A N D S I

Association Nationale des Dirigeants en Sciences de l'Information
www.andsi.fr

RGPD à J+18 mois : Où en sont les entreprises : démarche, actions significatives de la CNIL sur 2019 et enjeux 2020.

Compte rendu rédigé par ANDSI – Pierre Delort

En bref…

Didier PAWLAK présentera les actions conduites par l'entreprise Pénélope afin de se mettre en conformité avec le Règlement Général sur la Protection des Données avant d'effectuer un bilan de la mise en œuvre après 18 mois. Cécile VERNUDACHI interviendra ensuite afin de dresser le bilan 2018 de la CNIL à travers les sanctions prononcées. Elle exposera également les enjeux de l'action de la CNIL pour 2020. Enfin, un cas concret relatif à la manière de gérer un contrôle de la CNIL sera détaillé.

La démarche RGPD chez Pénélope (agence d'hôtes et hôtesse d'accueil)

Didier PAWLAK indique que plusieurs actions ont été menées afin de se mettre en conformité avec le RGPD. La première a consisté à nommer un DPO Groupe. Ensuite, un courrier a été envoyé à l'ensemble des 3 000 clients afin de leur expliquer les objectifs de ce nouveau Règlement. Un courrier revêtant la forme d'une notice d'information et d'un questionnaire a également été envoyé aux fournisseurs. En outre, l'ensemble des contrats clients a été modifié tandis qu'une mise à jour des mentions légales des sites Internet a été réalisée.

Par ailleurs, divers documents ont été rédigés à propos de l'engagement de confidentialité des salariés, de la portabilité des données, etc.

Au niveau technique, il importe de signaler le déploiement d'une procédure de réponse aux incidents de sécurité ainsi qu'une revue de la politique générale des données personnelles ou de la politique générale de sécurité des SI. Le PRA a également été mis à jour.

Int : Y a-t-il un lien entre le RGPD et le PRA ?
Didier PAWLAK : Non. Nous avons profité du RGPD pour mettre à jour un certain nombre d'éléments.

Bilan chez Pénélope : 18 mois après

Tout d'abord, le DPO et le DSI sont seuls à gérer le dossier RGPD. De plus et suite aux 3 000 courriers envoyés aux clients, 74 dossiers (dont 10 nouveaux clients) ont été traités. Ces dossiers se répartissent en quatre catégories, à savoir une simple information réciproque ; une simple acceptation réciproque ; les dossiers pouvant être gérés par le DPO/DSI ; les dossiers nécessitant l'intervention de Cécile Vernudachi (une dizaine).

Int : Ces divers éléments renvoient à des points de forme. Cette contrainte réglementaire du RGPD n'a rien apporté.
Cécile VERNUDACHI : Tout dépend des organisations. Cette nouvelle disposition a tout de même permis à certaines organisations de progresser en matière de sécurité.
Int : Le fait pour vos collaborateurs de pouvoir accéder à 3 000 annuaires clients représente un risque.
DP : Leurs contrats de travail ont été modifiés.
Int : Le déploiement du RGPD a conduit chacun à se protéger sans apporter de réel bénéfice au final.

De surcroît, deux salariés ont demandé à ne plus être sollicités par mail dans le cadre de la mise en place d'une application de covoiturage.

Int : S'agissait-il de leur mail personnel ou professionnel ?
DP : Ces salariés ont refusé d'être contactés sur leur mail personnel.

Bilan 2018 de la CNIL

Cécile VERNUDACHI relève, concernant le bilan de la RGPD, des disparités importantes entre les acteurs. Aucune avancée n'a véritablement été observée dans le secteur public ou dans les TPE. La situation est différente au sein des grands groupes. Les données 2018 de la CNIL laissent apparaître une croissance du nombre de plaintes de plus de 30 % dont 36 % dans le secteur Internet et Télécom ou 21 % dans secteur commercial. Dans domaine des RH, les plaintes se rapportent notamment à la présence de caméras de surveillance. Le secteur de la santé est peu concerné. Par ailleurs, 1 170 notifications de violations de données ont été reçues en 2018.

Int : Ces chiffres ne sont pas significatifs, en comparaison avec la situation en Allemagne.
CV : La France n'est pas vraiment acculturée à cette thématique, même si la CNIL existe depuis 40 ans.

En outre, 310 contrôles ont été diligentés en 2018, en augmentation :

- 57 % : actions de la CNIL ;
- 16 % : programme annuel décidé par la CNIL ;
- 22 % : instruction de plaintes ou de signalements ;
- 5 % : plaintes.

Par ailleurs, 49 mises en demeure ont été prononcées (13 rendues publiques) ainsi que 11 sanctions (10 pécuniaires). Une mise en demeure peut pénaliser l'image d'une entreprise et conduire à une diminution du nombre de clients. Les sanctions faisant suite au non-respect du RGPD peuvent être civiles ou pénales. Les sanctions financières peuvent notamment atteindre jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial.

