La norme ISO 27701 garante de la protection de la vie privée

Par Amélie Paget, Consultante indépendante & Formatrice HS2

Avec le RGPD, les exigences en matière de protection des données personnelles se sont renforcées, autant en termes de sécurité que de droits des personnes. On assiste à un changement de paradigme, passant d'une autorisation préalable de la CNIL à un principe d'*accountability* : toute organisation traitant des données à caractère personnel (DCP) doit être en mesure de démontrer sa conformité à tout moment. Le public est sensibilisé à la protection de la vie privée et attend des engagements forts de tous les acteurs, prestataires et donneurs d'ordre. Pourtant, deux ans après l'entrée en application du Règlement européen, il n'existe pas encore de certification ni de label garantissant la conformité au RGPD. La norme ISO 27701, publiée en août 2019, marque une étape importante en ce sens. Ce référentiel, développé initialement sous le numéro ISO 27552, est une extension des normes internationales ISO 27001 et ISO 27002, reconnues et éprouvées en matière de cybersécurité. Elle vient ajouter un volet « *privacy* » au SMSI et aux mesures de sécurité de l'information détaillés dans ces deux normes. Elle propose un cadre pour l'implémentation d'un PIMS (*Privacy Information Management System*) ou, en français, Système de management de la protection de la vie privée, complété par de nouvelles mesures dédiées à la gestion des DCP et aux droits des personnes concernées. Elle couvre ainsi les principales exigences du RGPD et constitue un outil majeur de gestion de la conformité pour les acteurs du marché manipulant des données personnelles.

Fiche d'identité
ISO/IEC 27701 :2019 – Technique de sécurité – Extension d'ISO/IEC 27001 et ISO/IEC 27002 au mangement de la protection de la vie privée – exigences et lignes directrices.
1ère édition : Août 2019.
Langue d'origine : EN.
Traduite en FR. 80 pages.
Table des matières
1 – Domaine d'application
2 – Référence normatives
3 – Termes, définitions et abréviations
4 - Généralités
5 – Exigences spécifiques au PIMS liées à l'ISO 27001
6 – Recommandations spécifiques au PIMS liées à l'ISO 27002
7 – Recommandations supplémentaires de l'ISO 27002 pour les responsables de traitements
8 – Recommandations supplémentaires de l'ISO27002 pour les sous-traitants
Annexe A (normative) - Objectifs et mesures de référence spécifique au PIMS (RT)
Annexe B (normative) – Objectifs et mesures de références spécifiques au PIMS (ST)
Annexe C (informative) – Correspondance avec l'ISO 29100
Annexe D (informative) – Correspondance avec le RGPD
Annexe E (informative) – Correspondance avec l'ISO 27018 et ISO 29151
Annexe F (informative) – Comment appliquer l'ISO 27701 à l'ISO 27001 et l'ISO27002
Bibliographie

Figure 1 : Fiche d'identité - Norme ISO 27701 (tout droit réservé HS2)

A qui s'adresse cette norme ?

La norme ISO 27701 s'adresse, en premier lieu, à toute organisation dont la confiance en matière de protection de la vie privée représente un enjeu business. En effet, ce document est la première norme ISO qui permet de certifier sa gestion de la protection de la vie privée, et ainsi de démontrer les engagements *privacy* d'un prestataire. Certains l'ont bien compris et ont annoncé leur certification ISO 27701 avant même la parution de la norme d'accréditation associée. Ainsi, par exemple, les offres Microsoft Azure et Dynamics sont certifiées ISO 27001 et ISO 27701 par l'organisme américain Schellman [1].

La norme est également un très bon référentiel pour toute entité souhaitant gérer les exigences *privacy* légales, réglementaires et contractuelles sous la forme d'un système de management. Cette approche permet de structurer la démarche de mise en conformité, de maintenir cette conformité dans le temps et de l'améliorer

en continu. C'est le propre d'un système de management.

