anaxia conseil
personal data protection

FORMATION (présentiel)

Violations de données
Pour ne pas subir

Version du 3 août 2022

Présentation

Un responsable de traitement ne peut plus détourner les yeux en cas d'incident de sécurité impactant les données personnelles qu'il traite et doit – dans certaines circonstances – notifier la violation de données à la CNIL, voire la communiquer aux « victimes ».

Il s'agit pour les entreprises d'un véritable changement de paradigme et de multiples questions se posent :

- Quelles mesures prendre en amont pour éviter d'avoir à notifier une violation de données ?
- Comment détecter tous les incidents susceptibles d'être qualifiés de « violation » ? Et qui réalise cette qualification ?
- À partir de quand démarrent les « 72 heures » attendues par la CNIL pour réaliser la notification auprès d'elle ?
- Au final, qui prend la décision de notifier ?
- Comment décider s'il faut en plus communiquer la violation aux personnes concernées ? Et que leur dire ? Faut-il leur donner des précisions sur l'incident lui-même ? Faut-il s'excuser ? Et qui signe le courrier ?
- Faut-il craindre un contrôle de la CNIL à la suite d'une notification, voire une action de groupe de la part des « victimes » ?
- Que faut-il imposer aux sous-traitants à ce sujet ? Le modèle de clause contractuelle proposé par l'autorité de contrôle est-il suffisant ? Combien de temps maximum doit-on laisser à ses sous-traitants pour nous signaler un incident ?
- Quel lien entre violation de données, analyse d'impact et *Privacy by Design* ?
- Comment tirer des enseignements utiles des violations pour en faire un levier de progrès ?
- Quel rôle doit jouer le DPO : simple spectateur, pilote et leader, voire réalisateur ?

Autant de questions cruciales auxquelles Bruno RASLE, expert reconnu de longue date et DPO mutualisé de l'une des branches de la Sécurité sociale (plus d'une centaine de violations de données à son actif), répond lors d'une journée durant laquelle les aspects opérationnels sont privilégiés.

À l'issue d'une session très interactive, avec l'intense participation des apprenants (études et travaux sur des cas concrets – dont certains de ceux signalés au préalable par les participants –, mises en situation, travail en groupes, réponses aux questions, …), les participants repartent forts de toutes les connaissances leur permettant de maîtriser le sujet. De plus, l'intervenant partage des documents opérationnels qu'il a forgé dans le cadre de sa pratique professionnelle (exemples concrets, modèle de procédure, fiche « Réflexe », éléments de sensibilisation des parties prenantes, courriers types, …).

« *La question n'est pas « Allons-nous connaître des violations de données ? » mais « Quand allons-nous connaître des violations de données et devoir les notifier à la CNIL ? ». Je recommande à mes confrères DPO de positiver et de prendre ce sujet à bras le corps pour en faire un levier de progrès* » - Bruno RASLE, intervenant

Objectifs généraux de la formation

Au-delà de la théorie, permettre aux DPO (internes, externes) et aux futurs DPO (ainsi qu'à leurs collaborateurs) de disposer de tous les éléments pour se forger leur propre méthode de gestion des violations de données au titre des articles 33 et 34 du RGPD, afin :

- De préparer son organisation à cette éventualité ;
- Maîtriser la gestion d'une violation de données ;
- D'identifier les difficultés, les pièges, les freins ;
- D'identifier son articulation avec le Privacy by Design et les analyses d'impact ;
- De se forger sa propre doctrine, dans le respect du cadre imposé ;
- D'en faire un levier au service du DPO et un axe de progrès.

Cette journée permet aussi à toute personne prenant part à la gestion d'une violation de données d'optimiser ses apports (RSSI, Risk Manager, membre d'une cellule de crise, …).

Violations de données
Pour ne pas subir

Version du 3 août 2022

Public

- DPO (internes, externes) ou équivalent ;
- Personnes accompagnant le DPO dans ses missions (adjoint, collaborateurs, relais) ;
- Personnes amenées à piloter ou participer au traitement d'une violation de données personnelles.

Moyens et méthode pédagogiques

- Relevé préalable des attentes et des questions spécifiques auprès des participants ;
- Cours magistral très interactif, avec intense participation des apprenants (études et travaux sur des cas concrets –dont certains de ceux signalés au préalable par les participants-, mises en situation, travail en groupes, réponses aux questions, …) ;
- QCM ;
- Apports théoriques (cadre légal, doctrine de la CNIL, …) ;
- Support de formation ;
- Riches apports documentaires : outre la base documentaire (lignes directrices, sélection de sanctions, …), remise d'exemples concrets d'AIPD, de procédures, de fiches Reflex, de support de communication interne, d'exemples de notes d'analyse soumise au responsable de traitement, d'exemples de communication aux personnes concernées).

