MISE EN ŒUVRE DU RGPD

EXEMPLE PRATIQUE

Le **R**ègleement **G**énéral sur la **P**rotection des **D**onnées (RGPD) entre en vigueur ce 25 mai 2018. Tout le monde en a entendu parler. De très nombreuses entreprises s'y préparent. Mais rares sont ceux qui peuvent prétendre être prêts à 100 %.

Il existe de très nombreuses sources disponibles sur internet relative au RGPD, mais souvent, leur lecture laisse perplexe. Aussi, pour tenter de vous aider à mieux appréhender cette nouvelle législation, nous vous proposons de partir de l'**exemple simple** détaillé ci-dessous. Nos lecteurs avertis ne nous en voudront pas si, dans un souci de simplification et de pragmatisme, nous nous montrons peut-être parfois un peu trop « basics ».

L'asbl Au Plaisir de Lire gère une bibliothèque à Louvain-la-Neuve. Elle possède environ 20.000 ouvrages. Elle a 400 lecteurs réguliers et un « fonds de lecteurs » d'environ 3.000 personnes. Voici quelques années, elle s'est totalement informatisée. Bien plus, elle est proactive : elle connaît les goût de lecture de ses 'clients' en manière telle que, par exemple, lorsqu'elle acquiert de nouveaux livres, elle peut prévenir ses lecteurs susceptibles d'être intéressés par ceux-ci.

Pour l'exercice, nous prenons la place d'un administrateur de l'asbl qui fait rapport au CA.

Mise en œuvre du RGPD – rapport au Conseil d'administration

Préliminaire **En tant qu'asbl sommes-nous concernés par le RGPD ?**

Oui, parce que :

→ toutes les « organisations», ou « entités » sont visées, même les asbl ;

→ nous « traitons » des données, c'est-à-dire que nous les collationnons, les organisons, les modifions, les sauvegardons, etc. ;

→ il s'agit de données concernant les personnes physiques.

Action n° 1 **Faire l'inventaire de nos bases de données**

Notre asbl dispose des bases de données suivantes :

1) liste des membres effectifs et adhérents ;
2) registre du personnel ;
3) liste des administrateurs et des anciens administrateurs ;
4) liste des donateurs ;
5) **liste des lecteurs ;**

À ce stade, nous nous concentrons sur la liste des lecteurs.

Relevons en outre que les anciennes fiches papier et les vieux back-up des données sont également visés par le Règlement (le mieux serait sans doute de s'en débarrasser).

Action n° 2 **Faire la cartographie des traitements actuels des données personnelles que nous effectuons sur la liste des lecteurs**

Voici quelques questions à se poser :

1) De quelles données disposons-nous ?
2) S'agit-il de données particulières[1] ou sensibles ?
3) Quel usage en faisons-nous ?
4) Pourquoi les traitons-nous ?
5) Pendant combien de temps les gardons-nous ?
6) Où sont-elles stockées / sauvegardées ?

Nous devons analyser la situation de façon systématique, pour chaque base de données. Le mieux est de travailler sur base d'un tableau.

Voici une présentation **simplifiée** des **traitements actuels** sur notre base « lecteurs » :

Quelles données traitons-nous ?	S'agit-il de données particulières ?	S'agit-il de données sensibles ?	Pourquoi traitons-nous ces données ?	Jusqu'à quand conservons-nous ces données ?
Cordonnées classiques des lecteurs (nom, adresse, etc.)	Non	Non	Pour identifier le lecteur et conclure le contrat de prêt Pour l'informer de la vie de l'asbl	Aucune limite de temps
Liste des livres empruntés	Non	Oui, le lecteur n'a pas envie que cela soit connu de tous	Pour faire respecter le contrat Pour proposer de nouveaux livres	Pendant 3 ans après le retour du dernier livre emprunté
Respect du contrat (état du livre, retard, amendes, etc.)	Non	Oui, le lecteur n'a pas envie que cela soit connu de tous	Pour récupérer les livres Pour faire payer les amendes de retard	Pendant 1 an après les paiements des amendes

Action n° 3 **Faire le tri dans les données que nous traitons**

En très bref, le RGPD prévoit que **nous devons éviter d'en faire trop**.

Conserver les données d'une personne, c'est potentiellement risquer de porter atteinte à sa vie privée. L'une des finalités fondamentales du Règlement est de **limiter ce risque**.