L'ISO 27701 est une norme internationale. Plusieurs autorités de protection des données ont participé aux groupes de travail de l'ISO (Organisation internationale de normalisation), des autorités européennes, mais aussi des États-Unis, d'Asie, du Canada ou d'Australie. De nombreuses contributions ont également été déposées par les acteurs majeurs du secteur, via la liaison officielle entre le CEPD (Comité Européen de la Protection des Données) et l'ISO. La portée de l'ISO 27701 est donc mondiale. Elle permet à une organisation d'intégrer les exigences du RGPD (Règlement général sur la protection des données) à son système de management, mais pas seulement. Elle est également adaptée aux réglementations étrangères, comme la loi californienne, brésilienne ou australienne. C'est d'ailleurs un autre avantage de la norme si votre entreprise s'inscrit dans un contexte multinational.

Tout comme l'ISO 27001, la norme ISO 27701 s'adresse à tout type d'organisation, tant publique que privée, de petite ou grande taille, ayant un niveau de maturité variable dans sa gestion de la sécurité de l'information et de la protection de la vie privée. Pour autant, avoir un système de management certifié ISO 27701 sous-entend une certification ISO 27001 préalable. Cette démarche représente un investissement important pour une organisation. Un SMSI (Système de management de la sécurité de l'information) déjà certifié au sein d'une organisation mature en matière de compliance n'aura pas de difficulté à obtenir une certification ISO 27701. Pour les autres, une étude préalable des coûts *versus* avantages apparaît incontournable.
Enfin, cette norme s'adresse tant aux responsables et co-responsables de traitement qu'aux sous-traitants et sous-sous-traitants. Les recommandations ajoutées à la norme ISO 27002 se décomposent en trois parties : clauses 6, 7 et 8 de la norme ISO 27701. La première s'adresse à toute organisation, alors que la deuxième cible les responsables de traitement et la dernière les sous-traitants.

STANDARD

The ISO 27701 standard guarantees protection of privacy

By Amélie Paget, Freelance Consultant and HS2 Trainer

The requirements in terms of protection of personal data have been reinforced under GDPR, both in terms of security and the rights of persons. It amounts to a paradigm shift, changing from the delivery of a prior CNIL authorisation to a principle of accountability: any organisation processing personal data (DCP) must be able to demonstrate its compliance at all times. The public is now familiar with, and mindful of the protection of privacy and expects clear commitments from all actors, providers and contractors. However, two years after the entry into force of the European Regulation, there is still no certification or label guaranteeing compliance with GDPR. ISO 27701, published in August 2019, marks an important step in this direction. This standard, initially developed under the number ISO 27552, is an extension of the international standards ISO 27001 and ISO 27002, widely accepted, tried and tested in cybersecurity. It adds a "privacy" component to the ISMS and to the information security measures detailed in these two standards. It offers a framework for the implementation of a PIMS (Privacy Information Management System), supplemented by new measures dedicated to the management of personal data and related personal rights. It thus covers the main requirements of the GDPR and constitutes a major compliance management tool for market players handling personal data.

Qu'est-ce qu'un PIMS ?

La norme ISO 27701 vise à mettre en place un PIMS (*Privacy Information Management System*) ou Système de management de la protection de la vie privée en français. Calqué sur le SMSI dont il est une version dérivée, le PIMS reprend les caractéristiques et les briques du système de management. C'est un ensemble de mesures organisationnelles et techniques permettant d'atteindre un objectif et de le maintenir dans la durée. Il repose sur 3 piliers : l'approche par le risque, l'amélioration continue et l'auditabilité. Cette dernière implique une documentation et une traçabilité solide. En présence d'un PIMS, il s'agit d'intégrer la protection de la vie privée à l'ensemble de ces éléments.

