

DPO : Réussir sa conformité avec la norme ISO/IEC 27701

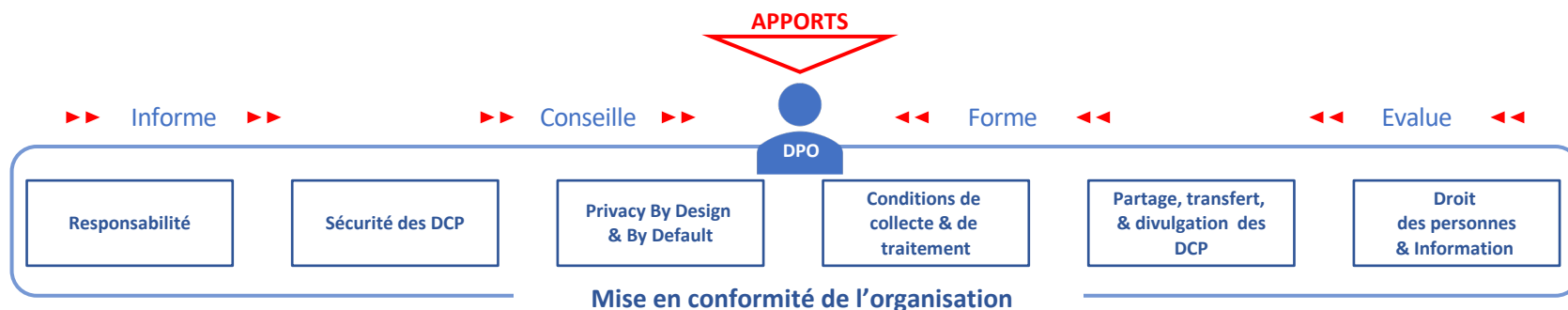
1^{ère} norme internationale en matière de protection des données personnelles

Réalisé avec le concours de la CNIL

Questions

Objectifs

POURQUOI ? Justification du projet	Dans quel but ? Quel est l'objectif visé ? Quelle finalité ?	Atteindre un niveau de sécurité en adéquation avec les risques relevés de l'organisme
QUOI ? Problématique	De quoi s'agit-il ? Quel est le sujet	Mettre en place un système de management de la protection de la vie privée (PIMS)
QUI ? Parties prenantes	Qui sont les acteurs ? Qui décide ? Qui propose le sujet ?	Constituer une équipe dédiée soutenue par la direction générale
OÙ ? Terrain d'action	Où cela se passe-t-il ? Dans quels services ?	Déterminer le périmètre d'intervention et/ou de certification
QUAND ? Planification	A quel moment faut-il s'engager ?	Planifier selon les objectifs de l'organisme et de la direction générale
COMMENT ? Plan d'action	Quelles sont les étapes pour y parvenir ?	Organiser la gouvernance, mettre en place les moyens nécessaires, impliquer les parties prenantes
COMBIEN ? Evaluation budgétaire	Quel coût ? Quels moyens ? Quelles ressources ?	Evaluer les écarts et valoriser les besoins en ressources



DPO : Réussir sa conformité avec la norme ISO/IEC 27701

1^{ère} norme internationale en matière de protection des données personnelles

Réalisé avec le concours de la CNIL

Pourquoi ?

Aucune obligation n'impose aux organismes d'être certifiés ISO/IEC 27701, il s'agit d'une démarche volontaire et individuelle permettant de démontrer son niveau de sécurisation des données traitées par l'organisme et de piloter sa gestion de la protection de la vie privée. Elle permet également de démontrer les engagements de Privacy pris par l'organisme.

Les entreprises du CAC 40, les ETI, les PME, les organismes publics (dont les collectivités territoriales) ont, en revanche, obligations de démontrer à leurs clients et aux autorités de protection que les données collectées et utilisées sont sécurisées. LE RGPD, la Loi Informatique et Libertés mais également le code de la consommation, le code des communications ... exigent, de la part des entreprises, une sécurisation de ces données adaptée aux risques.

La Norme ISO/IEC 27701 répond parfaitement à cette exigence.

Cette norme impose et implique des ressources et des moyens que toutes les entreprises n'ont pas ou ne peuvent pas mettre en œuvre pour obtenir une certification formelle. Il est intéressant en revanche pour tous les organismes privés ou publics de connaître cette norme et de tendre vers les règles et processus qu'elle décrit.