Évaluation et sanction de la formation

- Évaluation finale ;
- Évaluation de satisfaction via un questionnaire ;
- Attestations de présence et de formation.

Prérequis

Aucun.

Il est cependant préférable d'avoir suivi au préalable les formations suivantes
(ou de détenir les connaissances équivalentes) :

- « *Réaliser une analyse d'impact (AIPD) : de la théorie à la pratique* » (1 jour) ;
- « *L'informatique appliquée au RGPD* » (1 jour).

Le fait d'avoir participé à la gestion d'une violation de données – de s'être frotté à la réalité - est un plus.

Durée • Tarif

1 journée de 7 heures
Tarif : nous consulter
12 apprenants maximum

Lieu

PARIS • La salle sera déterminée en fonction des dates et du nombre de participants.
Elle sera communiquée avec la convocation.

Nous sélectionnons uniquement des salles accessibles aux personnes à mobilité réduite

Modalités

Contact et inscriptions : formation@anaxia-conseil.fr • 06 33 15 81 83

Violations de données
Pour ne pas subir

Version du 3 août 2022

Sujets abordés au cours de la journée

En sus des questions évoquées *supra*, voici quelques autres sujets abordés au cours de la journée :

- La notification auprès de la CNIL : obligation de résultat ou de moyens ?
- Quel est le but que poursuivait le législateur européen avec cette disposition ?
- Le nombre de personnes concernées par la violation doit-il être pris en compte : concrètement, si l'incident ne concerne qu'une seule « victime », sommes-nous obligés de notifier ?
- Et si le responsable de traitement décide de ne pas notifier (alors qu'il le devrait) ?
- À quoi doit ressembler la « documentation » exigée par l'article 33.5 du RGPD ?
- Quelles sont les dispositions qui permettent d'éviter d'avoir à communiquer la violation aux personnes concernées ?
- Au sein d'un groupe d'entreprises qui partagent des applications et des ressources communes, qui doit notifier ?
- Et en cas de responsabilité conjointe ?
- En cas de relation entre deux responsables de traitement, le destinataire est-il contraint de signaler au fournisseur de données qu'il a subi une violation de données ?

Intervenant

Bruno RASLE forme les professionnels de la Privacy depuis 2007 au niveau le plus élevé (Mastère spécialisé). L'un des tous premiers membres de l'AFCDP (association française qui regroupe et représente les DPO), il en a été Délégué Général durant douze ans.

Il est Délégué à la Protection des Données mutualisé (pour une centaine d'organismes) pour l'une des branches de la Sécurité sociale. Il a cœur de partager son expérience et sa vision du métier de DPO.

- Expert RGPD certifié IAPP CIPP/E
- Spécialiste de la Sécurisation/protection des données
- Coauteur des ouvrages Halte au Spam (Eyrolles, 2003), Correspondant Informatique et Libertés : bien plus qu'un métier (AFCDP, 2015), Droit à l'oubli (Larcier, 2015), Se préparer au RGPD (Éditions législatives, 2017)
- Depuis 2005 : Expert « Informatique et Libertés »
  - Membre du Groupe de contact avec la CNIL sur l'avenir du métier de DPO
  - Membre du Comité de Pilotage du Mastère Spécialisé en Management et Protection des Données à Caractère Personnel (ISEP) • Chargé de cours • Tuteur de thèses professionnelles
  - Créateur de la formation « Kit de survie Technique pour Juristes, Avocats et DPO »
  - Créateur et animateur de plusieurs groupes de Travail : Préparation à un contrôle sur place de la CNIL • Cybersurveillance • Conformité des RSE • Notification des violations de données
  - Créateur et organisateur de l'Université des CIL/DPO jusqu'en 2020
  - Co-auteur du code de déontologie du DPO et de la version annoté, commentée et indexée du RGPD
  - Auteur des propositions de l'AFCDP adressées au G29 concernant les lignes directrices (RGPD), créateur du Job board des DPO
  - *Community Manager* d'AGORA AFCDP (> de 2.000 utilisateurs), réseau social privé de l'association des DPO
  - *Board Member* de CEDPO (Confédération européenne des associations de professionnels de la protection de la vie privée) et partenaire de l'IAPP (*International Association of Privacy Professionnals)*
  - Nombreuses publications et articles
  - Rédacteur de la lettre de veille « L'Actualité des données personnelles » de l'AFCDP
  - Nombreuses interventions en conférence