LES ESSENTIELS

La norme ISO 27701

Mars 2022

CLUSIF

L’article L. 122-5 de la propriété intellectuelle n’autorisant pas les représentations ou reproduction intégrale, ou partielle, faite sans le consentement de l’auteur ou de l’ayant droit ou ayant cause, sauf exception stricte (« copies ou reproductions réalisées à partir d’une source licite et strictement réservées à l’usage privé du copiste et non destinées à une utilisation collective », analyses et les courtes citations dans un but d’exemple et d’illustration, etc.), toute représentation ou reproduction, par quelque procédé que ce soit du présent document sans autorisation préalable du Clusif constituerait une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Table des matières

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Thomas	**VAN DEN HEUVEL**	Agence de la biomédecine

Les contributeurs :

Amélie	**PAGET**	HS2
Grégory	**ADROT**	Armand Thiery
Frédéric	**VILLANOVA**	Effective Yellow
Afaf	**FAFI**	Banque de France
Thierry	**MATUSIAK**	Microsoft
Thomas	**BOUSSON**	ON-X

Le Clusif remercie également les adhérents ayant participé à la relecture.

Le présent document est une note synthétique visant à présenter la norme ISO 27701. Il sera complété par un dossier technique détaillé consacré au déploiement d'un système de management de la protection de la vie privée (PIMS - *Privacy Information Management System*).

1 Qu'est-ce que la norme ISO 27701 ?

Titre : ISO 27701:2019

Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée – Exigences et lignes directrices

Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

Edition : 1ère édition 2019-08

Langue : En Anglais et en Français

Nombre de pages : 80

Lien : https://www.iso.org/fr/standard/71670.html

2 Présentation de la norme

La norme ISO 27701 est une extension des normes ISO 27001 et ISO 27002. Elle n'est pas autosuffisante. Ainsi, pour avoir une lecture complète de la norme, il faut être muni des trois documents.

Elle complète les exigences de la norme ISO 27001. Le SMSI (Système de Management de la Sécurité de l'Information) défini par la norme ISO 27001 intègre la gestion des données personnelles pour devenir un PIMS : système de management de la protection de la vie privée (ou *Privacy Information Management System*).

Elle apporte également des recommandations complémentaires et supplémentaires à la norme ISO 27002. La norme ISO 27701 présente un catalogue de mesures de sécurité des données personnelles, mais aussi des mesures liées à la protection des droits des personnes concernées, à la proportionnalité et à la nécessité des traitements.

Objectifs de la norme

Permettre à une organisation, sur un périmètre donné, de déployer un PIMS et de le maintenir dans la durée.

Rappel

Normes ISO/CEI : normes produites par l'*International Organization for Standardization* (ISO) et la Commission électrotechnique internationale (CEI). Elles sont consacrées au management et à la qualité. Leur objectif est de définir, pour un secteur et un sujet donné, les bonnes pratiques en matière de management et de qualité. Elles sont reconnues à l'internationale. Certaines permettent d'obtenir la certification d'un système de management déployé au sein d'un organisme ou encore une certification de personnes démontrant leur compétence pour implémenter ou auditer un tel système.

Norme ISO 27001

ISO/IEC 27001:2013

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Norme ISO 27002

ISO/IEC 27002:2013

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information

Remarque

La norme ISO/IEC 27002:2013 reste à prendre en référence pour la certification ISO/IEC 27701:2019, malgré la publication de la norme ISO/IEC 27002:2022.

3 Qu'est-ce qu'un PIMS ?

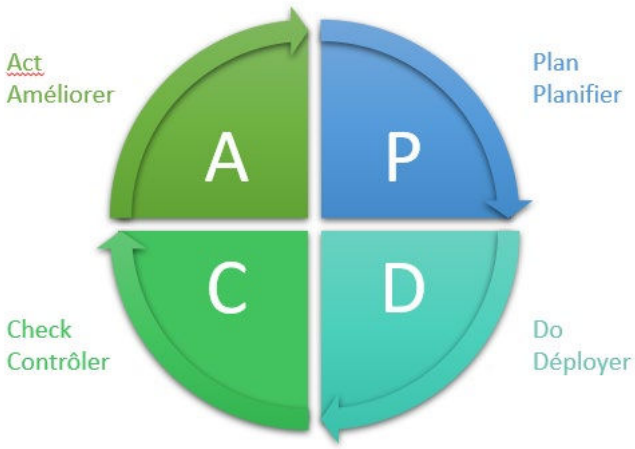
Système de management

Un système de management permet d'établir des politiques, de définir des objectifs et des processus et d'atteindre des objectifs (ISO 9000 et ISO 27000).