Bilan 2019 des actions et sanctions CNIL

Les actions et sanctions prononcées en 2019 concernent par exemple Google (50 000 000 euros), Sergic (400 000 euros), Active Assurances (180 000 euros) ou Futura Internationale (500 000 euros). Récemment, la CNIL a mis en demeure le Ministère de l'Intérieur pour violation de la réglementation concernant les radars tronçons en raison d'une durée de conservation trop importante des plaques minéralogiques.

Que retenir des actions de la CNIL ?

Tous les acteurs et secteurs d'activité sont concernés. Pour autant, l'occurrence demeure faible avec un personnel composé de 200 personnes.

Int : Le RGPD a-t-il augmenté le pouvoir de la CNIL ?
CV : La loi permet à la CNIL de sanctionner davantage. La CNIL dispose aussi d'un rôle pédagogique et de formateur.

Enjeux et perspectives de l'action de la CNIL pour 2020

Les principaux enjeux se déclinent comme suit :

- rôle proactif dans les instances européennes, géopolitique internationale de la donnée ;
- éthique et régulation du numérique (IA, biométrie) ;
- domaines de contrôle : coresponsabilités/sous-traitance secteur de la publicité (publicité ciblée).

Int : Nous ne pourrons plus charger un sous-traitant afin de s'exonérer de ses responsabilités.
CV : Un sous-traitant pourra être condamné par la CNIL s'il est prouvé qu'il a manqué à ses obligations contractuelles ou légales en ne se conformant pas aux instructions d'une entreprise cliente.
Int : D'où l'intérêt de faire figurer cet aspect dans les contrats.
CV : Le plafond de responsabilités correspond à un réel enjeu. La CNIL va essayer de déterminer les responsabilités afin d'identifier le manquement grâce à des expertises. A ce jour, nous ne disposons pas de jurisprudence en la matière. Nous ignorons la position des autorités de contrôle. Il sera délicat pour une telle autorité de déresponsabiliser le responsable de traitement.

Il convient de relever l'existence de quatre types de contrôles : le contrôle en ligne, le contrôle documentaire, le contrôle par convocation, le contrôle inopiné. Une entreprise peut refuser un contrôle si les inspecteurs de la CNIL ne disposent pas d'une autorisation du juge. Normalement, le motif du contrôle doit être précisé.

En cas de contrôle, il convient de prévenir immédiatement le référent interne conformité de l'arrivée des inspecteurs, de vérifier la carte professionnelle et l'ordre de mission, de lire attentivement l'ordre de mission et le document relatif au droit d'opposition et le signer. Il apparaît utile d'affecter une ressource derrière chaque contrôleur afin de rédiger un journal, ce qui facilitera la rédaction du procès-verbal. Le DPO peut être assisté de son équipe et de son avocat. Dans l'hypothèse où des données sensibles sont en jeu (données médicales), il convient de demander la présence d'un médecin parmi les contrôleurs. Enfin, le contrôle sur place se termine par un procès-verbal de constatation, document pouvant donner lieu à la formulation de réserves.

Débat

Int : La durée d'un contrôle s'établit-elle à une journée ?
CV : Je ne relève pas de limite. Ce type d'intrusion de la part de la CNIL s'avère plutôt anxiogène.

Int : Les enjeux sont-ils identiques au niveau européen ?
CV : Oui. Toutefois, les autorités sont assez dynamiques en Angleterre ou en Allemagne.

Int : Les contrôles s'avèrent beaucoup plus conséquents en Angleterre. Une harmonisation est-elle envisageable en la matière et à quel horizon ?
CV : Il est n'est pas aisé de répondre à cette interrogation.

Int : En Angleterre, ce RGPD permettra-t-il à des avocats de gagner de l'argent ?
CV : Je ne le pense pas. Par ailleurs, il semblerait intéressant de se focaliser sur l'harmonisation de la donnée. Je relève un véritable enjeu démocratique, en lien avec la surveillance de masse.

Int : Le bandeau pour les *cookies* constitue-t-il une obligation ?
CV : Tout à fait. Il n'est pas possible de préjuger du consentement de la personne. De plus et sur 310 contrôles, 110 ont été effectués en ligne.

Int : Ce bandeau pour les *cookies* n'est pas évident à déployer.
Int : Certains sites hôteliers déposent jusqu'à 70 *cookies*. Certains sites tracent les visiteurs de manière conséquente, ce qui peut être dangereux à terme. Google a tout de même acquis son pouvoir grâce aux informations qui lui ont été communiquées gratuitement.

Présentation des orateurs

Cécile Vernudachi a été responsable juridique et Secrétaire Général de Quintess avant de reprendre son métier d'avocat en droit des affaires, maintenant associée IT/protection IT chez DMS Avocats, cvernudachi@dms-avocats.fr .

Didier Pawlak, DSI de Quintess puis maintenant de Pénèlope, a récemment été distingué comme le 9eme DSI le plus influent sur Twitter. https://www.brandwatch.com/fr/blog/top-30-dsi-francais/