La norme ISO27701 pour l'implémentation d'un PIMS

Club 27001

Réunion parisienne

21 janvier 2021

Amélie PAGET
Consultante indépendante - Protection des données personnelles
Formatrice HS2

HS2
Hervé Schauer Sécurité

Norme ISO27701

Pour l'implémentation d'un PIMS

Amélie PAGET

Consultante indépendante

Protection des données personnelles

Formation et Conseil

Audit & Accompagnement

DPO externe & Adjoint DPO

Management de la protection des données

Sensibilisation & Formation

Apaget.consultant@gmail.com

Norme ISO27701

1. Norme ISO27701
2. Atouts de la norme
3. Articulation avec les autres normes ISO *Privacy*
4. Rapports avec le RGPD
5. Difficultés de mise en œuvre d'un PIMS

Norme ISO27701

1 & 2

La norme ISO27701 & ses atouts

Norme ISO27701

Présentation de la norme

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 27001and ISO/IEC 27002 for privacy information management – Requirements and guidelines

1ère édition 2019-08

En Anglais et en Français

80 pages (Fr)

Norme ISO27701

Présentation de la norme

Norme Internationale qui permet de :

- Intégrer les exigences et bonnes pratiques en matière de vie privée à un **système de management**
  - Processus documenté, pérenne, auditable ; amélioration continue
- **Certifier** un système de management de protection de la vie privée
  - Ou ***PIMS – Privacy Information Management System***
- Renforcer la confiance : **Atout business** pour les fournisseurs de produits et prestataires de services impliquant des DCP
- Offrir un parfait **outils de gouvernance** de la vie privée pour les DPO et une vision **opérationnelle**

Norme ISO27701

Présentation de la norme

Points de vigilance

La certification ISO27701 est un projet lourd

- *Repenser sa conformité sous l'angle de la gouvernance*
- *D'intégrer le volet conformité au SMSI*

La certification ISO27701 n'est pas une certification RGPD.

La certification ISO27001 est un prérequis pour certifier son PIMS

Ce n'est pas un projet juridique mais organisationnel

Il est impératif maîtriser les normes ISO27001 et ISO27002 pour manier l'ISO27701

Norme ISO27701

Présentation de la norme

Extension des normes ISO27001 et ISO27002

- Apporte des **spécifications aux exigences de l'ISO27001**
- Ajoute des **recommandations spécifiques et supplémentaires aux mesures de l'ISO27002**
- Implique un **SMSI** sur l'ensemble du périmètre du **PIMS**
  - Mais pas nécessairement un périmètre confondu
- S'adresse à tout type d'organisme
  - Privé ou public,
  - **Responsable de traitement** et **Sous-traitant**

Structure du document

Respecte le HLS (*High Level Structure*) des normes ISO dédiées aux systèmes de management

- 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'ISO27001
6. **Recommandations spécifiques au PIMS** liées à l'ISO27002
7. **Recommandations supplémentaires pour les RT**
8. **Recommandations supplémentaires pour les ST**

- Annexes

Structure du document

Annexes

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

Norme ISO27701

Présentation de la norme

Articulation avec les normes ISO27001 et ISO27002

Dans le corps des normes ISO27001 et ISO27002

- Remplacer « sécurité de l'information »
  - par « **sécurité de l'information et protection de la vie privée** »

Article 5	**précise** certaines exigences de l'ISO27001
Article 6	**complète** certaines recommandations de l'ISO27002
Article 7	**ajoute** de nouvelles recommandations à destination des **RT**
Article 8	**ajoute** de nouvelles recommandations à destination des **ST**