C'est un ensemble de mesures organisationnelles et techniques permettant d'atteindre un objectif et de le maintenir dans la durée.

Chaque processus comprend des éléments d'entrée et de sortie déterminés et repose sur des acteurs dédiés. Il repose sur le cycle PDCA (Roue de *Deming*[1]) :

- Plan : Planifier
- Do : Déployer
- Check : Contrôler
- Act : Améliorer



Cycle PDCA, illustration HS2

Un système de management est transverse : il inclut les différents métiers de l'organisation et chaque échelon de l'organigramme (de la direction générale aux agents et utilisateurs).

Il est basé sur des référentiels écrits : une norme et des exigences, des procédures écrites et des preuves écrites. Un système de management est auditable. Un PIMS est un système de management. C'est une extension d'un SMSI, un « SMSI augmenté ».

SMSI : Système de management de la sécurité de l'information

Système de management dont l'objectif est, sur un périmètre donné, d'assurer la sécurité de l'information.

[1] https://fr.wikipedia.org/wiki/Roue_de_Deming

L'information regroupe l'ensemble des actifs informationnels, y compris les informations financières, la propriété intellectuelle, les informations sur les employés, ou les informations qui leur sont confiées par des clients ou des tiers (ISO 27000).

La sécurité consiste en la protection de la confidentialité, de l'intégrité et de la disponibilité de l'information. D'autres propriétés peuvent être ajoutées. Ainsi, la traçabilité est régulièrement intégrée : DIC(T). Cela est particulièrement intéressant en matière de protection des données personnelles pour s'inscrire dans le concept d'*accountability*.

PIMS : Système de management de protection de la vie privée

Privacy Information Management System

ISO 27701 - 3.2 « Système de management de la sécurité de l'information qui gère la protection de la vie privée telle que potentiellement affectée par le traitement des DCP (Données à caractère personnel). »

Ce système de management permet d'assurer, sur un périmètre donné, la protection des données personnelles de manière stable et pérenne, documentée et tracée.

Il intègre la sécurité des données personnelles mais aussi la protection des droits des personnes concernées ainsi que la proportionnalité et la nécessité des traitements.

4 A qui s'adresse la norme ?

La norme s'adresse à toute organisation souhaitant gérer la protection des données sous la forme d'un système de management.

- Secteur public ou privé
- Petites, moyennes et grandes entités
- Organisations nationales, européennes et internationales
- Responsables de traitement (RT) et/ou sous-traitants (ST).

Cette norme est pertinente pour toute personne souhaitant avoir une approche de la protection des données personnelles sous l'angle d'un système de management. Elle offre une vision complète de la protection de la vie privée. Elle couvre en effet tant les aspects sécurité des données que le volet « conformité » (tels que les principes de *privacy by design and by default*, la gestion des droits des personnes, le respect des principes fondamentaux de proportionnalité et de nécessité des traitements). De plus, elle permet d'intégrer à un système de management les exigences des juridictions européennes mais aussi étrangères.

5 Quels sont les intérêts de la norme ? Pourquoi déployer un PIMS ?

L'approche de la protection de la vie privée proposée par la norme permet de gérer la conformité de son organisation au RGPD (Règlement général sur la protection des données) ainsi qu'aux éventuels autres textes applicables et d'assurer la sécurité des données personnelles sous l'angle d'un système de management.

La mise en place d'un PIMS permet :

- d'inscrire l'organisation dans une démarche vertueuse, unifiée et fédératrice pour l'ensemble de ses entités ;
- de gérer les exigences du RGPD et toutes exigences légales et réglementaires applicables à l'organisation ;

- d'offrir une bonne visibilité sur ses traitements de données personnelles, ses processus, sa conformité et sa maturité ;
- de s'inscrire dans une démarche saine, stable et pérenne ;
- d'assurer l'amélioration continue ;
- d'intégrer les concepts de *Privacy by design et by default* ;
- d'assurer son *Accountability* (responsabilité, documentation, traçabilité et auditabilité) ;
- d'assurer la protection des données personnelles en synergie avec un SMSI existant.

