Fichiers perdus, volés, piratés… Pour éviter un drame et anticiper le nouveau règlement européen sur la protection des données personnelles, des outils existent !

Guide

PROTECTION des DONNÉES PERSONNELLES : L'APPORT DES NORMES VOLONTAIRES

Avril 2018

afnor NORMALISATION

SOMMAIRE

1 INTRODUCTION 3

2 OBJECTIF 5

3 APPROCHE PAR LES RISQUES 6

4 TERMINOLOGIE 8

5 RAPPELS SUR LE CADRE LÉGAL 11

5.1 Europe et France 11
5.2 Principes fondamentaux 12
5.3 Focus sur l'obligation de sécurité 13

6 DES NORMES VOLONTAIRES POUR RÉPONDRE AUX ENJEUX RÉGLEMENTAIRES 14

6.1 Connaître la terminologie et les principes 15
6.2 Mettre en place un système de management prenant en compte la protection de la vie privée 16
6.3 Comprendre comment mener une analyse d'impact 17
6.4 Disposer de bonnes pratiques génériques 18
6.5 Disposer de bonnes pratiques spécifiques au cloud computing 18
6.6 Disposer de référentiels techniques 19
6.7 Connaître les techniques de dé-identification 19

7 CONCLUSION 20

Ce document a été élaboré par la commission de normalisation AFNOR Sécurité des systèmes d'information (CN-SSI)



INTRODUCTION

En 2017, Equifax a révélé avoir été victime d'un piratage de données personnelles très sensibles (notamment bancaires) liées à plus de 145 millions d'Américains. Les faits sont là : dans un monde interconnecté, les informations propres aux clients peuvent rapidement tomber dans les mains des pirates de la Toile. Vigilance et réactivité sont donc de mise. Et obligatoires : un nouveau règlement européen sur la protection des données personnelles entrera en application en mai 2018. Pour s'y conformer au plus vite et protéger leur système informatique contre les menaces, les organisations ont à leur disposition divers outils. Dont certains, insoupçonnés, sont inventés par les organisations elles-mêmes, par consensus après concertation : les normes volontaires.

Les normes volontaires peuvent concerner divers profils ou métiers qui collaborent aux projets, responsables de traitements comme sous-traitants. Par exemple, pour un chef de projet, un juriste ou un responsable des achats, l'application d'une norme par un sous-traitant représente une assurance que les engagements contractuels du prestataire sont conformes à l'état de l'art et que leur réalité opérationnelle peut être vérifiée dans le cadre des audits de conformité. Par ailleurs, le législateur européen et les autorités de contrôle considèrent désormais que la responsabilisation des organisations (notion d'« *accountability* » en anglais) doit devenir la pierre angulaire de la protection de la vie privée. L'approche préconisée consiste à mettre en œuvre des mesures pour satisfaire aux exigences légales ou réglementaires et à être en capacité d'en rendre compte.

Dans ce contexte, l'organisation internationale de normalisation (ISO) et la commission électrotechnique internationale (IEC) jouent un rôle déterminant. Et c'est grâce à l'engagement et aux compétences des professionnels qui apportent leurs connaissances au comité technique commun pour la sécurité des technologies de l'information dénommé (JTC 1/SC 27). Un groupe de travail est d'ailleurs dédié à la protection des données personnelles (WG 5 du SC 27). L'un des objectifs de ce groupe de professionnels est de faire en sorte que les normes volontaires puissent efficacement contribuer à la mise en œuvre de solutions pour protéger les données personnelles et la vie privée.

1. INTRODUCTION

« *Demain, ces normes seront incontournables pour mettre en place un système de management en sécurité informatique, cadre de progrès qui devra notamment intégrer la protection des données personnelles* », soutient Matthieu Grall, chef du service de l'expertise technologique de la CNIL[1], organisme qui a participé au groupe de travail d'AFNOR Normalisation à l'origine du présent guide.

Ces solutions doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur réalisation, un niveau de sécurité adapté au regard des risques présentés par les traitements de données à caractère personnel et de la nature de ces données. Le groupe a ainsi pris en compte l'environnement réglementaire européen. Il faut souligner que les autorités de contrôle européennes, par l'intermédiaire d'une liaison avec le Groupe de l'Article 29[2], sont très impliquées dans l'élaboration de ces normes internationales.

