

Formation « PIA/ ISO 29134 »

« Etude d'impact sur la vie privée : Quand, pourquoi, comment ? » / #EIVP #DPIA

Réf : PIA

Avec l'avènement du règlement européen de protection des personnes physiques à l'égard de leurs données à caractère personnel (« RGPD »), s'est opéré un changement profond de paradigme. La gouvernance globale des données à caractère personnel est repensée au sein des organismes. Les responsables de traitement sont non seulement responsables de protéger ces données en adoptant des mesures adaptées mais également en charge de le prouver. L'incidence la plus directe est donc la place prépondérante que les organisations doivent donner au management des risques mais également au contrôle interne. En effet, il leur revient désormais d'évaluer elles-mêmes la part de risques sur la vie privée des personnes dont elles collectent, consultent, manipulent, stockent, transfèrent les données... Reste qu'analyser, évaluer et gérer ce risque spécifique suppose d'abord de maîtriser le management des risques mais aussi de comprendre et d'intégrer ce qui caractérise un risque sur la vie privée.

La formation insistera particulièrement sur :

- le management des risques sur la vie privée
- l'appréhension de l'ensemble des écosystèmes, au-delà de l'organisation
- la nécessité d'intégrer le PIA par défaut et au plus tôt des projets

Objectifs

- Maîtrise des règles encadrant le déclenchement et la réalisation des PIA
- Capacité à mobiliser les différentes parties prenantes et les faire collaborer aux PIA
- Disposer d'une démarche et d'une boîte à outils méthodologiques propres à éviter certains écueils

Durée & horaires

- 3 jours soit 21 heures
- Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Responsable de traitement / Sous-traitant
- Directions métiers
- Direction générale
- Fonctions support (Juridique, Marketing, Communication, DSI, RSSI, et autres fonctions spécialisées)
- DPO

Pré-requis

- Avoir suivi à minima une formation sur le RGPD, au mieux une formation DPO.

Méthode pédagogique

Le PIA étant avant tout une question de pratique, la formation alterne entre dispense des règles encadrant le PIA, et mises en situation coachées, notamment en utilisant l'outil PIA de la CNIL.

L'interactivité y est fortement encouragée grâce à des jeux de rôle.

Supports

- Support de cours au format papier en français
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PIA par HS2.

Programme

Jour 1 - Fondamentaux du PIA

- Définitions, vocabulaire
- Introduction au management du risque
- Présentation de l'outil PIA de la CNIL
- Atelier pratique : "PIA pas à pas, à l'aide de l'outil PIA CNIL"

Les formateurs distillent un PIA et les méthodologies différentes pour y parvenir.

Jour 2 - Cycle de vie du PIA

- Dans quel cas faut-il réaliser un PIA ?
- Quand faut-il déclencher le PIA, le mettre à jour ?
- La transmission du PIA
- Atelier pratique : "PIA : Jeu des différences"

Les stagiaires analysent un PIA existant et doivent l'améliorer au regard des acquis de la veille.

Jour 3 - Clôture et Examen

- Correction de l'atelier pratique de la veille
- Clôture et Q/R
- Examen