De plus, la norme ISO 27701 est certifiante et les certifications ISO sont reconnues en France, en Europe et à l'échelle internationale. C'est un atout en termes d'image, de confiance, de business.

6 La norme est-elle certifiante ?

Oui, cependant la norme ISO 27701 n'est pas autosuffisante.

La norme ISO 27701 permet de certifier un système de management de protection de la vie privée (PIMS). Mais attention, la certification du SMSI selon la norme ISO 27001, couvrant le périmètre du PIMS, est un prérequis. Il existe également des certifications de personnes pour l'implémentation et les audits de PIMS.

Exigences pour un PIMS (extension d'ISO 27001) :

- Présentation du contexte et des enjeux
  - Inclusion des traitements de DCP
  - Détermination du statut / responsabilité de l'organisation et des parties prenantes
  - Identification des exigences légales et réglementaires en matière de protection des données personnelles
- Définition du périmètre
  - Notamment par la cartographie des données personnelles, des traitements et des flux
- Politique et engagement de la direction
- Gestion des risques sur la vie privée liés aux traitements de DCP
  - Analyse/appréciation des risques liés à la sécurité des données personnelles
  - Analyse/appréciation de la proportionnalité et de la nécessité des traitements (conformité)

Recommandations pour les RT et les ST (extension d'ISO 27002) :

1. Sécurité des données personnelles
2. Principes fondamentaux (licéité, minimisation des données…)
3. Droits des personnes (information, consentement, droit d'accès…)
4. Gouvernance (*Privacy by design and by default*, *Privacy Impact Assessment*, *Accountability*)
5. Partage, transfert et mise à disposition

7 Quel est le contenu de la norme ?

Plan de la norme ISO 27701 :

Avant-propos

Introduction

1 - Domaine d'application

2 - Références normatives

3 - Termes, définitions et abréviations

4 - Généralités

5 - Exigences spécifiques au PIMS liées à l'ISO/IEC 27001

6 - Recommandations spécifiques au PIMS liées à l'ISO/IEC 27002

7 - Recommandations supplémentaires de l'ISO/IEC 27002 pour les RT

8 - Recommandations supplémentaires de l'ISO/IEC 27002 pour les ST

Annexe A (normative) : Objectifs et mesures de référence spécifiques au PIMS (responsables de traitement)

Annexe B (normative) : Objectifs et mesures de référence spécifiques au PIMS (sous-traitants)

Annexe C (informative) : Correspondance avec l'ISO/IEC 29100

Annexe D (informative) : Correspondance avec le Règlement général sur la protection des données

Annexe E (informative) : Correspondance avec l'ISO/IEC 27018 et l'ISO/IEC 29151

Annexe F (informative) : Comment appliquer l'ISO/IEC 27701 à l'ISO/IEC 27001 et l'ISO/IEC 27002

Bibliographie

Lien : https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:fr

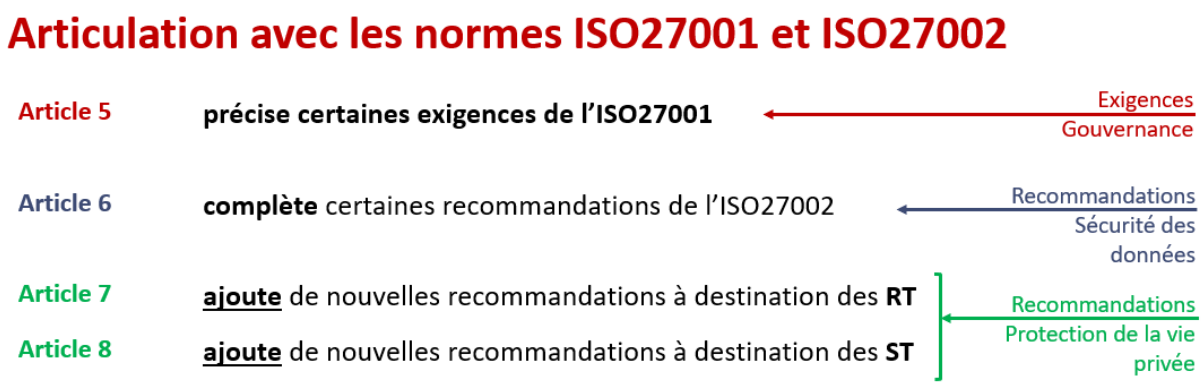
8 Comment la norme ISO 27701 s'articule-t-elle avec les normes ISO 27001 et ISO 27002 ?