Cette norme peut être utilisée comme un outil de pilotage de la conformité, de contrôle et d'audit du RGPD et de la Loi Informatique et Libertés.

Il s'agit au final d'un ENJEU BUSINESS.

DPO : Réussir sa conformité avec la norme ISO/IEC 27701

1^{ère} norme internationale en matière de protection des données personnelles

Réalisé avec le concours de la CNIL

Quoi ?

ISO 27701 est une norme permettant de faire reconnaître un système de management de la protection de la vie privée dans le cadre de la gestion des risques liés aux traitements des données personnelles.

Publiée en 2019, **c'est la 1^{ère} norme certifiante d'une portée mondiale** qui a pour vocation principale de s'adapter à toutes les lois et réglementations relatives à la protection des données personnelles en vigueur dans le monde.

Extension des normes ISO 27001 et ISO 27002, ISO 27701 répond à **la nécessité de mettre en place un Système de management de la sécurité de l'information (SMSI) qui intègre le volet Privacy (PIMS).**

Qui ?

La norme ISO 27701 s'adresse au secteur public ou privé, PME, ETI et grands groupes, nationaux, européens et internationaux, agissant en qualité de responsables de traitement ou sous-traitants.

L'instance de pilotage est constituée par le DPO et le RSSI et par toutes personnes mettant en place des traitements de données à caractère personnel pour le compte d'un organisme.

Où ?

Toutes les composantes de l'organisme sont concernées, la sécurité et la conformité sont l'affaire de tous. Dans le cas d'un groupe, le projet s'étend à l'ensemble de ses implantations (filiales, succursales, bureaux ...) y compris à l'étranger. Pour faciliter la mise en œuvre, on pourra toujours s'appuyer **sur un périmètre déjà certifié ISO 27001 dans l'entreprise.**

Quand ?

Partant des résultats de l'audit de préparation (analyse des écarts, ...), la durée du projet dépend du périmètre de la certification, de la maturité de l'organisation et des moyens alloués au projet.

Il faut compter une durée de 6 mois minimum avec une préparation, variable en fonction du statut (RT, ST), de la taille, de l'implantation géographique de l'organisme ainsi que du secteur d'activité et de la typologie des données traitées.

Il s'agit ensuite d'entretenir et de maintenir cette conformité (en cas de certification, une fois par an).

DPO : Réussir sa conformité avec la norme ISO/IEC 27701

1^{ère} norme internationale en matière de protection des données personnelles

Réalisé avec le concours de la CNIL

Comment ?

Il faut constituer une équipe dédiée. Le travail des équipes DPO/RSSI doit être parfaitement coordonné. La documentation doit être accessible et régulièrement mise à jour, sécurisant le DPO dans sa démarche *d'accountability*.

La direction générale doit être impliquée et toutes les parties prenantes doivent avoir suivi une formation. Les collaborateurs doivent être sensibilisés (mise en place de pages intranet, de supports, d'affichage, d'insertion dans le livret d'accueil...). Tout moyen profitable à la **pérennisation** des actions doit être mis en œuvre et s'intégrer dans un processus **d'amélioration continue**.

Combien ?

Le coût du projet varie en fonction du périmètre de certification et de la maturité de l'organisme.

Il faut identifier et valoriser les coûts indirects et cachés (collaborateurs impliqués dans la démarche, cabinets sollicités pour la préparation à la certification et cabinet de certification à blanc, audit final ...)

Conseils

- Il est indispensable de bien comprendre les exigences de la norme ISO 27701 avant de commencer.
- Seules les formes verbales «**doit**» et «**doivent**» sont utilisées pour exprimer **une ou des exigences pour se conformer à la norme**.
- Les exigences des articles 5, 7 (RT), 8 (ST) ainsi que les annexes A et B **sont obligatoires**.
- Les expressions telles que «*il convient*», «*il est recommandé*», «*peut*» et «*peuvent*» caractérisent les **bonnes pratiques d'implémentation**, elles ne concourent en aucune façon à exprimer une exigence.
- Il est recommandé de s'informer s'il subsiste dans les archives de l'organisme une documentation créée lors d'une mise en conformité RGPD qui pourront alimenter la *base* du dossier de certification.
- Les **principes directeurs du RGPD** sont repris et intégrés dans la norme ISO 27701.
- **Pour autant la norme ISO 27701 ne constitue pas une certification au sens du RGPD (Art 42).**