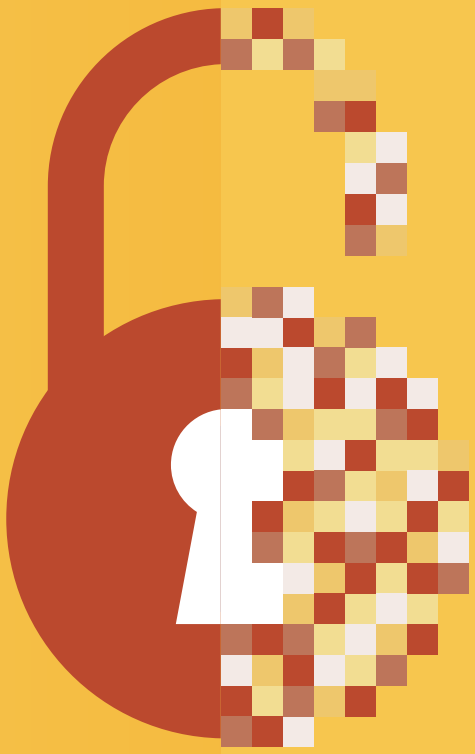
LA PROTECTION DES DONNÉES POUR LES INSTITUTIONS PUBLIQUES

Analyse pratique et retours d'expériences

SOUS LA COORDINATION D'**AXEL BEELEN**

PRÉFACE D'**ALEXANDRA JASPAR**



INTERVIEW DE JEAN-PIERRE HEYMANS

ANTHEMIS

Retour d'expérience : interview de Jean-Pierre Heymans

1. Pouvez-vous en quelques mots vous présenter ? Et présenter les activités de Privacy Praxis ?

J'ai fondé Privacy Praxis en 2012 (https://www.privacypraxis.com). Privacy Praxis est un cabinet de conseil en protection des données et en sécurité de l'information qui offre une palette complète de services visant à aider les entreprises privées ou publiques à protéger leurs ressources, ainsi que les données personnelles qu'elles traitent.

Privacy Praxis s'appuie sur son expertise en matière de protection des données personnelles, avec plus de 10 ans d'expérience, et ce, avant même l'existence du Règlement général sur la protection des données (RGPD).

Depuis l'adoption du règlement, en mai 2016, notre entreprise a été l'un des premiers cabinets de conseil en protection des données à se spécialiser dans la compréhension des enjeux et des impacts que ce règlement peut avoir pour des entreprises de taille moyenne ou de grands groupes ainsi que pour les institutions publiques.

Dans ce contexte, nous avons travaillé avec de nombreuses entreprises et institutions issues de différents secteurs afin de leur permettre d'atteindre leurs objectifs grâce à du conseil personnalisé, en établissant des plans d'action et en leur fournissant des ressources spécialisées.

Je suis aussi expert judiciaire informatique[1]. Désigné par un juge, celui-ci donne son expertise dans le dossier lorsque ce dernier est très technique et complexe d'un point de vue informatique.

2. Nous savons que le RGPD impacte les activités de toutes les institutions publiques (ainsi que des sociétés privées bien sûr). Pouvez-vous expliquer quelles sont, d'après vous, ses conséquences les plus importantes ?

En regard des institutions publiques, le plus difficile est souvent, encore, d'expliquer ce qu'est le RGPD. Le texte est encore mal connu, mal appréhendé. Beaucoup ignorent toujours ce que sont les droits des personnes concernées (ici les citoyens), ce qu'est une violation de données personnelles (alors que

[1] Numéro d'identification : EXP2018610.

ce concept est très large), etc. Il s'agit de processus totalement nouveaux dont la maturité reste assez faible, deux ans après l'entrée en vigueur du RGPD. Il y a encore beaucoup de travail de sensibilisation à réaliser sur ce point.

Dans les administrations, le changement et la transformation induits par le RGPD sont parfois plus difficiles à réaliser que dans les institutions privées. En effet, les administrations publiques sont remplies de procédures souvent figées, une hiérarchie lourde et impactante. Souvent, les initiatives sont paralysées et le personnel n'a pas encore été formé à être « agile ». Il y a donc souvent de réelles difficultés à mettre en place des nouvelles initiatives car ce n'est pas dans l'ADN de l'administration publique.