Norme ISO27701

Présentation de la norme

Articulation avec les normes ISO27001 et ISO27002

Article 5 **précise** certaines exigences de l'ISO27001

Article 6 **complète** certaines recommandations de l'ISO27002

Article 7 **ajoute** de nouvelles recommandations à destination des **RT**

Article 8 **ajoute** de nouvelles recommandations à destination des **ST**

Exigences
Gouvernance

Recommandations
Sécurité des données

Recommandations
Protection de la vie privée

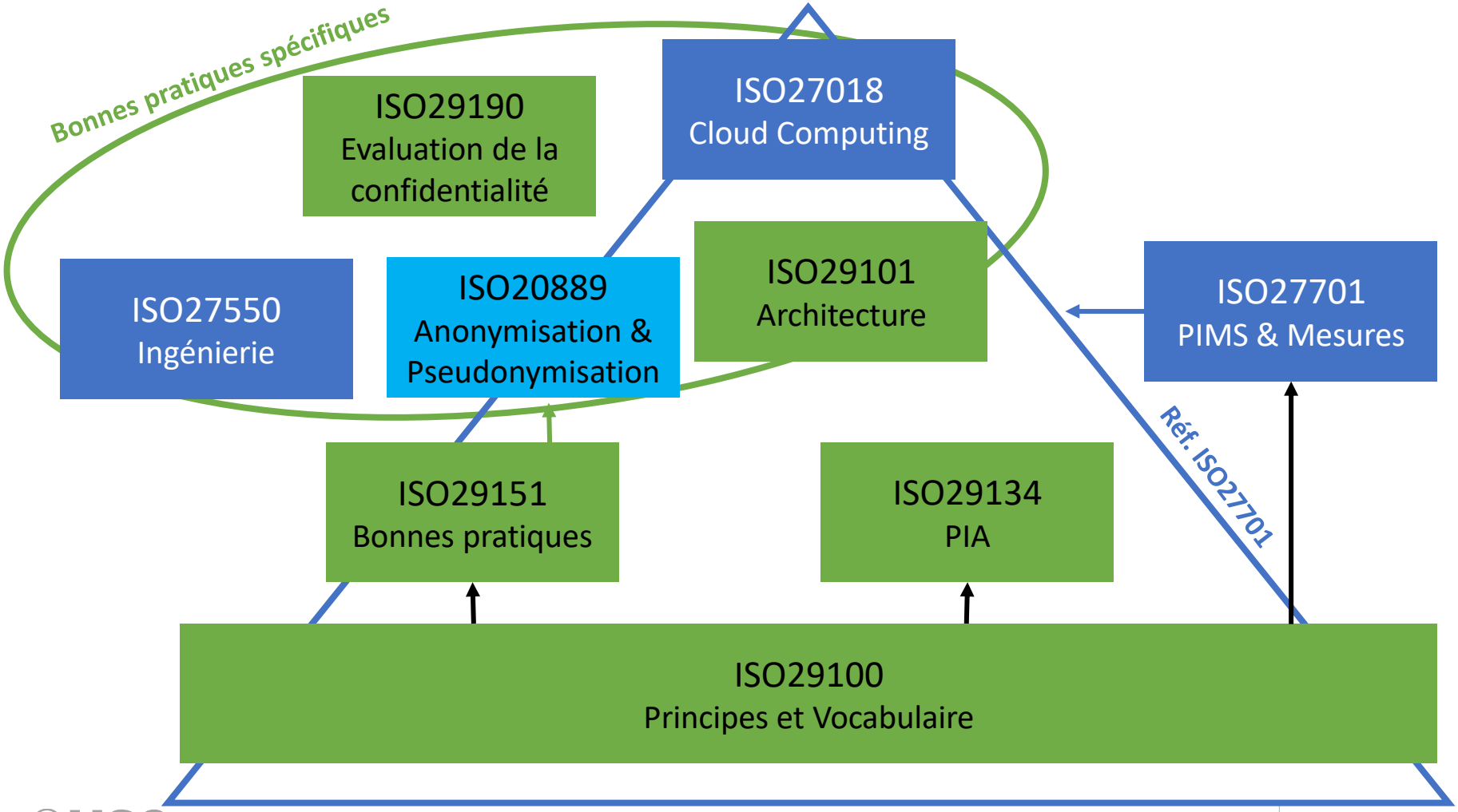
Norme ISO27701

3 & 4

Articulation avec les autres normes & le RGPD

Norme ISO27701

Articulation avec les autres normes Vie Privée



Norme ISO27701

Articulation avec les autres normes Vie privée

Quid de la norme ISO27018

ISO/IEC 27018:2014

Technologies de l'information — Techniques de sécurité

Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

- Déclinaison des normes :
  - ISO 17788 (cadre et vocabulaire du *Cloud*),
  - ISO 27002 (bonnes pratiques de sécurité de l'information)
  - ISO 29100 (principes de protection de la vie privée).
- Mesures recommandées pour un fournisseur de *cloud computing* hébergeant des DCP pour le compte d'un RT
- Ne traite pas de la gouvernance chez l'hébergeur

Norme ISO27701

Articulation avec les autres normes

Quid de la norme ISO27018

La norme ISO27701 :

- **Reprend le contenu** de la norme ISO27018 à son article 8 consacré aux sous-traitants
- **Met à jour** les dispositions de l'ISO27018
- Est d'application **plus large** que la norme ISO27018

La norme ISO27018 va-t-elle :

- Être absorbée par l'ISO27701 et devenir caduque ?
- S'articuler avec l'ISO27701 ?

Norme ISO27701

Articulation avec le RGPD

- Plusieurs autorités de protection des données ont participé aux groupes de travail de l'ISO :
  - Allemagne, France, Italie, Etats-Unis, Canada, Australie, Asie…
  - Les experts de la **CNIL** participent à chaque session.

- De nombreuses contributions ont été déposées via la liaison officielle entre le **CEPD** et l'ISO :
  - L'objectif est d'intégrer les concepts européens dans les normes internationales.