La norme ISO27701 n'est pas autosuffisante. Elle s'adosse aux normes ISO27001 et ISO27002. Ainsi, pour avoir une lecture complète de la norme ISO27701 vous devez être en possession des trois documents.

Pour avoir une lecture complète du corpus documentaire il faut, dans le corps des normes ISO27001 et ISO27002, remplacer « sécurité de l'information » par « sécurité de l'information et protection de la vie privée ».

Au sein de la norme ISO27701 :

- l'article 5 précise certaines exigences de l'ISO27001 ;
- l'article 6 complète certaines recommandations de l'ISO27002 ;
- l'article 7 ajoute de nouvelles recommandations à destination des responsables de traitement ;
- l'article 8 ajoute de nouvelles recommandations à destination des sous-traitants.



Extrait de la présentation de la norme ISO27701 - GT RSSI-DPO du Clusif – Clusif

L'annexe F détaille l'articulation de l'ISO 27701 avec les normes ISO 27001 et 27002. Elle précise qu'il existe trois cas pour l'articulation :

- application des normes de sécurité en l'état avec l'extension des termes indiquée ci-dessus ;
- affinement des normes de sécurité par des exigences ou des recommandations spécifiques à la protection de la vie privée ;
- ajouts aux normes de sécurité avec des exigences ou des recommandations spécifiques à la protection de la vie privée.

9 La mise en place d'un PIMS garantit-elle ma conformité au RGPD ?

Non.

Elle permet de gérer la protection de la vie privée dans le cadre d'un système de management. Le périmètre d'un PIMS est un système de management et non des traitements de données personnelles. C'est donc une démarche qui est certifiée et non des traitements, un produit ou un service.

Il ne s'agit pas d'une certification prévue par le RGPD, notamment à son article 42.

Cependant, la mise en place d'un PIMS implique de :

- Identifier les exigences légales et réglementaires en matière de protection de la vie privée, ainsi que les recommandations des autorités de contrôle ;
- Assurer sa conformité à ces exigences et la prise en considération de ces recommandations pour tout traitement inclus dans le périmètre du PIMS.

De plus, les rédacteurs de la norme ont intégré les exigences du RGPD dans les recommandations complémentaires et supplémentaires ajoutées à la norme ISO27002.

Ainsi, si la certification d'un PIMS ne garantit pas la conformité au RGPD, elle reste un bon indicateur en terme *d'accountability* (art. 5 et 24 du RGPD) tant pour les clients et partenaires que pour les utilisateurs, les personnes concernées et pour les autorités de contrôle telles que la CNIL. Elle permet également d'intégrer les principes de *Privacy by design and by default* dans sa gestion des données à caractère personnel (art. 25 du RGPD).

10 La mise en place d'un PIMS me permet-elle d'intégrer les exigences du RGPD ?

Oui.

La mise en place d'un PIMS implique :

- d'identifier les exigences légales et réglementaires en matière de protection de la vie privée, ainsi que les recommandations des autorités de contrôle ;
- d'assurer sa conformité à ces exigences et la prise en considération de ces recommandations pour tout traitement inclus dans le périmètre du PIMS.

De plus, les rédacteurs de la norme ont intégré les exigences du RGPD dans les recommandations complémentaires et supplémentaires ajoutées à la norme ISO27002.

Plusieurs autorités de protection des données participent aux groupes de travail de l'ISO (Allemagne, France, Italie, Etats-Unis, Canada, Australie, …)

Les représentants de la CNIL préparent chaque session et y participent.

De nombreuses contributions sont déposées via la liaison officielle entre le CEPD (Comité européen de la protection des données) et l'ISO. L'objectif est d'intégrer les concepts européens dans les normes internationales.