Un mot encore sur le fait qu'une bonne coordination est difficile à mettre en place car chaque service ou entité dans une administration est plus ou moins autonome. Il est dès lors difficile (par exemple, pour le DPO de l'administration publique) d'avoir une vue transversale sur les activités de son administration. Il est malheureusement encore trop souvent seul dans son travail de mise en conformité de l'administration au RGPD. Celle-ci devrait lui adjoindre davantage de moyens financiers et humains (comme un *project manager* pour implémenter ses recommandations).

Par exemple, lorsqu'une violation de donnée se réalise, beaucoup ne savent pas encore comment réagir et comment faire en sorte que le délai de 72 heures (3 jours !) soit respecté. Le DPO, lorsque cela se réalise, court énormément et ne sait plus quoi faire !

Nous nous devons de reconnaître que, même deux ans après l'entrée en vigueur, le 25 mai 2018, du RGPD, une mise en conformité au RGPD des activités quotidiennes n'est pas encore en place pour beaucoup d'administrations.

3. Les institutions belges, tout doucement, se mettent en ordre par rapport au RGPD. Nous savons qu'elles ont énormément de soucis à prioriser les changements demandés (et ils sont nombreux) par la mise en conformité au Règlement. Quels chantiers sont, selon vous, à privilégier ?

Toute bonne mise en conformité se réalise d'abord par la création du registre des activités de traitement des données personnelles via une cartographie des données traitées par l'organisme concerné. Cela permet d'avoir une vue sur ce que l'administration réalise comme traitements, d'arrêter les collectes de données inutiles et de prendre conscience des tâches à réaliser pour une bonne mise en conformité complète.

La mise en œuvre de ce registre va faire apparaître aussi le fait qu'il lui faudra réaliser souvent des analyses d'impact (des *data protection impact*

assessment – des DPIAs). En effet, il n'est pas rare que les administrations traitent énormément de données dites sensibles (de santé, notre numéro de registre national). Les institutions publiques fonctionnent aussi de plus en plus avec les nouvelles technologies : la géolocalisation (lorsqu'elles mettent à disposition des véhicules à leurs employés ou ouvriers), le cloud, l'intelligence artificielle, etc. L'utilisation de ces nouvelles technologies impose de réaliser un DPIA.

Les administrations (et les sociétés privées aussi d'ailleurs) doivent concrétiser une des nouvelles obligations du RGPD qu'est le *privacy by design*. Autrement dit, elles se doivent de penser à la sécurité informatique autour des données personnelles qu'elles ont collectées et qu'elles vont traiter dès le début de la collecte.

Prenons l'exemple de l'utilisation d'Office 365 de Microsoft au sein d'une institution publique à la suite d'un appel d'offre. Lors de l'utilisation du logiciel, il faudra prévoir un ensemble de mesures de sécurité en amont en vue de protéger les données collectées dès le début. L'APD a d'ailleurs publié un avis dans lequel elle recommande aux institutions publiques de prévoir une même ligne de conduite dans le traitement des informations et leur sécurité au sein d'Office 365.

Rappelons que toutes les administrations publiques, petites ou grandes, se doivent de nommer un délégué à la protection des données (un *data protection officer* – DPO). Elles peuvent bien sûr mutualiser ce poste. On s'aperçoit que toutes les administrations n'en ont pas nommé un. Nous avions lu dans la presse que même de grandes institutions n'en ont pas nommé un directement après le 25 mai 2018 (nous pensons ici à Sciensano qui semble enfin s'être mis en conformité sur ce point-là). Il ne s'agit sûrement pas d'un cas isolé.