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

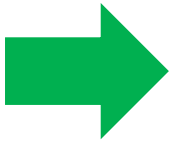
Norme ISO27701

Articulation avec le RGPD

- L'organisme de normalisation européen (**CEN/CLC**) dispose d'un groupe de travail dédié « vie privée » :
  - Adoption de la norme ISO 27701 au niveau européen
  - Volonté de travailler avec le CEPD et ses membres, notamment sur les critères de certification du RGPD (art. 42)

- Il y a une concordance de **vocabulaire** entre l'ISO27701, l'ISO29100 et le RGPD.

- L'ISO27701 est soumise à une enquête publique pour devenir une **norme française homologuée (NF)**



Vers une certification RGPD s'appuyant sur la norme ISO27701 ?

Norme ISO27701

Articulation avec le RGPD

L'annexe D - Articulation ISO 27701 & RGPD

- Correspondance indicative avec les Articles 5 à 49 du RGPD.
  - à l'exclusion de l'article 43 sur les Organismes de certification
- Montre comment la conformité aux exigences et aux mesures de l'ISO 27701 **peut être pertinente** pour satisfaire aux obligations du RGPD.

Purement indicatif : conformément aux articles de l'ISO 27701, il incombe aux organisations d'évaluer leurs obligations légales et de décider comment s'y conformer.

Norme ISO27701

Articulation avec le RGPD

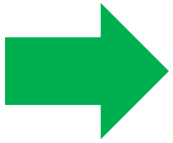
Et la certification RGPD ?

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 »

⇨ L'ISO 27701 n'est pas une certification au sens Art.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
- La CNIL et le CEN réfléchissent à son adaptation au cadre de l'Art.42



Une certification RGPD pourrait s'appuyer sur un système de management certifié ISO27701.

Norme ISO27701

Articulation avec le RGPD

Les atouts de la norme pour sa conformité au RGPD

- Adopter une démarche de **gouvernance** de la protection de la vie privée
  - Approche systématique
  - Processus pérenne
  - Documentation et traçabilité
  - Surveillance et amélioration continue
- Intégrer les **exigences légales et réglementaires** applicables en matière de protection de la vie privée
- Répondre au principe d'***Accountability***

