MAGAZINE

POUVOIRS LOCAUX

LES NOUVEAUX DÉFIS / SALON DES MANDATAIRES

SUPPLÉMENT DE IPM ADVERTISING

luminus ENVIRONMENT & ENERGY AWARDS 2017

DONNÉES PRIVÉES, quoi de neuf ?

Pour Philippe Laurent, avocat au Barreau de Bruxelles et spécialiste de la protection des données, le RGPD renforce avant tout le cadre de ce qui existait déjà avec la précédente Directive. Il insiste cependant sur trois aspects : un renforcement de la responsabilité des organisations, une augmentation des risques en cas de non respect des règles, ainsi qu'une harmonisation des règles au niveau européen. Petit tour non exhaustif des nouvelles dispositions.

Philippe Laurent

PAR OÙ COMMENCER POUR SE METTRE EN ORDRE ?

Villes, Communes, Asbl, entreprises privées et publiques, petites ou grosses structures…, tout le monde devra se mettre au parfum du RGPD. Quels sont les principaux points d'attention ? Voici quelques conseils de Frédéric Gelissen (Procsima), spécialiste en sécurité.

1

D'abord pas de panique ! Il y avait déjà des lois sur les données privées avant le RGPD. Prenez le temps de bien comprendre celui-ci et d'identifier ce qui est applicable dans le contexte de votre organisation.

2

Parlez-en avec votre avocat et/ou juriste, avec d'autres responsables dans le même cas, participez à des conférences et workshops. Ouvrez-vous et échangez sur le sujet.

3

Ensuite donnez-vous les moyens de retrouver les données privées dans la multitude de documents (électroniques et papier), bases de données, backups, archives, copies…

Harmonisation :
A la différence de la Directive, le Règlement est un outil législatif d'application immédiate. Il ne doit pas être transposé en droit national et les règles sont les mêmes pour tout le monde, même s'il laisse quand même une marge aux Etats pour adapter certains aspects.

Pénalités plus grandes :
Par le passé, la Commission Vie Privée (organe de contrôle en Belgique) n'avait pas le pouvoir de mettre des amendes administratives, et l'amende maximale au pénal était de 600.000€. Le changement le plus marquant du RGPD est de donner aux organismes de contrôle plus de pouvoir et d'augmenter le montant des sanctions auxquelles on s'expose : jusqu'à 20 millions € ou 4% du chiffre d'affaires mondial de l'organisation.

Plus de responsabilité :
Le RGPD prévoit que les responsables des données privées des organisations doivent pouvoir montrer qu'ils ont adopté toutes les mesures de protection et de gestion. Tout doit être documenté afin de pouvoir fournir, en cas de problème, tout document prouvant qu'on a fait ce qu'on devait faire. Dans certains cas, les sociétés doivent créer le poste de DPO (Data Privacy officer), en charge du contrôle et respect de la vie privée.

Analyse des risques :
Dans certains contextes où le risque est élevé pour les droits et libertés des personnes physiques dont on traite les données, l'organisation doit effectuer, avant le traitement des données, une appréciation de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel (Prior Impact Assessment).

Transparence et communication renforcées :
En cas de violation des données personnelles détenues par une organisation, celle-ci devra informer un certain nombre de personnes, comme la Commission Vie Privée, mais aussi toutes les personnes qui pourraient subir des dommages/un impact.

Liliane Fanello

BALISES
Données à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable. Personne physique identifiable : une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

« La protection des données est aussi essentielle qu'un risque d'incendie »

CONSEILS AUX MANDATAIRES PUBLICS

L'Agence nationale luxembourgeoise des informations partagées dans le domaine de la santé a été créée pour répondre au besoin des professionnels de la santé de disposer d'une plateforme leur permettant d'échanger et partager des données électroniques de santé.
Les données de santé étant considérées comme des données à caractère personnel sensibles, dès le début, l'Agence eSanté a mis en place une politique assurant un haut degré de sécurité et un engagement fort de protection de la vie privée, conformément aux dispositions prévues par la Directive Vie Privée.
Cet organisme public a notamment nommé un chargé de la protection des données, fonction charnière qui fait le lien entre l'autorité de contrôle nationale (Commission Nationale pour la Protection des Données), la direction de l'Agence eSanté, dont il dépend directement, le responsable des systèmes de sécurité informatique, ainsi que l'ensemble des collaborateurs. Hervé Barge est le directeur de l'Agence.
« Le fait que les membres de la direction aient conscience de l'importance d'intégrer cette thématique dans la gestion des risques est un facteur-clé de réussite. Ce sont eux qui donnent l'impulsion.
Si je dois donner un conseil aux mandataires publics, ce serait celui de s'approprier le GDPR, d'être transparent et de faire ce qu'on dit qu'on va faire. Ensuite, c'est de commencer par réaliser une analyse des risques, analyse qui n'est malheureusement pas toujours faite. La protection des données doit être intégrée à tous les niveaux de réflexion. Ce ne doit pas être un plan que l'on rédige dans un coin. Tous les acteurs de la chaîne doivent être sensibilisés et impliqués. Cela va de l'ensemble des membres du personnel aux fournisseurs et partenaires externes.
Tout le monde doit être conscient du fait qu'on ne peut pas demander n'importe quelles données aux gens et doit être informé des risques.
Enfin, pour que ça fonctionne, il faut aussi que le chargé de la protection des données intervienne dans une optique d'appui de la direction et de tous les services, et pas comme un Père Fouettard. Il a avant tout une mission pédagogique.
Ne pas prendre en compte cette problématique est prendre un risque stupide. La protection des données à caractère privé doit être traitée de façon aussi normale qu'un risque d'incendie. »

4
Classification des données : il faudra savoir ce que vous détenez et le gérer.

5
Saisissez cette opportunité pour faire de la protection des données by design (c'est-à-dire repenser les procédés/exigences de développement et la fourniture des services).

6
Chaque organisation fait déjà un nombre de choses très bien. Identifiez les bonnes pratiques et comblez les manquements simplement. Pas d'usine à gaz ! Référez-vous aux standards ISO27001, réutilisez ces systèmes de gestion pour couvrir les exigences et évitez de réinventer la roue, de manière à aller vers un système unique/intégré et simple.

7
Désignez un responsable de cette problématique.

8
Enfin, n'oubliez vos fournisseurs, car ils font partie de la chaîne. N'hésitez pas à revoir vos contrats et à les renégocier si nécessaire. Il en va de votre propre responsabilité.