Pour répondre à ces enjeux, zoom sur 6 catégories de normes (détail page 15) :

- Terminologie et principes
- Lignes directrices pour mener des analyses d'impacts relatives à la protection des données
- Maturité dans les processus
- Bonnes pratiques génériques pour la protection de la vie privée
- Bonnes pratiques de protection de la vie privée spécifiques au cloud computing
- Techniques de cryptographie
- Techniques de dé-identification

1. Commission nationale de l'informatique et des libertés.
2. http://ec.europa.eu/justice/data-protection/article-29/index_fr.htm



OBJECTIF

Ce document a été élaboré pour répondre à 4 objectifs :

- Mieux appréhender l'éventail des normes en matière de protection de la vie privée et les garanties qu'elles présentent. Il doit notamment permettre à une organisation, publique ou privée, quelle que soit sa taille, de se repérer dans le paysage des normes internationales ISO et de positionner ces normes en fonction du cadre légal et réglementaire qui lui est applicable.
- Permettre aux divers fonctions ou métiers qui collaborent sur des projets de traitement (système d'information, juridique, marketing, responsable d'audit, conformité, etc.) de trouver des références normatives applicables pour leur activité. Souvent réservées aux techniciens informatiques et aux ingénieurs, les normes deviennent désormais des référentiels incontournables pour tous les métiers et ce afin d'appréhender au mieux des environnements informatiques de plus en plus complexes (informatique en nuage ou *cloud computing*, technologies mobiles, etc.).
- Contribuer à un processus d'information, d'aide à la décision et de responsabilisation.
- Expliquer comment les normes volontaires ISO pour la sécurité de l'information et la protection de la vie privée, apportent des réponses aux exigences légales et sociétales en matière de protection des données à caractère personnel.



APPROCHE PAR LES RISQUES

L'approche préconisée dans ce document est basée essentiellement sur la gestion des risques. Elle s'avère, en effet, la plus cohérente par rapport aux fondements de la réglementation, qui garantit les droits fondamentaux des personnes dont les données sont traitées et repose sur les mesures à mettre en œuvre par les responsables de traitement et les sous-traitants afin d'empêcher toute atteinte aux dits droits. La sécurité de l'information, au sens de la série de normes ISO/IEC 2700x, et la protection de la vie privée, au sens du règlement 2016/679[1]), sont ici imbriquées. L'objectif est en effet de protéger à la fois l'organisme et les personnes concernées contre les risques liés aux traitements de leurs données, dans le respect des droits des personnes.

Au-delà du respect des principes fondamentaux de protection de la vie privée (information des personnes, obtention de leur consentement, droit d'accès, droit de rectification…), qui sont « non négociables », une approche par les risques, qui vise à déterminer des mesures proportionnées, s'inscrit dans un processus itératif d'amélioration continue de la sécurité et de la protection des données personnelles. Les données sont prises en compte sur l'ensemble de leur cycle de vie.

Ainsi, il convient de mettre en œuvre une approche par les risques dès le démarrage des projets et avant les phases de développement et d'intégration (notion de « *Privacy by design* » ou de « *Privacy by default* »). Cependant, si le traitement est déjà opérationnel, les méthodes proposées dans ce

1. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

document peuvent également s'appliquer. Si les risques identifiés sont trop importants et que les mesures de sécurité sont impossibles à mettre en œuvre, l'arrêt du service est envisageable.

Au-delà du contexte légal, il est important que l'organisation définisse une ambition permettant de traiter la protection de la vie privée comme une opportunité pour le développement de ses activités. En cohérence avec l'approche par les risques, la définition de l'ambition s'appuie sur le fait que chaque fois qu'il y a un conflit entre une organisation souhaitant effectuer un traitement et une personne concernée par ce traitement, la législation tend à privilégier la protection de la personne[1]). Protéger les données personnelles équivaut à protéger la personne contre l'usage abusif et l'utilisation frauduleuse de ses données personnelles. Ainsi, l'objectif de la protection de la vie privée est de permettre à la personne concernée de garder la maîtrise de ses données personnelles.

1. cf. article 1er de la loi n°78-17.



TERMINOLOGIE

Comment se faire comprendre et être compris dans une société où les technologies évoluent sans cesse, où de nouveaux marchés se développent… ? Les normes volontaires sur la « terminologie » permettent de donner une définition claire, précise et adaptée à tout type de secteur, marché ou thématique afin que chacun puisse parler le même langage. Les définitions décrites dans les normes sur la terminologie sont devenues indispensables pour les échanges internationaux, les traductions…

Voici quelques définitions utiles aux acteurs concernés par la protection des données à caractère personnel :

Donnée à caractère personnel ou donnée personnelle[1]

Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociales[2].

1. Dans ce document, les termes « donnée personnelle » et « donnée à caractère personnel » (DCP) sont synonymes. Leur définition correspond également à celle de « PII » correspondant aux termes anglais de « *Personally Identifiable Information* ».
2. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. (considérant 26 du règlement 2016/679).