[1] Selon le RGPD, sont des données particulières, celles relatives à l'origine raciale ou ethnique, les opinions politiques, religieuses ou philosophiques ou encore l'appartenance syndicale, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé (y compris la santé mentale et la prestation des soins de santé) et les données concernant la vie sexuelle ou l'orientation sexuelle. Les données relatives à des infractions et des condamnations pénales appellent également un traitement particulier

Nous ne pouvons donc pas traiter des données inutiles ou non pertinentes, nous ne pouvons pas les conserver trop longtemps, nous devons nous assurer qu'elles sont exactes et à jour, etc.

Ainsi donc, pour chaque donnée que nous conservons, pour chaque traitement que nous effectuons, nous devons nous demander : est-ce que nous n'en faisons pas trop ? Est-ce légitime ?

Par exemple,

- Nous gardons la liste des ouvrages empruntés par chaque lecteur afin connaître ses goûts de lecture et ainsi lui proposer d'autres ouvrages dans le même style. C'est légitime.

- Nous conservons pendant 10 ans la liste des lecteurs qui rendent les ouvrages avec retard. Garder cette liste est légitime, mais la durée de conservation paraît être excessive.

- Un employé facétieux a ajouté dans la base de données une rubrique « sexy » à propos des lectrices/lecteurs. C'est typiquement le genre de données qui n'a pas y s'y trouver !

Action n° 4 **Identifier la base juridique qui nous autorise à traiter les données.**

En bref, les données personnelles peuvent être traitées,

→ soit parce que la personne y a pleinement consenti ;

→ soit parce que nous avons conclu un contrat avec la personne ;

→ soit parce que nous avons un intérêt légitime à traiter ces données ;

→ soit parce qu'il y a une obligation légale à conserver les données.

À ce niveau, notre asbl est confrontée à une grande **difficulté**.

En effet, les personnes reprises dans notre base de données « lecteurs » y figurent parce que, à un moment donné (il y a 10 ans, 2 ans ou 3 semaines), elles nous ont emprunté un livre. En principe, le fondement légal pour le traitement de leurs données est donc l'élaboration, la conclusion et l'exécution d'un **contrat de prêt**.

MAIS,

→ nous en faisons plus avec les données personnelles des lecteurs, que ce qui est simplement justifié par le contrat ;

→ jusqu'à présent, même à l'occasion de la conclusion des contrats de prêt, nous n'avons informé les lecteurs ni sur la finalité du traitement de leurs données, ni sur la durée de celui-ci, ni sur leurs droits (et pour cause puisque le RGPD fait naître de nouveaux droits (droit à l'oubli, droit à la portabilité des données, etc.) dont nous ignorions qu'ils existeraient un jour) ;

→ pour le passé, nous ne sommes absolument pas en mesure de prouver que tous les lecteurs repris dans la base de données nous ont effectivement un jour emprunté un livre.

Par conséquent,

→ **pour l'avenir**, c'est-à-dire s'agissant des prêts d'ouvrages après l'entrée en vigueur du RGPD (25 mai 2018), nous soumettrons une « policy » (voir ci-après) aux lecteurs ;

→ **pour le passé**, c'est-à-dire s'agissant de notre « fonds ~~de commerce~~ de lecteurs », nous devrons régulariser notre base de données en contactant toutes les personnes y figurant afin de solliciter leur accord explicite sur le traitement de leurs données personnelles.

Voici le document que nous leur proposons de leur soumettre :

Mes coordonnées :

Nom :
Prénom :
Adresse :
Date de naissance :
Adresse email :
N° de téléphone :

J'autorise l'asbl Au Plaisir du Lire à traiter mes coordonnées en relation avec les livres que j'emprunte ou lui ai empruntés dans le passé afin de lui permettre : (cochez les cases)

- ☐ *d'établir la traçabilité de ses livres (obligatoire),*
- ☐ *de contrôler le respect des conditions d'emprunt et de faire respecter celles-ci (obligatoire),*
- ☐ *d'établir des analyses statistiques (facultatif),*
- ☐ *de lui permettre d'améliorer ses services (facultatif),*
- ☐ *de me tenir informé de la vie de l'asbl (facultatif),*
- ☐ *de me proposer la location d'autres ouvrages correspondant à mes goûts de lecture (facultatif),*
- ☐ *de communiquer mes coordonnées à des éditeurs afin de lui permettre d'obtenir des remises commerciales sur l'achat de nouveaux livres (facultatif).*

Je marque mon accord pour que ces informations soient conservées jusqu'à deux ans après la restitution de chaque livre.

