

Formation « ISO 27701 (ex. 27552) – Privacy Information Management System (PIMS) »

Réf : ISO27701LI

Avec l'entrée en application du RGPD, les exigences en matière de protection des données personnelles se sont renforcées. Le principe d'accountability est au cœur de la réglementation. Pourtant il n'existe pas encore de certification ni de label permettant aux organismes de démontrer leur conformité au RGPD.

La norme ISO 27701 est une étape importante vers la création d'une certification relative à la protection des données personnelles. Extension des référentiels ISO 27001 et ISO 27002, elle définit un cadre et énumère les mesures nécessaires à la mise en œuvre d'un PIMS (Privacy Information Management System) ou Système de management des données personnelles.

La formation ISO 27701 – Privacy Information Management System (PIMS) d'HS2 est dédiée à cette nouvelle norme. Son objectif est de présenter les apports de l'ISO 27701 aux référentiels ISO 27001 et ISO 27002 afin de permettre aux stagiaires d'implémenter et d'auditer un processus PIMS, notamment dans un contexte RGPD.

Objectifs

- Présenter le RGPD, les principes et les enjeux de la protection des données personnelles
- Présenter l'articulation de la norme ISO 27701 avec les référentiels ISO 27001 et ISO 27002
- Présenter les apports de la norme ISO 27701 en matière de protection des données personnelles, notamment dans un contexte RGPD
- Présenter les différentes étapes d'implémentation d'un PIMS (Système de management des données personnelles)
- Présenter les éléments utiles pour auditer un PIMS

Durée & horaires

- 5 jours soit 35 heures réparties en 31h30 de cours, 1h00 de travail individuel sur les exercices le soir et 2h30 d'examen.
- Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 17h00/17h30.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- DPO / RSSI / RSMSI
- Toute personne souhaitant implémenter un PIMS (Privacy Information Management System) au sein de son entreprise.

Pré-requis

- Connaître les normes ISO27001 et ISO27002 est indispensable.
- Connaître le RGPD est un véritable plus.
- Pour information, la norme ISO 27701 n'existe actuellement qu'en anglais.

Méthode pédagogique

La méthode pédagogique se base sur les quatre points suivants :

- Cours magistral basé sur les normes ISO 27701, ISO 27001, ISO 27002 et ISO 29100.
- Exercices de contrôle des connaissances sur les concepts à connaître et sur les normes.

- Exercices pratiques individuels et collectifs effectués par les stagiaires.
- Formation nécessitant 1 heure de travail personnel durant la session.

Supports

- Support de cours au format papier en français
- Cahier d'exercices et corrections des exercices
- Tous les documents nécessaires à la formation en français ou anglais
- 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

- Cette formation prépare à l'examen de certification ISO 27701 Lead Implementer. A l'issue de cette formation, le stagiaire passe l'examen d'une durée de 3h30 en français. L'examen est constitué d'une partie QCM sur les notions de cours et d'une partie rédactionnelle sous forme d'étude de cas.

Programme

1 - Introduction : Rappel du cadre général

- 1.1 - Protection des données personnelles et RGPD
- 1.2 - SMSI – Système de management de la sécurité de l'information
- 1.3 – Panorama des normes ISO dédiées à la protection de la vie privée
- 1.4 – Présentation générale de la norme ISO27701

2 – Processus PIMS – Privacy Information Management System

- 2.1 - Présentation des briques du processus PIMS
- 2.2 – Notion de protection des données personnelles (protection of privacy)
- 2.3 – La protection des données personnelles intégrée au système de management
 - -> Intégration de la protection des données personnelles aux différentes briques du processus

3 – Mesures de protection des données personnelles

- 3.1 – Présentation générale des mesures
- 3.2 – Focus sur les mesures clefs de la protection des données personnelles
 - -> Présentation des mesures essentielles de sécurité des données personnelles

4 – Mesures de protection des droits à la vie privée

- 4.1 – Au-delà de la sécurité, la conformité aux autres principes du RGPD
- 4.2 – Conditions de collecte des données
- 4.3 – PIA – Privacy impact assessment
- 4.4. – Droits des personnes concernées
- 4.5 – Concepts de Privacy by design and by default
- 4.6 – Transferts de données
- 4.7 – Sous-traitance

5 – Boîte à outils

-> Documentation du PIMS, Indicateurs, Veille et documents tiers utiles

6 - Focus sur l'audit

- 6.1 – Rappel de la méthodologie d'audit
- 6.2 - Grille d'audit et Documentation

7 – Conclusion