Ainsi, la norme ISO 27701 est compatible avec les grands textes de protection des données personnelles, dont le RGPD.

L'annexe D détaille l'articulation de l'ISO 27701 avec le RGPD. Elle indique les correspondances indicatives avec les Articles 5 à 49 du RGPD (à l'exclusion de l'article 43 sur les Organismes de certification). Elle montre comment la conformité aux exigences et aux mesures de l'ISO 27701 peut être pertinente pour satisfaire aux obligations du RGPD. Cette annexe est purement indicative. Il incombe aux organisations d'évaluer leurs obligations légales et de décider comment s'y conformer.

11 La certification de mon PIMS est-elle une certification RGPD (art.42) ?

Non.

L'ISO 27701 a une portée mondiale et elle n'est pas spécifique au RGPD. Le RGPD (art.42) intègre la possibilité de certifications orientées « biens et services » plutôt que « système de management ». Les certifications entrant dans le cadre de l'article 42 devront être approuvées par l'autorité de contrôle compétente et/ou le CEPD.

L'ISO 27701 n'est pas une certification au sens de l'article 42 du RGPD mais :

- Elle présente l'état de l'art en protection de la vie privée ;
- Elle permet de monter en maturité et de démontrer une démarche active de protection des DCP ;
- Son système de management englobe les services et prévoit les PIA.

Rappel : Article 42 al.1 du RGPD : « *Les États membres, les autorités de contrôle, le comité et la Commission encouragent, en particulier au niveau de l'Union, la mise en place de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement. Les besoins spécifiques des micros, petites et moyennes entreprises sont pris en considération.* »

12 Le PIMS permet-il d'intégrer, de gérer les exigences légales et réglementaires étrangères en matière de protection des données personnelles ?

Oui.

La norme ISO 27701 a une portée internationale. Il revient à chaque organisme, lors de la mise en place du PIMS, d'identifier les exigences légales et réglementaires en matière de protection de la vie privée qui s'appliquent au périmètre du système de management et d'assurer leur conformité.

Ainsi, la norme fait régulièrement référence aux exigences des différentes juridictions qui doivent être identifiées et appliquées. Cependant, elle comporte moins de similitudes ou de « *pointeurs* » vers les autres textes que vers le RGPD.

13 Quelles sont les difficultés inhérentes au déploiement de mon PIMS ?

La certification ISO27001 est un prérequis.

Tout d'abord, l'implémentation d'un SMSI est un projet ambitieux et long (une année en moyenne). Il peut se révéler coûteux et doit donc avoir un véritable apport pour l'organisation. L'importance d'un tel projet doit être présentée, comprise et acceptée par la Direction.

Il nécessite d'impliquer l'ensemble des équipes entrant dans le périmètre (des décideurs aux utilisateurs finaux du système d'information). Ces équipes devront être régulièrement mobilisées pendant toute la durée du projet et au-delà.

Leur implication, accompagnée de la mise en place de procédures, de documentation et de traçabilité, peut être mal vécue par les équipes et perçue comme de la surveillance et une complication. La communication et le soutien de la direction sont donc primordiaux pour la réussite du projet. Trop souvent, un projet SMSI (comme PIMS) est perçu comme un projet documentaire. Or, la documentation ne doit être qu'un outil. Tout comme les processus, elle doit être basée sur l'existant et refléter la réalité des pratiques.

A ces difficultés, s'ajoutent celles propres au PIMS. Le PIMS est un projet hybride. Il nécessite des compétences organisationnelles, techniques et juridiques. De plus, l'implémentation et le maintien d'un PIMS nécessite de :

- Déterminer la qualification juridique de l'organisation (responsable de traitement, sous-traitant, co-responsable, destinataire, etc.) ;
- Gérer les deux statuts sur le périmètre du PIMS (mon organisation peut être à la fois responsable de traitement et sous-traitant sur le périmètre du PIMS) ;
- Identifier et gérer l'ensemble des exigences légales et réglementaires (tant européennes qu'internationales) en matière de protection de la vie privée ;
- Articuler le PIMS avec le SMSI ;
- Répondre aux attentes fortes des auditeurs en termes de conformité RGPD ;
- Réaliser l'appréciation des risques pour la sécurité de l'information et la protection de la vie privée.