Analyse d'impact relative à la protection des données, ou Privacy Impact Assessment (PIA)

Selon le règlement 2016/679, « *une analyse d'impact relative à la protection des données devrait être effectuée par le responsable du traitement, préalablement au traitement, en vue d'évaluer la probabilité et la gravité particulières du risque élevé, compte tenu de la nature, de la portée, du contexte et des finalités du traitement et des sources du risque. Cette analyse d'impact devrait comprendre, notamment, les mesures, garanties et mécanismes envisagés pour atténuer ce risque, assurer la protection des données à caractère personnel et démontrer le respect du présent règlement* ».

Privacy by design

Principe selon lequel la protection des données personnelles et la protection de la vie privée sont considérées dès la conception des produits ou des services.

Privacy Enhancing Technologies (PET)

Technologies de protection de la vie privée.

Responsable de traitement

Selon l'article 4 du règlement 2016/679 le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. En d'autres termes, le responsable de traitement est celui qui va décider de mettre en œuvre un traitement de données personnelles pour une finalité donnée (ex. traitement RH, messagerie d'entreprise, fichiers clients et prospects, etc.) avec ses propres ressources informatiques ou en recourant à celles d'un prestataire tiers

Note 1 La validation de la manière dont les risques ont été traités, ainsi que l'acceptation des risques résiduels (qui subsistent après application de mesures), relèvent de la responsabilité du responsable de traitement.

Note 2 Dans la version en anglais du règlement 2016/679, le responsable de traitement est appelé « *controller* ».

Sous-traitant

Il s'agit de la personne ou l'entité à laquelle le responsable de traitement délègue la réalisation du traitement (infogérant, prestataire de Cloud, etc.)

Note 1 Au regard de l'article 28 du règlement 2016/679, les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement. Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens du réglement.

Note 2 Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité mentionnées à l'article 32. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement. Dans la version en anglais du règlement 2016/679, le sous-traitant est appelé « *processor* ».

Personne concernée

Selon l'article 4 du règlement 2016/679, la personne concernée est une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociales.

Autorité de contrôle

Selon l'article 51 du règlement 2016/679, chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application du règlement, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union.

En France, l'autorité de contrôle en charge de la protection des données personnelles est la Commission nationale de l'informatique et des libertés (CNIL).

Le comité européen de la protection des données

Le comité européen de la protection des données est institué par l'article 68 du règlement. Le comité se compose du chef d'une autorité de contrôle de chaque État membre et du contrôleur européen de la protection des données, ou de leurs représentants respectifs. Ce Groupe succède au Groupe de l'Article 29 (G29) tel que défini par l'article 29 de la Directive 95/46/CE.

Fournisseur de solutions

Le fournisseur de solutions apporte des mesures techniques (solutions appelées aussi Privacy Enhancing Technologies, en anglais) ou organisationnelles pour la protection des données personnelles. Il accompagne le responsable de traitement dans la conception privacy by design ; et fournit de l'expertise dans le domaine des normes pour la protection des données personnelles (formateurs, consultants, organismes de certification…).

Note La CNIL définit les parties prenantes dans la création ou l'amélioration de traitement de données personnelles de la façon suivante :

- les responsables de traitements, qui peuvent avoir à justifier auprès de la CNIL des mesures qu'ils ont choisies de mettre en œuvre dans leurs systèmes ;
- les maîtrises d'ouvrage (MOA), qui doivent apprécier les risques pesant sur leur système et donner des objectifs de sécurité ;
- les maîtrises d'œuvre (MOE), qui doivent proposer des solutions pour traiter les risques conformément aux objectifs identifiés par les MOA ;
- les correspondants « informatique et libertés » (CIL), qui doivent accompagner les MOA dans la protection des données personnelles ;
- les responsables de la sécurité des systèmes d'information (RSSI), qui doivent accompagner les MOA dans le domaine de la sécurité des systèmes d'information (SSI).



RAPPELS SUR LE CADRE LÉGAL

5.1 Europe et France

En Europe, le traitement des données personnelles et leur libre circulation fait l'objet du **règlement général sur la protection des données 2016/679 (RGPD), qui remplace la Directive 95/46**. Les principales évolutions par rapport à la Directive sont les suivantes :

- les entreprises seront davantage responsabilisées au travers du principe d'« *accountability* », imposant de se mettre en conformité et de pouvoir le démontrer ;
- selon les enjeux des projets, et notamment la nature des données traitées, il conviendra en outre de consulter préalablement l'autorité de protection des données et de mener une analyse d'impact relative à la protection des données ;
- des mécanismes visant à garantir la protection des données par défaut ou dès la conception (notions de Privacy by design et de Privacy by default) devront être mis en œuvre ;
- un délégué à la protection des données devra être désigné dans certains cas ;
- les « violations de données à caractère personnel » devront être notifiées à l'autorité de protection des données et selon les cas, aux personnes concernées ;

- les sanctions se mesureront en % du chiffre d'affaire mondial consolidé (selon les cas avertissement privé ou public, sanction financière avec un maximum de 20 M€ d'amende ou 4 % du chiffre d'affaire mondial consolidé, injonction de cesser le traitement) ;
- les droits des personnes seront renforcés et étendus (ex : droit à la portabilité).