Ainsi, la norme ISO 27701 commence par indiquer que les exigences de l'ISO 27001 mentionnant la sécurité de l'information doivent être étendues à la *privacy*. En pratique, partout où il et écrit « sécurité de l'information » au sein de l'ISO 27001, il faut employer l'expression « sécurité de l'information et protection de la vie privée ».
A titre d'exemple, la PSI, document essentiel d'un SMSI par lequel la Direction affirme ses engagements et les objectifs en matière de sécurité de l'information, devient une Politique de sécurité de l'information et de la protection de la vie privée au sein de laquelle la Direction affirme également ses engagements et objectifs en matière de *privacy*.

Au-delà de ces amendements, la norme ISO 27701 complète les exigences de la norme ISO 27001 sur deux éléments du processus en phase *Plan* (Planification).
Il s'agit tout d'abord de la compréhension du contexte de l'organisation (Clause 4 de l'ISO 27001). Dans le cadre d'un PIMS, l'organisation doit déterminer sa qualification. Est-elle responsable de traitement, co-

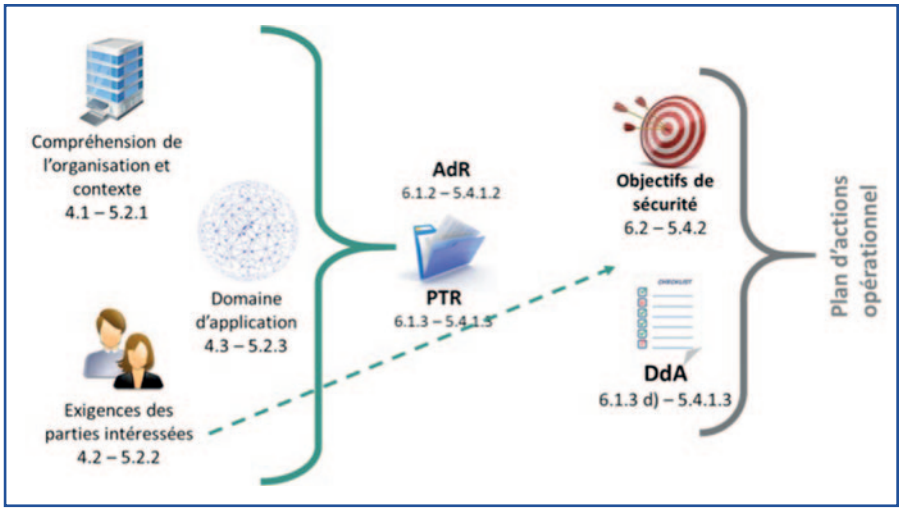

Figure 2 : PIMS - Projet d'implémentation (tout droit réservé HS2)

responsable ou sous-traitant ? De plus, parmi les éléments internes et externes à prendre en considération dans son contexte, doivent figurer les exigences légales et réglementaires en matière de protection de la vie privée, la jurisprudence, les recommandations des autorités compétentes en la matière, ainsi que les exigences contractuelles. Parmi les parties prenantes, on compte les autorités de contrôle, telles que la CNIL en France, les responsables et co-responsables de traitement et, bien évidemment, les personnes concernées. Lors de la définition du périmètre du PIMS, une description des traitements de DCP est attendue. Il s'agit ensuite de la planification (Clause 6 de l'ISO 27001), plus précisément de l'appréciation des risques et du plan de traitement des risques. En plus d'une appréciation des risques (AdR) de sécurité de l'information, l'organisation doit également réaliser une AdR sur la vie privée pour identifier les risques liés aux traitements des DCP. Doivent être considérées les conséquences potentielles pour l'organisation, mais aussi pour les personnes concernées. La norme précise que ces deux volets de l'appréciation des risques peuvent être distincts ou confondus. Dès lors, les mesures déterminées pour traiter les risques identifiés doivent couvrir les risques pour l'organisation, ainsi que pour les personnes concernées. Enfin, la Déclaration d'applicabilité, comme pour un SMSI, doit présenter les mesures nécessaires, la justification de leur insertion, si ces mesures sont mises en œuvre ou non, et la justification de l'exclusion de toute mesure des annexes A et B des normes ISO 27001 et ISO 27701. Concernant la justification d'inclusion et d'exclusion des mesures, l'ISO 27701 précise qu'elle peut être liée aux exigences légales et réglementaires. Dans un contexte européen, cette Déclaration d'applicabilité fait un lien direct entre l'ISO 27701 et le RGPD.

