HUSSARD
data privacy compliance

Le rôle essentiel du DPO dans la gestion des violations de données

Gauthier Broze, CEO/Founder

Les nouveaux défis technologiques

Les **innovations technologiques**, particulièrement l'intelligence artificielle (IA) ouvrent d'immenses perspectives pour les entreprises.

Malheureusement celles-ci s'accompagnent de **nouveaux risques pour la confidentialité et la sécurité des données personnelles** et en cas de violation, pour la **réputation** de l'entreprise.

Quel est le rôle du DPO dans l'anticipation des risques et
la gestion des contentieux devant l'Autorité de Protection des Données (APD) ?

La conformité au RGPD est-elle suffisante pour se mettre à l'abri ?

Illustration à partir d'un cas réel.

Et soudain…une violation de données

- Le laboratoire Adelphia découvre sur internet une **base de données** contenant des **résultats d'analyses sanguines**
- **Divulgation de données personnelles de patients**: nom, prénom et adresse postale, numéro de téléphone portable, adresse e-mail ainsi que le groupe sanguin et le numéro de sécurité sociale
- Des **informations médicales ultrasensibles** figurent aussi dans les données publiées, notamment celles relatives aux HIV, cancers, maladies génétiques, grossesses, traitements médicamenteux suivis par le patient, ou encore des données génétiques
- La source est identifiée: logiciel commercialisé par la société Minotora, sous-traitante d'Adelphia et spécialisée dans **l'édition de logiciels pour laboratoires**

Suivie d'une réaction en chaîne

- Le DPO d'Adelphia **notifie** l'incident à l'Autorité de Protection des Données (APD) dans les 72 heures et organise une campagne de **communication** auprès des personnes concernées.
- Les **patients sont furieux** et interpellent le laboratoire Adelphia. Le DPO d'Adelphia renvoie la responsabilité sur son sous-traitant Minotora qui n'a pas de DPO. Plusieurs dizaines de patients portent **plainte** contre le laboratoire auprès de l'APD tandis que le laboratoire, via son DPO, porte plainte contre Minotora.
- Adelphia et Minotora portent plainte contre le cyberdéliquant (APD et de la section cybercriminelle de la **police judiciaire**). Le laboratoire Adelphia attaque Minotora en responsabilité, avec demande de dommages et intérêts, devant les **instances judiciaires** tandis que Minotora introduit une demande reconventionnelle contre Adelphia estimant que cette dernière aurait porté atteinte à sa réputation lors de la communication de la violation aux personnes concernées.

Une violation de données éclabousse tout un écosystème

Face à l'APD: documenter la conformité

- Suite aux plaintes, l'APD prend contact avec le DPO d'Adelphia tandis que Minotora est interpellée sur l'absence de DPO
- Transmission d'une copie du **registre**
  - Date création du registre => quid depuis 25 mai 2018?
  - Date de la dernière mise à jour? Fréquences des mises à jour?
  - Politique interne pour la tenue et la mise à jour du registre?
- Transmission du **registre des violations de données** (historique détaillé)
- Quid **formation** du personnel? => copie des supports pédagogiques
- Quid des **mesures techniques et organisationnelles**? Analyse d'impact?
- Présence de clauses de **confidentialité**? Politique générale?
- **Eléments factuels** détaillés de la violation de données

Votre DPO peut-il gérer?

- Si DPO nommé, quid de son profil ? Selon art. 37, « *désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39.* »
- Si le DPO est nommé en interne (ex. CFO/CTO) => il fait partie intégrante de la gouvernance du responsable de traitement + si employé, lien de subordination => conflit d'intérêt + quid « *connaissances spécialisées du droit et des pratiques* »?
- Si le DPO est un avocat => obligation déontologique de distinguer les deux statuts et de ne pas représenter son client ni devant l'APD, ni devant les tribunaux => le dossier doit changer de main
- **Conseil**: Partir du principe qu'il faut un DPO sauf si … => externaliser le DPO => « juriste » 100% dédié (+ expérience technique ou contentieuse?)

A-t-il préparé le terrain en amont? (art.39)

- **Informer** et **conseiller** sur les obligations du RGPD
- **Contrôler** le respect du RGPD:
  - Tenue du registre (art.30 RGPD)
  - Répartition des responsabilités pour chaque opération de traitement (RACI)
  - Sensibilisation et formation du management et du personnel
  - Audits
- Dispenser des **conseils** sur l'**étude d'impact** et son exécution
- Être un point de **contact** pour l'APD et **coopérer** avec celle-ci

=> Obligation pour le DPO de tenir compte du **risque associé aux opérations de traitement** (nature, portée du contexte et des finalités du traitement)

Vous aider à gérer la crise et à en sortir

- Contentieux devant des **instances professionnelles** (ex. Conseil de l'Ordre des Médecins)
- Contentieux pénal: **police cybercriminelle**, parquet, etc. => le pénal tient le civil en l'état
- Contentieux administratif devant l'**Autorité de Protection des Données (APD)** ou d'autres autorités de contrôle UE si violation de portée internationale
- Contentieux **judiciaire**: attente de l'issue du contentieux administratif puis dommages et intérêts => arriéré judiciaire?
- Fenêtre d'**opportunité**: négociation/médiation/conciliation

Conclusion: le DPO est un acteur majeur de la confiance digitale

- Le DPO accompagne son client sur le chemin de la **conformité au RGPD**
- En amont, il joue un rôle essentiel dans la prévention des violations de données => **analyse de risque**
- Quand le risque se réalise, il participe directement à la **gestion de la crise**: obligations de notification et de communication => protège la **réputation**
- Il doit toujours être en mesure de **documenter** le niveau de conformité de son client auprès de l'APD (« accountability »)
- Il développe des **arguments** en faveur de son client durant les procédures contentieuses et négocie les sorties de crise
- Il fait de chaque crise une **opportunité** de se transformer

HUSSARD
data privacy compliance

Merci de votre attention

Contact: gab@hussard.com – Site: www.hussard.com