En France, la loi n°78-17, couramment appelée loi « Informatique et libertés », va être adaptée au réglement européen.

5.2 Principes fondamentaux

Conformément au cadre légal et réglementaire de protection de la vie privée, un traitement automatisé de données doit respecter cinq principes fondamentaux :

- **principe de finalité :** les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime. Par exemple, un traitement utilisant un outil de géolocalisation ne peut avoir pour objet d'espionner les personnes concernées. En outre, la finalité du traitement ne doit pas être détournée (par exemple, un réseau social d'entreprise ne doit pas être utilisé à des fins publicitaires) ;
- **principe de proportionnalité et de pertinence des données :** seules doivent être traitées les informations pertinentes et nécessaires au regard des objectifs poursuivis ;
- **principe d'une durée de conservation des données limitée :** les informations ne peuvent être conservées indéfiniment. La durée de conservation doit être précise et déterminée ;
- **principe de sécurité des données :** le responsable de traitement doit prendre les mesures nécessaires pour traiter les risques d'accès illégitime, de modification non désirée et de disparition de données à caractère personnel, de manière proportionnée ;
- **principe du respect des droits de la personne :** ce principe se décompose essentiellement comme suit :
  - **droit à l'information :** toute personne a un droit de regard sur ses propres données. Par conséquent, quiconque met en œuvre un fichier ou un traitement de données personnelles est obligé d'informer les personnes fichées de son identité, de l'objectif de la collecte d'informations et de son caractère obligatoire ou facultatif, des destinataires des informations, des droits reconnus à la personne, des éventuels transferts de données vers un pays hors de l'Union Européenne ;
  - **droit d'accès :** toute personne peut prendre connaissance de l'intégralité des données la concernant dans un fichier en s'adressant directement à ceux qui les détiennent, et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction ;
  - **droit d'opposition :** toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier, et peut refuser sans avoir à se justifier, que les données qui la concernent soient utilisées à des fins de prospection commerciale ;
  - **droit de rectification :** toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations la concernant lorsqu'ont été décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.
  - **droit à la portabilité :** Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement,

dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle sous les conditions décrites à l'Article 20 du RGPD.

Pour connaître l'ensemble des droits de la personne (notamment droit à la portabilité), se référer au chapitre III du règlement 2016/679.

5.3 Focus sur l'obligation de sécurité

Le règlement 2016/679 stipule dans son article 32 que « *compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ».

Le règlement 2016/679 prévoit des sanctions considérables en cas de manquements à ces obligations.

Au-delà de cet aspect contraignant, il y va finalement de l'intérêt même des entreprises. Protéger son patrimoine numérique est une nécessité pour une entreprise, par rapport à la valeur des informations personnelles bien sûr, mais aussi pour des raisons d'image. Une faille de sécurité ou une violation de données à caractère personnel peut en effet donner une très mauvaise réputation à une entreprise, dont l'impact économique pourra être bien supérieur à la valeur même des données perdues.

De plus, au regard de l'**article 28 du règlement 2016/679**, le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité appropriées. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. En d'autres termes, contrairement à une idée reçue, l'organisation qui recourt à un prestataire informatique pour mettre en œuvre un traitement (infogérant, prestataire de cloud computing) restera responsable de la conformité de ce traitement.

Jusque là imposée par les directives du « **Paquet télécom** » aux fournisseurs de services de communications électroniques (fournisseur d'accès à Internet, opérateurs de téléphonie fixe et mobile), l'obligation de notifier les violations de données personnelles aux autorités nationales compétentes, et dans certains cas, aux personnes concernées, se généralise à l'ensemble des acteurs avec le règlement 2016/679.



DES NORMES VOLONTAIRES POUR RÉPONDRE AUX ENJEUX RÉGLEMENTAIRES

Les normes volontaires ISO, rédigées par des professionnels pour des professionnels, s'organisent, ici, selon plusieurs catégories :

- un cadre qui définit **la terminologie et les principes** ;
- des méthodologies qui spécifient la mise en place d'**analyses d'impacts relatives à la protection des données** ;
- des catalogues de points de contrôle qui classifient les **bonnes pratiques** de façon générale ou sectorielle. Il existe également des **mesures techniques** de protection à mettre en œuvre.

Certaines normes sont déjà publiées et disponibles, d'autres sont actuellement en cours d'élaboration.

