RGPD, mode d'emploi de l'analyse d'impact

DELPHINE IWEINS | Le 17/01 à 06:00

Pour aider les entreprises, la CNIL a aussi établi, le 6 novembre dernier, une liste des types d'opérations de traitement pour lesquelles une analyse d'impact est requise. - Shutterstock

Tendance | Sanctionné par la CNIL d'une amende de 250.000 euros pour avoir insuffisamment protégé les données de ses clients B & You, l'opérateur Bouygues Telecom aurait pu éviter cette faille de sécurité grâce notamment à une analyse d'impact.

Issue du **règlement européen de protection des données personnelles** (RGPD), l'analyse d'impact aide à construire des traitements de données respectueux de la vie privée. Elle se réalise en deux temps. Il faut d'abord s'assurer que le traitement est bien conforme au RGPD. L'étape suivante est d'évaluer le risque de ce traitement pour les droits et les libertés des personnes. « *Il faut ensuite identifier les mesures à mettre en oeuvre pour réduire les risques du traitement* », complète Anne Renard, avocate, directrice du département conformité et certification du cabinet Lexing Alain Bensoussan Avocats.

Identifier correctement les traitements concernés

En pratique, la première difficulté est de distinguer les traitements concernés par les analyses d'impacts. A priori, il s'agit de tous ceux présentant des risques pour les droits et les libertés des personnes concernées. Le G9, groupe des CNIL européennes, a défini neuf critères pour aider à cette identification. Il s'agit notamment des données hautement personnelles et/ou concernant des personnes vulnérables - **le salarié est considéré comme tel** -, l'utilisation de solutions technologiques comme les algorithmes et l'intelligence artificielle. Si le traitement concerné remplit au moins deux de ces neuf critères, l'analyse d'impact est alors nécessaire.Pour aider les entreprises, la CNIL a aussi établi, le 6 novembre dernier, une liste des types d'opérations de traitement pour lesquelles une analyse d'impact est requise. « *La CNIL a une vraie démarche d'accompagnement des entreprises dans la mise en conformité* », estime celle qui est aussi recommandée comme DPO pour la profession d'avocat par le Conseil national des barreaux.

S'équiper d'outils spécifiques

Une fois le traitement identifié, il faut mettre en oeuvre cette analyse d'impact. Pour se faire, les cartographies de risques établies pour d'autres dispositifs comme celui de la lutte contre la corruption peuvent être utilisées. Depuis le 6 décembre, la CNIL met aussi à disposition un outil d'analyse d'impact, afin de créer des modèles. « *Cette fonctionnalité a été conçue pour permettre la création de bases d'analyse à la fois adaptées au secteur d'activité et réutilisables pour d'autres analyses d'impact* », précise l'autorité administrative indépendante. Chez Orano, l'analyse d'impact est réalisée automatiquement pour tous les nouveaux traitements. « *Nous devons en interne vérifier les traitements et protéger l'être humain. Le RGPD nous rappelle les droits et les libertés des personnes* », explique Hélène Legras, DPO d'Orano. Pour être en conformité avec le RGPD, un fichier Excel surnommé « What you need for your securitie », auquel toutes les parties prenantes à un traitement sont associées, a été créé. Il permet de détecter le niveau le niveau de protection et les risques du traitement.

Un travail d'équipe

Un travail d'équipe est primordial pour s'assurer du respect de la vie privée par les traitements. Une difficulté non négligeable pour les entreprises. Les plus grandes d'entre elles ont **nommé un DPO comme l'exige le règlement européen** , mais ce n'est pas suffisant. Celui-ci doit avoir son réseau, travailler en équipe. « *Un bon DPO doit communiquer et faire preuve de pédagogie* », confirme Hélène Legras. Le responsable métier qui met en place le traitement l'explique au DPO et le directeur des systèmes d'information intervient pour mettre en oeuvre l'analyse d'impact. « *Les sous-traitants des outils en cause ont l'obligation d'aider les entreprises à identifier les risques et d'apporter leurs connaissances précises* », ajoute Anne Renard.

https://business.lesechos.fr/directions-juridiques/droit-des-affaires/contentieux/0600458034763-rgpd-mode-d-emploi-de-l-analyse-d-impact-326316.php