Quel périmètre pour un PIMS ?

La certification ISO 27001 du système de management est un prérequis à la certification ISO 27701. Les périmètres du PIMS et du SMSI n'ont pas à être confondus. Cependant, le périmètre du PIMS doit nécessairement être couvert intégralement par celui du SMSI.

La certification ISO 27701 ajoute une complexité au SMSI de par ses exigences et recommandations supplémentaires. Dans ce contexte, il convient de mener une réflexion approfondie quant au choix du périmètre du SMSI et du PIMS. Si plusieurs offres méritent d'être couvertes par une certification ISO 27001 et ISO 27701, faut-il opter pour un large périmètre couvrant l'ensemble de ces offres ? Ou bien préférer scinder ce périmètre en plusieurs SMSI et PIMS ? Ce deuxième choix peut complexifier la démarche, notamment en termes de documentations, revues et audits. Pour autant, il apporte une sécurité quant aux certifications : une non-conformité sur l'un des systèmes de management peut ici impacter la certification d'une seule offre et non de l'ensemble. Cet avantage est d'autant plus pertinent qu'il peut être complexe de maintenir dans la durée la conformité sur un large périmètre.
En présence d'un SMSI et d'un PIMS, se pose également la question de la double documentation. Par exemple, faut-il une PSI et une Politique de protection de la vie privée ou bien une Politique unique couvrant les deux thématiques ? La norme ISO 27701 laisse la possibilité de choisir entre les deux options. Si les périmètres diffèrent, que le SMSI est plus large que le PIMS, une documentation distincte peut être justifiée. Dès lors que les périmètres sont confondus, la bonne pratique tend à limiter au maximum la double documentation. Le premier atout de la norme ISO 27701 est d'intégrer la gestion de la conformité en matière de protection de la vie privée au système de management existant.

Quels acteurs pour le PIMS ?

Plusieurs acteurs sont incontournables pour l'implémentation, puis la gestion d'un PIMS.

Comme pour un SMSI, la Direction de l'organisation tient un rôle important. Elle endosse la responsabilité du système de management et détient le pouvoir décisionnel. Elle porte les objectifs de sécurité de l'information et de protection de la vie privée. Elle doit approuver et valider chaque étape du processus, notamment le périmètre, l'appréciation des risques, la déclaration d'applicabilité et le plan de traitement des risques. Elle assiste aux revues de direction. De même, un PIMS est un projet transverse, dont le succès dépend de l'implication de l'ensemble des équipes de l'organisation. Enfin, la certification ISO 27701 est un projet complexe qui nécessite la désignation d'un chef de projet. Le chef de projet idéal est compétent en matière de sécurité de l'information et de protection de la vie privée. Il doit avoir un profil juridique et technique. A défaut, il doit être épaulé par un profil soit juridique, soit technique, selon ses besoins. Mais surtout, le chef de projet doit maîtriser la notion de SMSI et son implémentation, ainsi que la norme ISO 27001. La certification ISO 27701, l'implémentation d'un PIMS, bien que dédié à la protection de la vie privée, n'est pas un projet purement juridique ni documentaire. Il s'agit avant tout de mettre en place un système de management adapté à l'existant, pertinent et opérationnel dans la durée.