Ce document sera envoyé par email ou par courrier postal à tous les lecteurs repris dans notre base des données. Il sera également disponible dans nos locaux et téléchargeable sur notre site internet.

Les lecteurs pourront :

→ soit déposer un exemplaire signé dans nos locaux ;

→ soit nous adresser par email le scan d'un exemplaire signé ;

→ soit remplir le document online (utilisation la signature électronique ou consentement en deux étapes : envoi d'un courrier électronique de la personne donnant son consentement puis envoi d'un lien de vérification à celle-ci ou un SMS avec code de vérification -> développement informatique à prévoir).

Action n° 5 **Informer les lecteurs sur leurs droits.**

Nous devons rédiger une « **Policy** » à faire approuver par nos lecteurs et qui sera disponible sur notre site internet.

Attention, il ne s'agit pas de rédiger un texte abscons que personne n'a le temps ou le courage de lire (comme c'est presque toujours le cas pour les conditions générales des entreprises). Le RGPD insiste lourdement sur ce point.

Nous rédigerons donc une Policy **claire, brève et compréhensible** dans laquelle nous expliquerons au lecteur :

- → quelles sont les données que nous traitons ;
- → pourquoi nous les traitons ;
- → quel fondement légal nous autorise à conserver ces données ;
- → que nous traitons ses données afin de lui proposer des livres adaptés à ses goûts de lecture (le Règlement parle d'un « processus de décision automatisée » (profilage)) ;
- → que nous sommes susceptibles de transférer ses données à un autre acteur ; ainsi, nous partageons notre liste de lecteurs avec un éditeur qui, en échange, nous accorde une remise de 35 % sur les livres que nous achetons chez lui ;
- → quels sont ses droits s'agissant de ses données (droit d'accès, droit à l'oubli, droit à la rectification, droit d'opposition au marketing direct, etc.) ;
- → qu'il a la possibilité de déposer plainte auprès de l'autorité de contrôle.

Action n° 6 Désigner un « Délégué à la protection des données » (Data Protection Officer = DPO)

Le « délégué à la protection des données » (DPO) est le chef d'orchestre de la mise en conformité et du suivi du Règlement.

Il est, dans chaque entreprise, le point de contact des autorités de contrôle.

Selon les cas, sa désignation est obligatoire ou seulement recommandée.

Concernant notre asbl, a priori, nous ne devrions pas désigner de DPO parce que :

- → nous ne sommes pas un organisme public ;
- → nous ne traitons pas de données qualifiées de « particulières » par le Règlement ;
- → notre « *activité principale ne* (nous) *amène pas à réaliser un suivi régulier et systématique des personnes à grande échelle* ».

Néanmoins la prudence est de mise !

En effet, nous ne savons pas comment la jurisprudence va évoluer !

Ainsi,

- → nous recevons des subsides publics pour plus de la moitié de notre budget ;
- → nous ne détaillons pas les opinions politiques, religieuses ou philosophiques de nos lecteurs, mais nous traitons les listes des ouvrages qu'ils empruntent : « dis-moi ce que tu lis, je te dirai qui tu es » ;
- → c'est quoi exactement un suivi régulier et systématique à grande échelle ? Où place-t-on le curseur ?

En outre, en cas de problème, vu que la désignation d'un DPO est fortement recommandée, si nous n'en désignons pas, sur base du critère de gestionnaire normalement prudent et raisonnable, ne va-t-on pas nous le reprocher ?

En conclusion, mieux vaut pour nous d'effectivement désigner un DPO.

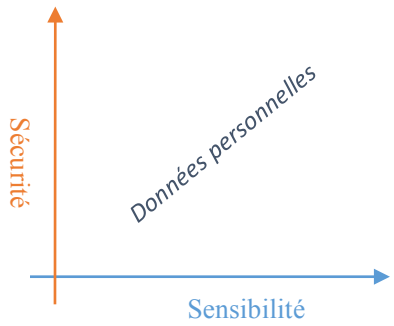
Action n° 7 **Établir une Étude d'impact (Privacy Impact Assessment = PIA) ?**

Même si certaines données que nous traitons sont sensibles en ce sens que nos lecteurs ne souhaiteraient sans doute pas qu'elles se retrouvent sur la place publique ou même, plus simplement, qu'elles soient diffusées à des tiers, il n'en reste pas moins que la nature, l'importance, le contexte et les finalités du traitement de celles-ci ne pourraient conduire à un **risque élevé** pour les droits et libertés des personnes concernées.