Le DPO doit avoir les qualifications nécessaires, une excellente connaissance de la matière et du secteur de son institution, connaître un peu de gestion du risque (*risk management*)… Il se doit aussi d'être proactif et alerte en sécurité informatique et être un très bon communicateur. En effet, il se devra d'être capable de lire une convention juridique, de faire des recommandations, de se faire entendre et d'être capable de répondre aux nombreuses questions internes et externes. N'oublions pas qu'il se doit d'agir de manière indépendante et de ne pas avoir de conflit d'intérêts dans son chef.

Souvent, il est plus utile dans les administrations de nommer un DPO externe que de chercher, dans son personnel, quelqu'un qui voudra bien prendre cette casquette. En effet, le DPO externe permet d'assurer une continuité et une stabilité dans ce poste pour l'administration.

Une analyse (un *mapping*) de la situation devrait être réalisée par le pouvoir politique. Il doit en effet voir si l'ensemble des communes dispose d'un

délégué à la protection des données en ce compris des institutions se trouvant sous la tutelle des communes (comme les écoles par exemple).

4. Une de vos autres spécialités est la sécurité informatique. Ce qu'il y a de bien avec le RGPD, c'est que, dorénavant, le juriste doit dialoguer avec les experts informatiques de son institution. Cette communication n'est pas évidente. Comment évaluez-vous la sécurité informatique des institutions publiques ?

Selon nous, cette sécurité informatique est assez bonne (surtout dans les grandes institution). C'est plus rarement le cas dans les petites institutions ou communes qui ne disposent pas d'une véritable gouvernance en la matière. Une gouvernance est le fait que les pratiques et la sécurité informatique sont documentées, que la sécurité est testée, que les différents systèmes sont mis à jour, que les fonctionnaires sont formés adéquatement. Nous conseillons de réaliser un Welcome Pack pour les nouveaux arrivants. Ce Welcome Pack devrait comprendre une copie des (ou un renvoi vers les) différentes politiques internes de l'institution. Une de ces politiques devrait être relative à la violation des données personnelles (qu'est-ce qu'une violation des données, que faire si elle se produit, qui contacter en interne, etc.).

N'oublions pas que les institutions doivent aussi parfois (et même toujours) respecter d'autres réglementations (comme la directive NIS pour les infrastructures critiques).

5. Nos lecteurs sont avides de retours d'expériences pratiques. Quels sont les défis ou difficultés que rencontrent les institutions publiques dans leur mise en conformité au Règlement ?

Ce travail de mise en conformité des activités au jour le jour en totale conformité avec le RGPD (rappelons que le RGPD n'est pas un but mais un respect au quotidien) permet aux institutions publiques d'être plus transparentes vis-à-vis des citoyens et donc, par ricochet, de leur inspirer confiance.

Cette confiance est fondamentale dans l'action des administrations publiques. Par exemple, en France, l'application StopCovid a été un échec (moins de 2 % de la population française l'a téléchargée) car l'administration française n'a pas été transparente sur les traitements réalisés par l'application. Elle n'a pas su générer la confiance adéquate par rapport à cet outil.

Les administrations se doivent de créer un cercle vertueux de la donnée : de la collecte à son utilisation. La création de cette culture de la confiance et son maintien doit faire partie de sa mission.

En résumé, nous pourrions dire que le mouvement est lancé même si on remarque dans nos activités que certaines institutions sont encore loin du

but. Les priorités et surtout les moyens ne sont pas les mêmes d'une institution publique à l'autre et beaucoup agissent (voire réagissent) encore au cas par cas (de la violation de donnée, de la demande d'un citoyen, etc.).

À ce sujet, nous posons la question de la pertinence de l'exemption par les administrations publiques des amendes administratives prévues par le RGPD. Cette exemption aurait-elle créé un effet de paralysie (un *chilling effect*) dans les administrations publiques ? N'était-ce pas un mauvais signal envoyé par le législateur à ce sujet (qu'importe ce que vous faites, vous n'en subirez de toute façon aucun impact financier) ? Rappelons aussi que l'Autorité de protection des données peut imposer d'autres mesures correctives aux administrations qui contreviendraient au RGPD comme l'arrêt du traitement de données litigieux (mesure autrement plus importante qu'une simple amende si celle-ci aurait dû être peu importante).