecte des personnes concernées dans plusieurs Etats membres. Dans ce cas, le règlement organise la coopération entre les différentes autorités de contrôle concernées, des prérogatives et une priorité étant réservées à l'autorité du principal établissement du responsable (autorité de contrôle « chef de file »).

Conclusion : établissez votre liste de tâches dès maintenant !

Il est grandement temps de préparer l'entrée en vigueur du GDPR. Chaque entreprise adoptera sa propre stratégie en fonction, entre autres, de ses activités, des données traitées et de ses spécificités organisationnelles.

Une liste de tâches devrait généralement inclure les points suivants:

1. Préparer un programme de mise en conformité et mettre en place une structure de gouvernance
2. Cartographier les traitements de données, les flux transfrontières et identifier les bases légales applicables
3. Identifier l'autorité de contrôle compétente
4. Vérifier la nécessité de tenir un registre des traitements dans les formes prescrites par le GDPR
5. Vérifier la nécessité de désigner un délégué à la protection des données
6. Effectuer un audit des systèmes d'information et de sécurité
7. Adapter les politiques internes de protection de la vie privée
8. Réviser les contrats conclus avec les sous-traitants et avec les tiers
9. Réviser les déclarations de respect de la vie privée
10. Réviser les formulaires et les techniques utilisées pour obtenir le consentement des personnes concernées
11. Considérer l'adhésion à un code de conduite et l'usage de mécanismes de certification
12. Adopter des procédures pour respecter les droits des personnes concernées et réagir à leurs requêtes
13. Considérer la nécessité de faire une analyse d'impact avant chaque nouveau traitement
14. Intégrer les principes de « privacy by design » et « privacy by default »
15. Préparer un plan de crise au cas où surviendrait une violation de données à caractère personnel