Et quelle est la place du délégué à la protection des données (ou DPO pour *Data Protection Officer* en anglais) ? La norme ISO 27701 ajoute, aux recommandations liées aux fonctions et responsabilités issues des mesures de sécurité de l'ISO 27002, la désignation d'un point de contact pour les clients et les personnes concernées pour toutes questions liées aux traitements de DCP, ainsi que la nomination d'une personne responsable du programme de gouvernance et de protection de la vie privée à l'échelle de l'organisation. La norme précise l'expertise, les missions, l'indépendance et le positionnement auprès de la direction que devrait présenter ce responsable. Ces critères sont très proches de ceux énumérés à l'article 38 du RGPD dédié au DPO. D'ailleurs, l'ISO 27701 précise explicitement que « cette personne est appelée 'délégué à la protection des données' dans certaines juridictions ». Ainsi, le DPO est appelé à être le responsable du volet Protection de la vie privée d'un PIMS, comme le RSSI est souvent responsable du volet sécurité de l'information d'un SMSI. Cela fait un point de plus en faveur d'une collaboration étroite entre DPO et RSSI au sein de l'organisation. L'un comme l'autre, dès lors qu'il dispose des ressources et compétences nécessaires, pourrait être chef de projet PIMS sans que cela ne soit systématique.

Quelles sont les mesures associées au PIMS ?

La norme ISO 27701 ajoute une « surcouche » aux recommandations de la norme ISO 27002. Ces ajouts permettent d'intégrer les enjeux *privacy* et de protection des DCP, catégorie particulière d'informations. Ils insistent sur les points critiques de la sécurité des DCP, tels que le chiffrement des données, la mise au rebut du matériel, la gestion des accès et des habilitations, la sauvegarde et la restauration des données, la journalisation et la surveillance, la sécurité lors des transferts de données, la protection des données de test, la gestion des incidents de sécurité et, bien évidemment, la sécurité dans les contrats avec les fournisseurs. Ces recommandations s'adressent indifféremment aux responsables de traitement et aux sous-traitants.

Au-delà de ces recommandations organisationnelles et techniques, la norme ISO 27701 comporte deux chapitres (7 et 8) dédiés respectivement aux responsables de traitement et aux sous-traitants. Ces chapitres énumèrent de nouvelles mesures à intégrer à la déclaration d'applicabilité. Elles sont d'ailleurs reprises dans ce sens en annexes A et B de la norme ISO 27701. Ces ajouts correspondent davantage à des mesures de conformité en matière de protection de la vie privée. Elles

permettent notamment d'intégrer les exigences du RGPD. On y retrouve ainsi les six principes fondamentaux énumérés à l'article 5 du Règlement européen [2] et la gestion des droits des personnes concernées.

Aux termes de la norme ISO 27701, ces mesures ne sont pas obligatoires. Il s'agit de recommandations. Elles peuvent être inclues ou exclues, le tout devant être justifié. Pour autant, l'une des premières étapes du PIMS est la définition du contexte, des exigences légales et réglementaires, mais aussi celles des parties prenantes, dont les autorités de contrôles. Or, la majorité des mesures énumérées aux clauses 7 et 8 de la norme ISO 27701 reprennent des exigences du RGPD, bien qu'étant moins précises que notre cadre légal. Ainsi, de par son approche, la norme ISO 27701 offre une méthodologie solide pour appréhender l'ensemble des exigences légales et réglementaires en matière de protection de la vie privée. La mise en place d'un PIMS répond également à l'exigence d'*accountability* érigée par le RGPD.

Quelles sont les autres normes ISO indispensables ?

Au-delà des normes ISO 27001 et ISO 27002, une pleine appréhension de la norme ISO 27701 nécessite notamment de connaître : 1) la norme ISO 29100 [3] qui présente le cadre dédié à la protection de la vie privée, 2) la norme ISO 29101 [4] consacrée plus spécifiquement à l'architecture de référence en matière de *privacy* et 3) l'ISO 29134 [5] dédiée à l'Analyse d'impact sur la vie privée.

La connaissance de ces normes, ainsi que du cadre légal et réglementaire en matière de protection de la vie privée, pourrait d'ailleurs être un prérequis pour les auditeurs ISO 27701 dans le cadre de la procédure de certification. A ce titre, la norme d'accréditation est à l'étude depuis avril 2020 [6] . Outre des conditions de qualification supplémentaires des auditeurs, les durées d'audits pourraient également être allongées par rapport aux audits ISO 27001.