Norme ISO27701

5

Les difficultés à l'implémentation d'un PIMS

Norme ISO27701

Les difficultés à l'implémentation d'un PIMS

1. La qualification de l'organisme
   - Ses rôles et responsabilité : RT, Co-RT ou ST
2. L'intégration à l'existant
3. La documentation
4. L'appréciation des risques
5. L'appréhension des articles 7 et 8 de la normes
   - Volet « juridique »

Norme ISO27701

Les difficultés à l'implémentation d'un PIMS

La qualification

Définir des rôles et responsabilités de l'organisme sur le périmètre du PIMS

- **Responsable de traitement, Co-responsable ou Sous-traitant ?**
- Ne pas s'emmêler dans la sélection des mesures
- Bien penser son périmètre pour limiter cette complexité

L'intégration à l'existant

Articulation du PIMS avec le SMSI

- **Les périmètres sont-ils confondus ?**
  - Oui : possibilité de refondre les processus et la documentation existante pour intégrer les exigences et mesures liées au PIMS.
  - Non : créer une extension des processus et de la documentation existante avec un système de renvoi.
    - Le PIMS est un SMSI amélioré sur un périmètre restreint.

Norme ISO27701

Les difficultés à l'implémentation d'un PIMS

La documentation

- L'implémentation d'un PIMS induit une forte documentation en matière de gestion des DCP. Et d'enrichir la documentation liée au SMSI
  - **Trouver le juste milieu** entre :
    - Trop de documentation, trop de détail, trop théorique
    - Et pas assez de documentation et de traçabilité pour assurer la pérennité du SM et satisfaire les auditeurs

Norme ISO27701

Documentation exigée par la norme

- **Domaine d'application du PIMS**
- **Politique de sécurité de l'information et de protection de la vie privée**
- **Objectifs liés à la sécurité de l'information et à la protection de la vie privée**
- Informations sur le processus d'AdR et de PTR
- **DdA**
- **PTR**
- Résultats des processus d'AdR et PTR
- Documents de preuve des compétences des personnels
- Information permettant d'avoir l'assurance que les processus ont été suivis comme prévus
- Preuves des résultats de la surveillance et des mesures
- Preuves de mise en œuvre des programmes d'audit et les résultats d'audit
- Nature des non-conformités et de toute action subséquente
- Résultats des actions correctives
- **Résultats des revues de direction**
- Informations que l'organisation juge nécessaires à l'efficacité du PIMS

Norme ISO27701

Documentation liée à la protection des DCP

- Fiche de poste et **Désignation du DPO**
- Cartographie des données
- Cartographie des flux
- **Registre des traitements**
- Etudes préalables et **PIA** (AIVP)
- Procédure de gestion des violations de données
- **Documentation des violations de données**
- Procédure de gestion des droits
- Liste des sous-traitants et co-responsables, **contrats et accords** associés
- **Documentation liées aux transferts hors UE**
- **Mentions légales d'information des personnes**
- Enregistrements liés au consentement
- Documentation liée à la sensibilisation du personnel
- Bilan annuels du DPO

L'appréciation des risques

2 volets :

- Appréciation des risques de sécurité de l'information
- Appréciation des risques sur la vie privée

& **2 échelles** : évaluer les conséquences potentielles :

- pour l'organisation
- pour les personnes concernées

Qu'est que le risque sur la vie privée ?

Notion de risque sur la vie privée

- Pas d'impact DIC(A)
- Mais des atteintes aux principes fondamentaux de la protection de la vie privée

Exemple :
- Atteinte aux principes fondamentaux de transparence des traitements, de minimisation des données
- Atteinte aux droits des personnes concernées tel que le droit d'accès, de rectification ou à l'effacement

Comment apprécier le risque sur la vie privée ?

- Pas d'impact en DIC sur les DCP.
- Mais des **atteintes aux principes fondamentaux**.

- Des **conséquences potentielles** pour l'**organisation**
- Et des **conséquences potentielles** pour les **PC**

- La **vraisemblance** dépend peu de la facilité d'exploitation.
- Eventuellement de la **probabilité d'occurrence**.

Est-ce pertinent d'apprécier les risques sur la vie privée ?