Synthèse des principales normes :

	Catégorie	Titre de la norme	Publication
6.1	Terminologie et principes	*Privacy framework (ISO/IEC 29100)*	2011
6.2	Systèmes de Management		
6.2.1		Norme ISO/IEC 27001 Système de Management de la Sécurité de l'Information	2013
6.2.2		Norme ISO/IEC 27552 Extension d'ISO/IEC 27001 et d'ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices	2019
6.3	Analyse d'impact	*Privacy Impact Assessment (ISO/IEC 29134)*	2017
6.4	Bonnes pratiques génériques pour la protection de la vie privée	*Code of practice for personally identifiable information protection (ISO/IEC 29151)*	2017
6.5	Bonnes pratiques de protection de la vie privée spécifiques au *cloud computing*	*Code of practice for protection of personally identifiable information (PII) in public clouds (ISO/IEC27018)*	2014
6.6	Techniques de cryptographie	*Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191)*	2012
		Blind digital signatures (ISO/IEC 18370)	2016
6.7	Techniques de dé-identification	*Privacy enhancing data de-identification techniques (ISO/IEC 20889)*	2018

6.1 Connaître la terminologie et les principes

La norme ISO/IEC 29100 (*Privacy Framework*) définit les principes et la terminologie relatifs à la protection de la vie privée. Elle constitue le socle des autres normes du groupe de travail international (WG 5) en tant que cadre sur le sujet [1]). Toutes les normes relatives à la protection de la vie privée devront s'inscrire dans ce cadre.

Les principes fondamentaux retenus dans la norme ISO/IEC 29100 représentent une base de référence dans la gestion des mesures de protection des données personnelles d'une organisation. Ils sont inspirés des textes fondateurs dans ce domaine. Par exemple, ils sont compatibles avec le cadre légal européen. La norme ISO/IEC 29100 mentionne ainsi que malgré les différences dans les facteurs sociaux, culturels, juridiques et économiques qui peuvent limiter l'application de ces principes dans certains contextes, l'application de tous les principes définis dans cette norme internationale est recommandée. Des exceptions à ces principes devraient être limitées. Les onze principes sont les suivants :

Consent and choice	Consentement éclairé des personnes concernées
Purpose legitimacy and specification	Légitimité et communication de la finalité des traitements
Collecte limitation	Données collectées adéquates, pertinentes et non excessives au regard de la finalité

1. http://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip

Data minimization	Données utilisées minimisées et cloisonnées
Use, retention, and disclosure limitation	Traitement, conservation et diffusion de données limités
Accuracy and quality	Données exactes, complètes et tenues à jour
Openness, transparency and notice	Information complète des personnes concernées
Individual participation and access	Droit d'accès et de rectification des personnes concernées
Accountability	Capacité à gérer les données et à rendre compte
Information security	Sécurité des données
Privacy compliance	Gestion des risques et contrôle continu

6.2 Mettre en place un système de management prenant en compte la protection de la vie privée

6.2.1 Norme ISO/IEC 27001 Système de Management de la Sécurité de l'Information

Comme souligné dans la section 3, l'approche préconisée est basée sur la gestion des risques. D'autre part, la sécurité est un des principes fondamentaux exprimé dans l'article 5 du règlement 2016/679, et est associée à la gestion des risques dans l'article 32 (comme rappelé la section 5.3). C'est pourquoi la norme 27001, qui fixe les exigences pour un système de management de la sécurité de l'information (en anglais *Information Security Management System* - ISMS) basé sur la gestion des risques, est très pertinente au regard de la conformité au règlement. Toutefois, la norme 27001 est focalisée sur la protection de l'organisation et ne couvre pas explicitement toutes les questions liées à la protection des données personnelles et aux droits des personnes relatifs à la vie privée, même si cela peut être compris implicitement dans les « parties intéressées » que mentionnent la norme. 27001 a pour compagnon la norme 27002 (Code de bonne pratique pour le management de la sécurité de l'information), qui détaille les mesures de sécurité et les bonnes pratiques recommandées pour la mise en œuvre du système de management.

6.2.2 Norme ISO/IEC 27552 Extension d'ISO/IEC 27001 et d'ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

Le propos de la norme 27552 est d'étendre 27001 pour couvrir la protection des données personnelles par des exigences spécifiques.

En plus des exigences faisant partie du système de management, la norme comprend également des mesures dont l'organisation doit considérer l'application. Cet ensemble de mesures constitue une extension de la norme 27002.