14 Quels sont les acteurs d'un projet d'implémentation d'un PIMS ?

Un tel projet nécessite un Responsable du PIMS. Il n'est pas nécessairement le DPO (Data Protection Officer) ou le RSSI (Responsable de la Sécurité des Système d'Information). En effet, il doit avant tout avoir des compétences solides en gestion de projet et une parfaite connaissance des normes ISO27001, ISO27002 et ISO27701.

Le RPIMS travaille en collaboration étroite avec le DPO et le RSSI. Ces derniers pourront le seconder sur le volet « protection de la vie privée » et « sécurité des données ».

Comme indiqué précédemment, le PIMS est un projet ambitieux. Si l'organisation part de zéro, et doit également implémenter un SMSI, le RPIMS pourrait être un poste à plein temps ou mi-temps selon la maturité de l'organisation et les délais impartis. Le PIMS pourrait également consommer un tiers du temps du DPO et du RSSI.

La Direction est régulièrement sollicitée. En effet, son soutien est primordial. De plus, elle doit régulièrement valider des étapes projet et approuver ce qui est implémenté.

Les équipes du RSSI et du DPO seront également mobilisées.

Enfin, les différents responsables des équipes entrant dans le périmètre devront également participer au projet pour l'appréciation et le traitement des risques, la mise en place des processus et l'approbation, voire la rédaction, de la documentation et des procédures.

Le cas échéant, l'équipe conformité et/ou qualité sont un soutien important au RPIMS.

14.1 Quel est le rôle du DPO ?

Le DPO (*Data Protection Officer*) tient un rôle important dans la mise en place d'un PIMS.

S'il peut être RPIMS, cela ne doit pas être systématique. Le DPO ne devrait remplir ce rôle que s'il dispose du temps et des moyens nécessaires au déploiement d'un tel projet. Il devra également disposer des compétences nécessaires : connaissance des normes de la famille ISO2700X, des systèmes de management, gestion des risques et gestion de projet. Enfin, le DPO devra connaître les implications et enjeux d'un tel projet et en accepter formellement la responsabilité.

En tout état de cause, le DPO assistera le RPIMS dans la mise en œuvre du PIMS. Il jouera un rôle dans les principaux processus du PIMS. Il disposera des informations utiles concernant les traitements de données personnelles, la protection des données et la gestion des droits des personnes concernées. Il devra donner son avis sur l'essentiel des processus déployés, des mesures mises en place et des documents produits.

14.2 Quel est le rôle du RSSI ?

Tout comme le DPO, le RSSI (Responsable de la Sécurité des Systèmes d'Information) tient un rôle central dans le déploiement d'un PIMS. Comme le DPO, il peut être RPIMS s'il dispose des ressources nécessaires pour accomplir cette mission, notamment en termes de temps et de compétence, et s'il en accepte formellement la responsabilité.

Comme le DPO encore, il assistera le RPIMS dans la mise en place d'un PIMS. Son rôle sera central en matière de sécurité des données personnelles. Il apportera donc son soutien pour la définition du périmètre du PIMS, l'appréciation des risques sécurité et la mise en place des processus de gestion des mesures de sécurité.

Les rôles du DPO et du RSSI devraient être complémentaires dans le cadre d'un projet de PIMS, et plus généralement, pour assurer la protection des données personnelles. En effet, la synergie entre le RSSI et le DPO apparaît indispensable pour traiter globalement et totalement la sécurité du système d'information et des données personnelles.

15 Existe-t-il d’autres normes ISO dédiées aux données personnelles ?

Oui.

Il existe de nombreuses autres normes ISO dédiées à la protection de la vie privée. Elles sont présentées ici : https://clusif.fr/publications/les-normes-en-matiere-de-protection-des-dcp/

L‘AFNOR a également produit un document sur ces normes :

https://normalisation.afnor.org/wp-content/uploads/2017/02/AFNOR_Guide_Protection_des_donnees_perso_HD.pdf

Tour ERIA
5 Rue Bellini
92821 Puteaux Cedex
clusif@clusif.fr

clusif.fr