Norme ISO29134 (6.4.4.1 NOTE)

Identification des risques :

> « *Ces possibilités de non-application ou d'application incorrecte des droits fondamentaux ne peuvent qu'être vérifiées et améliorées. Il est en effet impossible de ne pas appliquer ces droits fondamentaux.* »

(6.4.3, 7.4 et 7.5.5)

Prévoit un volet dédié à l'Analyse de la conformité

Outils PIA CNIL

Le volet « Principes fondamentaux »

- Ne fait pas l'objet d'une appréciation/valorisation
- Description des moyens mis en œuvre pour respecter les principes

Comment apprécier un risque lié à une non-conformité ?

1. Je ne valorise pas.
   - **Choix binaire** : Soit ma pratique est conforme soit elle ne l'ai pas.

1. Je valorise.
   - Notamment en fonction des conséquences pour les droits et libertés des personnes.
   - Permet de prioriser les non-conformités et de faciliter mes choix à venir dans le cadre du Plan de traitement des risques.
     - Exemple :

Conforme	Remarques	NC Mineures	NC Majeures

Norme ISO27701

Les difficultés à l'implémentation d'un PIMS

Quid du scénario d'incident pour les risques sur la vie privée ?

S'éloigner du concept

Proposition

- Mesures de protection de la vie privée existantes
- Atteintes aux principes fondamentaux constatés
- Traitements de DCP impactés
- Référence Légale et Réglementaire
- Non-conformité

Mesures de protection de la vie privée existantes	Mise en ô	Atteintes constatées	TDCP impactés	Réf. LR & N	NC

Conséquences pour les personnes concernées

Exemple d'échelle (inspirée des outils de la CNIL)

Niveau	Conséquences sur les personnes concernées
1-Insignifiant	Les PC ne seront pas affectées ou pourraient rencontrer quelques inconvénients mineurs (perte de temps , simple contrariété…)
2-Limité	Les PC pourraient rencontrer des inconvénients qu'elles seraient capables de surmonter sans difficulté (complexification de démarches administratives, frais mineurs, …) Peut avoir conséquences insignifiantes pour un nombre massif de PC
3-Signifiant	Les PC pourraient subir des conséquences significatives qu'elles seraient capables de surmonter mais avec difficultés (frais supplémentaires, refus d'accès à des prestations commerciales, peur, affection physique ou psychologique mineure, etc...) Peut avoir conséquences limitées pour un nombre massif de PC
4-Maximum	Les PC pourraient rencontrer des conséquences significatives, voire irréversibles ou insurmontables (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, affection physique ou psychologique grave…) Peut avoir conséquences signifiantes pour un nombre massif de PC

Appréhension des articles 7 et 8 de la norme

Ils permettent de couvrir l'essentiel des exigences légales et réglementaires européennes en matière de protection des DCP.

Implique :

- Des compétences juridiques, en tout état de cause, en protection des DCP
- Une culture du risque et du système de management adaptée à la conformité

L'implémentation d'un PIMS n'est pas un projet juridique

Norme ISO27701

Présentation de l'article 7 - RT

Rappel des principales exigences du RGPD

6 principes fondamentaux
Licéité, loyauté et transparence
Limitation des finalités
Minimisation des données
Exactitude des données
Limitation des durées de conservation
Intégrité et confidentialité des données

Gouvernance de la protection
Qualification de l'organisme
Désignation d'un DPO (rôles et responsabilité)
Privacy by design & by default
PIA (Gestion de projet)
Gestion des partenaires
Gestion des transferts de données
Accountability
Registre des traitements (gestion de la documentation)

Droits des personnes concernées
Droit à l'information
D'accès
De rectification et de retrait du consentement
De rectification
D'opposition
A l'effacement
A la limitation
À la portabilité
De ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé

Norme ISO27701

Présentation de l'article 7

6 principes fondamentaux

Licéité, loyauté et transparence	7.2.2 Identifier le fondement juridique 7.2.3 Déterminer quant et comment le consentement doit être obtenu 7.2.4 Obtenir et enregistrer le consentement
Limitation des finalités	7.2.1 Identifier et documenter la finalité
Minimisation des données	7.4.1 Limiter la collecte 7.4.2 Limiter le traitement 7.4.4 Objectifs de minimisation des DCP
Exactitude des données	7.4.3 Exactitude et qualité
Limitation des durées de conservation	7.4.5 Dé-identification et suppression des DCP à la fin du traitement 7.4.6 Fichiers temporaires 7.4.7 Conservation 7.4.8 Mise au rebut
Intégrité et confidentialité	6.2 à 6.14

Norme ISO27701

Présentation de l'article 7

Gouvernance de la protection des données

Qualification de l'organisme	5.2.1 Compréhension de l'organisation et de son contexte
Désignation d'un DPO	6.3.1.1 Fonctions et responsabilités liées à la sécurité de l'information
Privacy by design & by default	7.4 Protection de la vie privée dès la conception et protection de la vie privée
Gestion des partenaires	7.2.6 Contrats conclus avec les sous-traitants 7.2.7 Responsable conjoint de traitement
Gestion des transferts de données	7.4.9 Mesures de transmission des DCP 7.5 Partage, transfert et divulgation des DCP
Accountability	Le PIMS
Registre des traitements	7.2.8 Enregistrements liés au traitement des DCP
PIA	7.2.5 Etude de l'impact sur la vie privée

Norme ISO27701

Présentation de l'article 7

Droits des personnes concernées

Droit à l'information	7.3.2 Déterminer les informations destinées aux personnes concernées 7.3.3 Fournir des informations aux personnes concernées
D'accès	7.3.6 Accès, rectification et/ou suppression 7.3.7 Obligation d'information des tiers des RT de DCP 7.3.8 Fourniture de copies des DCP traitées
De rectification	
A l'effacement	
De rectification et de retrait du consentement	7.3.4 Fournir un mécanisme permettant de modifier ou de retirer le consentement
D'opposition	7.3.5 Fournir un mécanisme permettant de s'opposer au traitement des DCP

Droits des personnes concernées

A la limitation	X
À la portabilité	7.3.8 Fourniture de copies des DCP traitées
De ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé	7.3.10 Prise de décision automatisée
Gestion globale des droits	7.3.9 Gestion des demandes

Norme ISO27701

Présentation de l'article 8 - ST

Les obligations à la charge des sous-traitants

(Art. 8)

- Contenu du contrat client
- Respect des finalités
- Utilisation à des fins de prospection et de publicité
- Appréhension des instructions illicites
- Assistance au client
- Enregistrements liés au traitement (Registre)
- Gestion des métadonnées
- Restriction, transfert et mise au rebu des DCP
- Sécurité lors des transmissions de DCP
- Gestion des partage, transfert et divulgation des DCP

Les recommandations de l'art. 6 s'appliquent également aux sous-traitants

Norme ISO27701

Conclusion

Ce qu'il faut retenir

Ce qu'il faut retenir

- ✓ Une norme qui a de l'avenir
  - Atout business,
  - Certification internationalement reconnue
  - Vers une certification RGPD ?
- ✓ Permet une approche par le risque et d'intégrer la gouvernance
  - ***Accountability***
- ✓ Offre des billes opérationnelles pour appréhender la protection de la vie privée

Norme ISO27701

Conclusion

Ce qu'il faut retenir

- La **certification ISO27001** est un prérequis
- Difficile articulation entre le SMSI et le PIMS
- La certification ISO27701 porte sur un **système de management**
  - et pas un service, ni un produit ni même un traitement de DCP
- Ce n'est **pas une certification RGPD**.
- La qualification de l'organisme est primordiale
  - Responsable de traitement, co-responsable, sous-traitant ?
- L'appréciation des risques est complexe
- L'implémentation d'un PIMS et la certification ne sont **pas un projet juridique**

Merci

Club 27001

Réunion Parisienne

21 janvier 2021

Amélie PAGET

Apaget.consultant@gmail.com

HS2

Hervé Schauer Sécurité