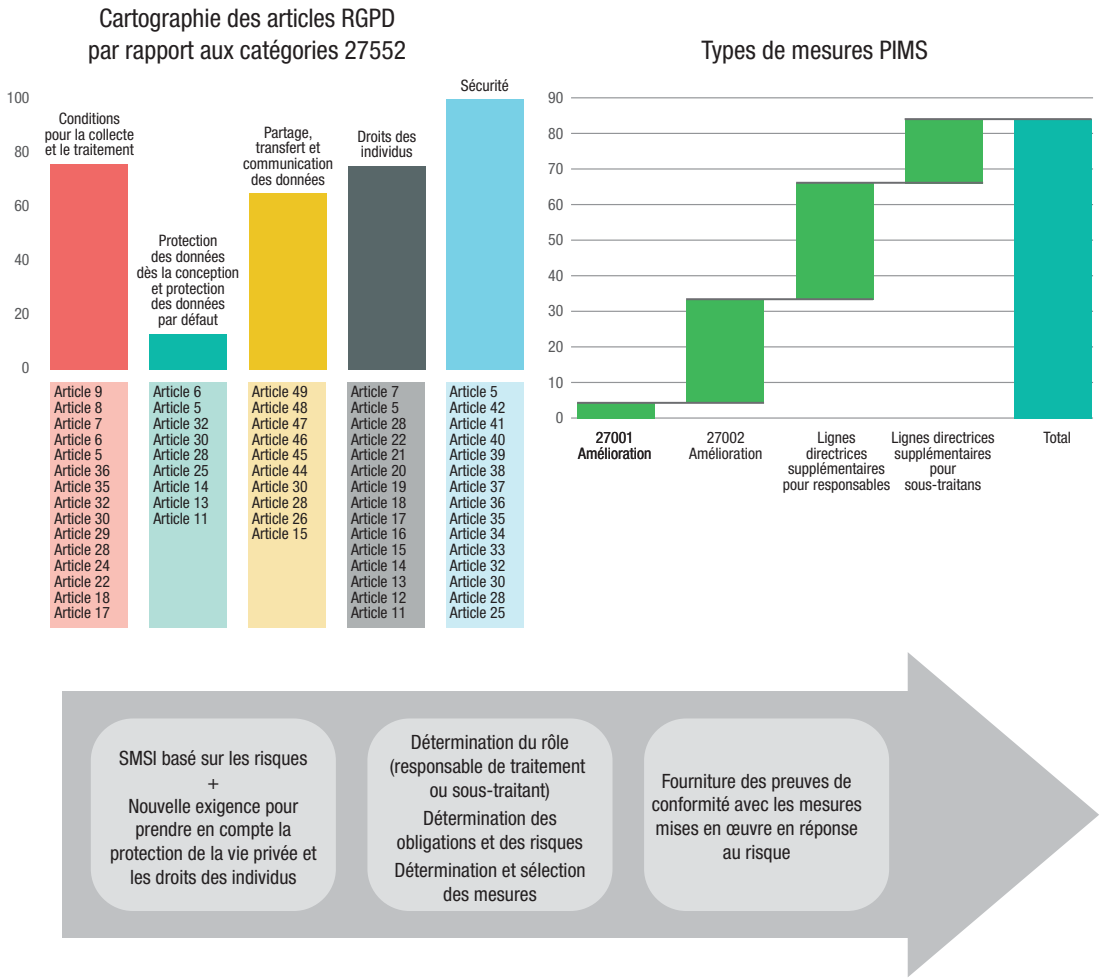
27552 est donc à la fois une extension de 27001 et une extension de 27002, et spécifie ainsi un « *Privacy Information Management System* » (PIMS).

Cette norme est applicable aux responsables de traitement et aux sous-traitants, et classe les mesures applicables à chaque catégorie dans des sections distinctes.

Une annexe informative établit les liens entre les spécifications de 27552 et les obligations du règlement RGPD. Cela montre comment la conformité aux spécifications de la norme peut être pertinente par rapport au règlement. Cette annexe est purement indicative, et il relève bien sûr de la responsabilité de l'organisation de déterminer quelles sont ses obligations légales et comment s'y conformer.

Toutefois, il est certain que la mise en œuvre de 27552 sera très utile pour l'organisation pour générer des justifications et preuves de bonnes pratiques, qui peuvent ensuite être utilisées dans une relation contractuelle responsable de traitement - sous-traitant, ou encore vis-à-vis du régulateur. La norme pourra donc être candidate à servir de base pour une certification au sens du règlement.

Le graphique ci-dessous illustre le contenu de la norme, les mesures réparties en quatre catégories, ainsi que les liens avec le règlement.



En avril 2018, la norme est au stade de consultation des pays membres à l'ISO, et devrait être publiée en 2019.

