RGPD : les 6 étapes obligatoires pour la mise en conformité

Pour se mettre en conformité avec le règlement RGPD (Règlement Général sur la Protection de Données personnelles), il est opportun de commencer par examiner les recommandations de l'autorité de tutelle, la CNIL. Elle détient, plus que jamais, le pouvoir de sanctionner et d'infliger de lourdes amendes (cf. volet1).

Le principe d'accountability ou responsabilité étendue

Néanmoins, Il faut noter que de nombreuses formalités auprès de la CNIL disparaissent. En contrepartie, la « responsabilité des organismes » est renforcée. C'est le principe anglo-saxon d'accountability ou responsabilité étendue, qui est souligné par la nomination d'un délégué, le DPO (Lire notre article) et par la nécessaire information et sensibilisation de tous dans l'entreprise.

« Fini les déclarations », comme nous le résume Olivier Itéanu, avocat spécialisé, « mais je dois être conforme et détenir les documents justificatifs ». Et le maintien en condition opérationnel et sécurisé des applications constitue une exigence nouvelle.

Les 6 étapes recommandées par la CNIL

La CNIL souligne que « les entreprises devront assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité ».

Voici, en résumé, les 6 étapes recommandées par la haute autorité :

1 -Désigner un « pilote » pour la gouvernance des données personnelles. C'est un « véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne » : le DPO, délégué à la protection des données est le prolongement du « correspondant informatique et libertés », chargé d'organiser les actions à mener.

2 – Cartographier les traitements de données personnelles. Il s'agit de « mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez ». Il faut commencer par « recenser de façon précise les traitements de données personnelles. Il est recommandé de constituer un « registre des traitements ».

Commentaire d'Alain Bensoussan, avocat spécialisé : « La cartographie exigée n'est pas réellement « techno » ; elle doit être légale ; elle concerne les traitements – moyens et finalités – et non les applications ».

3 – Prioriser les étapes à mener : sur la base du « registre de traitements », il faut identifier les actions à mener pour être conforme aux obligations actuelles et à venir. Cette priorisation s'établit

« au regard des risques que font peser les traitements sur les droits et les libertés des personnes concernées ».

4- Gérer les risques et lancer une étude d'impact : pour chacun des traitements de données personnelles « identifiés comme susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées », il faut mener une analyse d'impact sur la protection des données (PIA).

5 – Organiser les procédures internes : « Pour assurer un haut niveau de protection des données personnelles en permanence », il faut mettre en place « des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accés, modification des données collectées, changement de prestataire) ».

6- Documenter la conformité : pour prouver la conformité au règlement, il faut « constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu ».

Continuez Page 2 : Etablir votre feuille de route

Une feuille de route à établir

Au 25 mai, il faut donc être en « posture de mise en conformité », explique Arnaud de Chambourcy, « practise manager' »au sein de la société de services Umanis. «Vous avez commencé un état des lieux et établi les grandes actions de remédiation, qui devront figurer sur une feuille de route de mesures menant à la conformité ». Selon lui, il y a trois dimensions à prendre en compte :

1- l'aspect juridique, celui des contrats avec les fournisseurs (responsabilité en cascade), les collaborateurs, les processus.

2 – l'aspect organisationnel, à savoir la gouvernance des données, la nécessité, si l'organisation compte plus de 250 personnes, de créer le poste de DPO (Délégué à la protection des données, nouvelle dénomination du 'Correspondant informatique' en France). A défaut, il est possible de déléguer cette mission à un prestataire externe.

3 – la dimension informatique : « C'est la gouvernance au sens de se donner les moyens techniques de respecter le droit des personnes, tel que porté par le règlement : droit d'accès, droit de rectification, droit à l'effacement (ou 'droit à l'oubli') ».

A noter que la mise en œuvre de la « purge » des fichiers implique qu'on tienne un registre des traitements : « Le registre décrit la façon dont on expose les données des personnes. Tout doit y être consigné, comme par exemple la date d'échéance des contrats. Toute les actions à mener y sont déclinées en chantiers », précise Arnaud de Chambourcy.

Minimisation et engagement sur la résilience

Des exigences nouvelles se sont ajoutées, qui impliquent la résilience des plateformes utilisées, leur sécurisation permanente face aux risques de fuites, de vol, de 'hacking', de corruption ou de modification.

Les mesures prises doivent conduire à un principe-clé, celui de la minimisation des risques.
L' organisation fait la preuve qu'elle a réellement mis en œuvre des mesures préventives de protection.

En résumé, des mesures concrètes et effectives doivent être prises pour se mettre en conformité au 25 mai 2018. Tout nouveau traitement devra être conforme. Les applications et fichiers déjà existants donnent lieu à des chantiers en cours, qu'il faudra également détailler.

Lisez aussi :

RGPD : Les 8 priorités pour être prêt le 25 mai 2018

RGPD : après le 25 mai, quelles actions à moyen et long terme

Credit Photo : SmedersInternet on Visualhunt.com/ CC BY