Dans cette mesure, nous ne sommes pas tenus évaluer l'impact du traitement sur ces droits et libertés.

Action n° 8 **Vérifier les mesures de sécurité et de confidentialité des données mise en place**

Il va s'agir d'évaluer les risques et mettre en place de système de protection des données, sachant que, plus les données sont sensibles, plus la sécurité devra être renforcée. On va donc s'efforcer de respecter la matrice suivante :



Nous allons donc :

→ Revoir nos pratiques s'agissant des mots de passe d'accès à la base :

- ✓ tous les employés / bénévoles ne doivent pas nécessairement avoir accès à toutes les informations ;
- ✓ il faudra mettre en place une routine pour le remplacement régulier des mots de passe ;
- ✓ prévoir un système de mot de passe élaboré.

→ Vérifier notre abonnement auprès de l'éditeur de logiciel antivirus ;

→ Sécuriser de notre serveur contre le vol physique ;

→ Sensibiliser le personnel et les bénévoles à leurs obligations de confidentialité ;

→ Demander à notre fournisseur informatique de réaliser des tests d'intrusion à intervalles réguliers ;

→ Vérifier que Dropbox –qui nous sert de back-up- est en 'compliance' au niveau du RGPT (ce sera bientôt le cas : https://www.dropbox.com/fr/help/security/general-data-protection-regulation).

Action n° 9 **Organiser des processus internes**

Nous devrons mettre en place, avec le DPO, des procédures internes garantissant la protection des données.

Concrètement, nous devrons :

→ tenir un dossier de conformité de l'asbl au RGPD qui comportera notamment les éléments suivants :

- ✓ Le relevé des traitements de données que nous effectuons (voir le tableau 'cartographie' ci-dessus) ;
- ✓ Les informations relatives à la désignation du DPO, à ses missions et à ses interventions ;
- ✓ La preuve de l'encadrement des transferts en dehors de l'Union européenne (page Dropbox dont nous ne savons pas où sont situés les serveurs) ;
- ✓ Le détail des procédures mises en place pour s'assurer du consentement des lecteurs visées par le traitement de données et de l'exercice de leurs droits ;
- ✓ La description des procédures internes de prévention des risques et de réponse aux violations de la confidentialité des données, yc les informations/formation au personnel.

→ Mettre en place un processus nous permettant de répondre rapidement (le RGPD prévoit des délais assez stricts) pour répondre aux lecteurs qui émettraient une demande portant sur l'exercice d'un de leurs droits. Par exemple :

- ✓ Préciser clairement qui est chargé de répondre ;
- ✓ Rédiger des lettres types.

Conclusion

La mise en conformité de notre asbl au RGPD va représenter un gros travail et va demander des investissements, notamment au niveau informatique. Puisque nous n'avons pas le choix et que tout le monde est logé à la même enseigne, autant en prendre notre parti et profiter de l'occasion pour rationaliser la gestion de nos données.

Cet exemple est assez simple et pourtant, au fil de celui-ci, on constate que plusieurs questions restent ouvertes. L'exemple ne prend pas non plus en compte le fait que presque inévitablement, dans chaque entreprise, une partie au moins du traitement des données est sous-traitée (sauvegarde dans le Cloud, site internet hébergé chez un prestataire, etc.). Or, un volet important du RGPD concerne la relation entre le responsable du traitement des données et le sous-traitant. L'exemple ne prend pas non plus en compte la situation des enfants (un comble pour une bibliothèque !), alors que le Règlement y consacre des dispositions spécifiques.

En fait, chaque situation ou presque est spécifique et nécessite une analyse approfondie ; on ne pourra pas faire un simple copier/coller d'une entreprise à une autre. Du coup, inévitablement, l'implantation du Règlement dans les entreprises prendra un certain temps. Aussi, à l'approche de l'échéance, il est temps d'y mettre un grand coup.

Le 6 février 2018

Me Thierry Corbeel
Avocat spécialiste en droit des sociétés
et en droit commercial
thierry.corbeel@solutio.law