6.3 Comprendre comment mener une analyse d'impact

La norme ISO/IEC 29134 « Lignes directrices pour mener des études d'impact sur la vie privée » (*Privacy impact assessment - Guidelines*) a pour objectif de fournir un cadre pour mener des analyses d'impact sur la vie privée. Cette norme est à rapprocher des lignes directrices publiées par le WP29 en 2017 sur Data Protection Impact Assessment (DPIA) et de la méthodologie publiée par la CNIL en juin 2015. L'approche PIA s'adresse aux responsables de traitements pour bâtir leur conformité et être en capacité de le démontrer (principe d'*accountability* de la norme ISO/IEC 29100) et aux fournisseurs de produits pour montrer que leurs solutions ne portent pas atteinte à la vie privée dès la phase de conception (concept de *privacy* by design en anglais).

Par ailleurs, on note que la norme 27552 exige de considérer la mise en œuvre d'une analyse d'impact.

6.4 Disposer de bonnes pratiques génériques

Le projet de **norme ISO/IEC 29151** « Bonnes pratiques génériques pour la protection de la vie privée » (*Code of practice for PII protection*) a pour objectif de constituer un catalogue de base de bonnes pratiques pour la protection des données personnelles. Elle complète la norme ISO/IEC 27002 dont l'objectif est de fournir un catalogue de points de contrôle de sécurité de l'information selon onze chapitres de recommandations sur la politique de sécurité, le contrôle d'accès, la cryptographie, la conformité etc. Dans l'ISO/IEC 29151, des points de contrôle additionnels permettent de mettre en œuvre les principes de protection issus de la norme ISO/IEC 29100.

Il est à noter que ISO/IEC 29151 a été publiée en 2017, et que nombre d'obligations du règlement 2016/679 peuvent ne pas trouver de correspondance dans cette norme.

6.5 Disposer de bonnes pratiques spécifiques au cloud computing

En matière de bonnes pratiques, une norme dédiée au *Cloud Computing* existe déjà. C'est la norme **ISO/IEC 27018** (*Code of practice for protection of personally identifiable information (PII) in public clouds*), publiée en 2014. Cette norme s'appuie principalement sur les normes ISO/IEC 17788 sur le cadre et le vocabulaire du *Cloud*, ISO/IEC 27002 pour les bonnes pratiques de sécurité de l'information et ISO/IEC 29100 pour les principes de protection de la vie privée. Elle concerne les sous-traitants chargés des traitements de données personnelles pour le compte d'un responsable de traitements. L'adoption de cette norme participe au processus de mise en conformité. Elle représente un outil de co-régulation entre les acteurs du cloud computing et les autorités de contrôle. Il faut néanmoins garder à l'esprit que la norme ne couvre que les mesures recommandées pour un fournisseur de *cloud computing* et qu'il convient de s'assurer que les exigences de gouvernance (par exemple par la certification à ISO/IEC 27001) sont respectées du côté du fournisseur de *cloud computing*. On note que les bonnes pratiques relevant du responsable de traitement (client du fournisseur de *cloud*

computing) sont en dehors du périmètre de ISO/IEC 27018, et devraient faire l'objet de mesures spécifiques selon les principes fondamentaux exposés au chapitre 5.

Il est à noter que 27018 a été publiée en 2014, et que nombre d'obligations du règlement 2016/679 peuvent ne pas trouver de correspondance dans cette norme.

6.6 Disposer de référentiels techniques

En ce qui concerne les mesures techniques normalisées, elles reposent essentiellement sur la cryptographie dont le rôle est central dans la mise en place de solutions respectueuses de la vie privée. Au départ destinée à pouvoir chiffrer une information ou authentifier des messages, la cryptographie a dû évoluer afin de répondre aux nouvelles exigences de protection de la vie privée, en particulier pour la minimisation des données. Ainsi, des primitives cryptographiques ont été créées et sont regroupées dans ce que l'on désigne couramment aujourd'hui sous l'appellation anglaise de *Privacy Enhancing Technologies* (PETs). On peut citer les signatures de groupe, objet de la norme ISO/IEC 29191 publiée en 2012, ou les signatures aveugles dont les spécifications sont en cours de normalisation (ISO/IEC 18370). Ces mécanismes cryptographiques permettent notamment de concilier deux propriétés antinomiques de prime abord : l'authentification ou le contrôle d'accès (seules les personnes autorisées doivent pouvoir accéder à tel service) et l'anonymat (personne ne doit savoir qui est en train d'accéder au service).

D'autres groupes créent des normes de référentiels techniques contribuant à la protection de la vie privée. Par exemple le groupe relatif à l'identification des cartes et des personnes développe une norme sur des mécanismes et règles de protection de la vie privée à appliquer aux cartes à circuits intégrés (ISO/IEC CD2 19286, *Privacy enhancing protocols and services*).

