Normes et méthodes

ISO 27701 vs ISO 27001 - Norme internationale pour la protection des données personnelles

1 jour (7h00) | ★★★★½ 4,6/5 | ISO-RGPD | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Document mis à jour le 30/05/2023

Objectifs pédagogiques

- Décrire une vision globale d'un Système de Management des Informations Privées (SMIP)
- Expliquer les fondamentaux du Règlement Général européen de Protection des Données personnelles
- Définir les interactions entre ISO 27001 / 27002 et ISO 27701 / 27552.

Modalités et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatique...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Niveau requis

Avoir des connaissances fondamentales en matière de RGPD. Avoir de bonnes connaissances de l'ISO 27001 et l'ISO 27002 est un avantage. De plus, l'entreprise devra être certifiée aux normes ISO 27001 et ISO 27002 (à ce jour, la norme est exclusivement en anglais).

Public concerné

DPO, responsables de traitement, chefs de projet, RSSI et/ou sous-traitants.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Le contexte du RGPD pour l'entreprise

- Le Règlement Général pour la Protection des Données à caractère personnel exige que les responsables de traitement ou les sous-traitants adoptent des mesures organisationnelles et techniques pour réduire les risques de non-conformité, d'indisponibilité, de perte de confidentialité ou d'intégrité sur les traitements et les données.
- Les organismes doivent prouver qu'ils testent, analysent et évaluent régulièrement l'efficacité des mesures.
- Les normes ISO permettent de déterminer les cadres de travail de la mise en oeuvre d'un SMIP.

Rappeler les fondamentaux, les interactions et les obligations du RGPD dans le contexte de l'entreprise

Identifier les données personnelles et décrire les traitements des données pour le registre de traitement de données

- Comprendre les outils de suivi de conformité

Rappel de la norme ISO 29134

- Lignes directrices pour l'étude d'impacts sur la vie privée
- Les grilles d'évaluations
- Les propositions de la CNIL

ISO 27701

- Les exigences complémentaires par rapport à l'annexe A de la norme ISO 27001

Concept de "privacy by design"

- Intégration du "privacy by design" et du "privacy by default" (Art. 25 et considérant 78, Art. 40 et Art. 83) dans les projets (grille de détection, évaluation et bonnes pratiques)

Les processus d'anonymisation (avis G29, 05/214...) pour la gestion et l'alimentation des environnements de développement

- Proof Of Concept
- Test et recette avec les DCP de production

Concevoir et utiliser des grilles de conformité en se référant aux outils de l'ISO et de l'ANSSI

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)

Les + de la formation

Principe d'animation de cet atelier :

- La présentation magistrale d'un consultant certifié DPO

- Des exercices de compréhension

- La présentation des Normes Simplifiées de la CNIL comme guide rédactionnel

Support et outils mis à disposition :

- La présentation effectuée par le consultant au format PDF

- L'article 4 du Règlement Européen de Protection des Données personnelles

- Bibliographie Web des documents complémentaires à l'atelier