Et qu'en est-il des normes ISO 27151 et 27018 ? Vont-elles disparaître ? La première est consacrée aux bonnes pratiques pour la protection des DCP ; la seconde se concentre sur la protection de la vie privée dans le cadre du *Cloud Computing*. L'annexe E de la norme ISO 27701 dresse la correspondance entre ces trois documents. Elle montre comment les normes ISO 27151 et ISO 27018 ont été absorbées, complétées et mises à jour par la norme ISO 27701, ce qui les rend potentiellement obsolètes.

Quelle est la portée de la certification ISO 27701 ?

La norme ISO 27701, comme toute norme en 01, est certifiante. La norme d'accréditation des organismes de certification est en cours d'élaboration. En attendant, certains organismes proposent déjà des audits de certification ISO 27701 pour répondre à la demande pressante des acteurs du marché.

De plus, la certification de personnes est également possible. En France, différents organismes de formations proposent des examens certifiants. Ils permettent de démontrer la connaissance de la norme ISO 27701. Cette expertise est un prérequis pour être auditeur. C'est également un atout pour participer à l'implémentation d'un PIMS.

La norme ISO 27701, de par ses recommandations, couvre l'essentiel des exigences du RGPD. Comme l'indique la CNIL [7] , sa proximité avec le Règlement européen est matérialisée par l'Annexe D de la norme qui dresse la concordance entre l'ISO 27701 et les articles du RGPD. De par son auditabilité, la mise en place d'un PIMS s'inscrit parfaitement dans le principe d'*accountability* érigé à l'article 5.2 du Règlement. Pour autant, la norme ISO 27701 est internationale. Elle permet de répondre aux exigences du RGPD de par la sélection de mesures énumérées aux clauses 6, 7 et 8 de la norme, mais aussi aux exigences légales et réglementaires d'autres juridictions.

Bien que soutenue par la CNIL, qui en fait la promotion et participe activement aux groupes de travail de l'ISO, la certification ISO 27701 ne saurait être synonyme de légalité ou de conformité RGPD. De plus, elle ne correspond pas à la certification prévue à l'article 42 du RGPD. Pour autant, dans un avenir proche, on pourrait imaginer une certification RGPD approuvée par la CNIL et le CEPD qui serait basée sur la certification d'un système de management ISO 27701, un peu comme la certification HDS est basée sur l'ISO 27001 et l'ISO 20000-1.
En tout état de cause, la certification ISO 27701 permet de démontrer aux autorités de contrôle une démarche active de protection de la vie privée. Elle permet, en outre, aux organisations de monter en maturité et de se préparer à un éventuel contrôle de la CNIL. ■■■

[1] Certification Microsoft Azure et Dynamics : https://servicetrust.microsoft.com/ViewPage/MSComplianceGuideV3?command=Download&downloadType=Document&downloadId=e0572c64-5a40-44e0-ba9a-1fd55a22f3ee&tab=7027ead0-3d6b-11e9-b9e1-290b1eb4cdeb&docTab=7027ead0-3d6b-11e9-b9e1-290b1eb4cdeb_ISO_Reports
[2] Rappel des 6 principes fondamentaux de l'art. 5.1 du RGPD : a) licéité, loyauté, transparence ; b) limitation des finalités ; c) minimisation des données ; d) exactitude ; e) limitation de la conservation ; f) intégrité et confidentialité.
[3] Norme ISO/IEC 29100 : 2011 Technologies de l'information – Techniques de sécurité – Cadre privé
[4] Norme ISO/IEC 29101 : 2018 Technologies de l'information – Techniques de sécurité – Cadre d'architecture de confidentialité
[5] Norme ISO/IEC 29134 :2017 Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'étude d'impacts sur la vie privée
[6] Norme ISO/IEC WD 27558 : https://www.iso.org/fr/standard/71676.html
[7] L'ISO 27701, une norme internationale pour la protection des données personnelles : https://www.cnil.fr/fr/liso-27701-une-norme-internationale-pour-la-protection-des-donnees-personnelles