6.7 Connaître les techniques de dé-identification

La norme ISO/IEC 20889 « Techniques de dé-identification de données pour la protection de la vie privée » (*Privacy enhancing data de-identification techniques*) fournit une description des techniques de dé-identification et de pseudonymisation afin d'améliorer la protection de la vie privée. Le terme « dé-identification » est préféré à « anonymisation » car en pratique l'anonymisation réelle est rarement atteinte, et donc l'utilisation du terme peut souvent être abusive. Cette norme, rédigée sous forme de guide, a pour objectif de définir des mesures en conformité avec les principes de confidentialité de la norme ISO/IEC 29100. Cette dernière spécifie la terminologie, une classification des techniques d'anonymisation en fonction de leurs caractéristiques et de leur applicabilité pour réduire les risques de ré-identification. Elle peut être utilisée par tous les types et tailles d'organisations, responsables du traitement des données et sous-traitants, et permet de partager un même vocabulaire et donc de permettre la transparence dans la description des pratiques.



CONCLUSION

Les normes relatives à la protection de la vie privée constituent des outils de co-régulation complémentaires au cadre légal et réglementaire. Elles s'appuient sur des normes de sécurité autour desquelles un écosystème solide s'est construit.

Alors que l'environnement technologique est complexe et les obligations réglementaires exigeantes, les normes permettent d'appréhender la conformité à la protection de la vie privée de façon efficace, en s'appuyant sur un consensus très large, qui reflète l'état de l'art actuel.

Tout en restant d'application volontaire, les normes peuvent devenir essentielles dans des relations contractuelles, ou simplement dans l'optique de démontrer la conformité.

La place des normes dans l'écosystème devrait encore grandir, car le règlement européen prévoit la mise en place de certifications, qui s'appuieront sur des normes reconnues.

Mais qu'est-ce qu'une norme volontaire ?

Lancée à l'initiative des acteurs du marché, la norme volontaire est un cadre de référence qui vise à fournir des lignes directrices, des prescriptions techniques ou qualitatives pour des produits, services ou pratiques au service de l'intérêt général.

Elle est le fruit d'une co-production consensuelle entre les professionnelles et les utilisateurs qui se sont engagés dans son élaboration. Tout le monde peut participer à sa création et toute organisation peut ou non l'utiliser et s'y référer. C'est pourquoi, la norme est dite volontaire.

Avez-vous pensé à participer à l'élaboration des normes volontaires ?

L'élaboration des normes volontaires est un « jeu à plusieurs ». Mais avant tout, c'est à vous, acteurs du marché, qui le faites !

Les normes volontaires ont une empreinte insoupçonnée sur notre quotidien. Savez-vous qu'elles se cachent derrière le format A4, le WIFI ou encore la carte de paiement ?

La norme volontaire est issue des réponses apportées par de nombreux industriels, prestataires de service, fédérations professionnelles, associations de consommateurs, ONG, ministères… qui partagent leur retour d'expérience, leur savoir-faire et leur expertise pour consolider la meilleure réponse qui soit, pour tous les acteurs du marché économique et social.

AFNOR guide tous ceux qui, par leur implication dans l'élaboration des normes volontaires, veulent permettre à un projet, un secteur, de se développer dans les meilleures conditions, et ainsi, poser les bases de l'économie de demain.

La normalisation volontaire, un vrai plus pour l'activité des organismes qui s'y impliquent !

Quels que soient votre secteur d'activités ou la taille de votre organisation, vous avez tout à gagner à intervenir dans l'élaboration des normes volontaires. S'impliquer en normalisation, c'est en effet le moyen :

- d'anticiper et d'influer sur les règles du jeu qui demain seront utilisées par votre marché ;
- de rencontrer et d'échanger avec les acteurs de votre domaine ;
- de vous positionner comme une référence de votre secteur.

À l'international, la normalisation volontaire vous permet de développer un réseau d'influence et d'alliances et de valoriser vos intérêts dans les instances européennes (CEN et CENELEC) et internationales (ISO et IEC). Une étude du BIPE* de janvier 2016 le prouve : s'impliquer dans la normalisation est un investissement qui se révèle payant. 20%, c'est le surcroît de *croissance du chiffre d'affaires*, observé dans les entreprises investies dans des commissions de normalisation. **Pourquoi pas vous ?**

** Société indépendante d'études économiques et de conseil en stratégie.*

Bibliographie

[1] **Règlement (UE) 2016/679** du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[2] **Directive 95/46/CE** du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[3] **Loi n°78-17** du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004.

Pour tout savoir sur la normalisation :
www.normalisation.afnor.org

Pour suivre les normes volontaires :
www.norminfo.afnor.org

Communication Groupe AFNOR - S1702109 - 04/2018. Conception : GAYA.

11 rue Francis de Pressensé - 93571 La Plaine Saint-Denis Cedex - Tél. : +33 (0)1 41 62 80 00
www.normalisation.afnor.org

afnor NORMALISATION