# RÉFÉRENTIEL TECHNIQUE

## DE GESTION DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL POUR LES ENTREPRISES

BUREAU VERITAS CERTIFICATION HOLDING
Le Triangle de l'Arche – 8, Cours du Triangle, CS 90096
92937 Paris La Défense CEDEX
France

BUREAU VERITAS

# Sommaire

# Avant-propos

Le règlement européen (UE) 2016/679 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, adopté le 27 avril 2016 et publié au JOUE le 4 mai 2016 (ci-après dénommé "règlement") vise à moderniser le cadre européen pour la protection des données à caractère personnel afin de tenir compte des progrès technologiques.

La directive communautaire du 24 octobre 1995 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données a évolué, entraînant une augmentation exponentielle du traitement et du partage des données à caractère personnel.

Il est donc primordial de réduire les divergences juridiques entre les différentes législations des États membres de l'Union européenne, objectif qui est directement applicable dans les États membres de l'Union européenne le 25 mai 2018.

Dans cette perspective et dans le cadre de leur politique de conformité, les entreprises doivent intégrer dans leur stratégie :

- les obligations découlant du règlement;
- la mise en œuvre nécessaire d'actions pour se conformer à ces nouvelles exigences, dans les délais imposés.

Le règlement oblige les entreprises à assumer l'entière responsabilité des données qu'elles traitent, de sorte qu'elles doivent allouer des ressources et des compétences internes pour assurer une protection optimale des données à caractère personnel (principe de responsabilité).

Démontrer que les traitements effectués par les responsables de traitement et leurs sous-traitants sont conformes au règlement constitue un défi majeur pour les entreprises en ce qui concerne les pénalités encourues d'une part, leur compétitivité d'autre part.

C'est pourquoi le développement de ce référentiel a été initié pour permettre aux entreprises d'attester de leur respect de ces nouvelles obligations.

La particularité de ce référentiel technique est de définir les dispositions méthodologiques et documentaires applicables aux exigences de responsabilité telles que définies dans le règlement. La responsabilisation est un nouveau principe qui oblige les entreprises à justifier tout le système de contrôle et de surveillance mis en place pour assurer la protection des données à caractère personnel.

En particulier, il s'agit notamment de :

- l'obligation de documenter les exigences relatives au respect des diverses obligations imposées par le règlement ;
- la mise en place de mesures techniques et organisationnelles pour assurer la conformité et son maintien en conditions opérationnelles ;
- la preuve du respect du réglement.

# 1. Champ d'**application**

L'application d'un code de conduite approuvé comme le prévoit l'article 40 du règlement (UE) 2016/679, ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement et à ses sous-traitants.
Outre l'adhésion des responsables de traitement ou des sous-traitants et fournisseurs soumis au présent règlement, des mécanismes de certification de la protection des données peuvent être établis afin de démontrer l'existence de garanties appropriées fournies par les responsables de traitement ou les sous-traitants qui ne sont pas assujettis au présent règlement dans le cadre des transferts de données à caractère personnel des pays tiers ou des organisations internationales.

Toute certification vis-à-vis de ce référentiel ne réduit pas la responsabilité du responsable du traitement ou du sous-traitant quant à la conformité avec le règlement (UE) 2016/679 et ne préjuge pas des tâches et des pouvoirs des autorités de contrôle.

Ce référentiel technique spécifie les exigences de gestion de la protection des données à caractère personnel que l'organisation peut utiliser pour assurer sa conformité au règlement (UE) 2016/679.
Ce référentiel permet à une organisation d'atteindre la conformité réglementaire en matière de protection des données à caractère personnel.

Ce référentiel s'applique à toute organisation, quelle que soit sa taille, son statut et son secteur, et s'applique aux aspects relatifs à la protection des données à caractère personnel de ses activités, de ses produits et de ses services qu'elle peut contrôler ou influencer en tenant compte du cycle de vie.
Ce référentiel peut être utilisé en tout ou en partie pour améliorer systématiquement les performances.

Dans ce référentiel, les formes verbales suivantes sont utilisées:

- “doit” indique une exigence ;
- “il convient” indique une recommandation ;
- “peut” indique une permission, une possibilité, une capacité ;

Les informations mentionnées en “NOTE” sont destinées à faciliter la compréhension ou l'utilisation du document.

# 2. Références **normatives**

Les documents suivants, en tout ou en partie, sont référencés normativement dans ce document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document référencé (y compris les modifications) s'applique.

- ISO / CEI 29100: 2011, Technologies de l'information - Techniques de sécurité - Cadre privée ;
- ISO / CEI 29101: 2013, Technologies de l'information - Techniques de sécurité – Architecture de référence de la protection de la vie privée ;
- ISO 9000: 2015, Systèmes de management de la qualité - Principes essentiels et vocabulaire ;
- ISO 9001: 2015, Systèmes de management de la qualité - Exigences ;
- ISO 27001:2013, Technologies de l'information -- Techniques de sécurité -- Systèmes de management de la sécurité de l'information -- Exigences
- 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).

# 3. Termes et **définitions**

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

## 3.1 Système de Management

Cf. ISO 9000:2015

## 3.2 Organisme

Cf. ISO 9000:2015

## 3.3 Direction

Cf. ISO 9000:2015

## 3.4 Système de management de la protection des données

Partie du système de management (3.1) mis en oeuvre pour gérer les aspects des données à caractère personnel (3.7), assurer la conformité réglementaire (3.5) et traiter les risques et opportunités.

## 3.5 Obligations de conformité

Exigences légales auxquelles un organisme (3.2) doit se conformer et autres exigences auxquelles un organisme doit ou choisit de se conformer. Les obligations de conformité sont liées à la protection des données à caractère personnel comme prescrit par le règlement (UE) 2016/679.

## 3.6 Processus

Cf. ISO 9000:2015

## 3.7 Données à caractère personnel

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 sociale.

## 3.8 Données à caractère personnel sensibles

Toute information concernant une personne physique relative à :

- l'origine raciale ou ethnique ;
- les opinions politiques ;
- les convictions religieuses ou philosophiques ;
- l'appartenance syndicale ;
- les données génétiques ;
- la santé ;
- les données biométriques lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne.
- les données biométriques lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique ;
- la vie sexuelle ou l'orientation sexuelle ;
- aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes.

## 3.9 Données à caractère personnel à risque

Les données à caractère personnel à risque peuvent inclure :

- les données à caractère personnel sensibles (3.8) ;
- les données à caractère personnel relatives à des personnes physiques vulnérables ;
- les aspects personnels qui sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels ;
- les traitements qui portent sur un volume important de données à caractère personnel et/ou touchent un nombre important de personnes concernées.

Il convient de déterminer la probabilité et la gravité du risque pour les droits et libertés de la personne concernée en fonction de la nature, de la portée, du contexte et des finalités du traitement. Le risque devrait faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque ou un risque élevé.

## 3.10 Traitement

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

## 3.11 Responsable du traitement

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

## 3.12 Sous-traitant

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (3.11).

## 3.13 Destinataire

La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un
tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement.

## 3.14 Consentement de la personne concernée

Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

## 3.15 Violation de données à caractère personnel

Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

## 3.16 Autorité de contrôle

Une autorité publique indépendante qui est instituée par un État membre en vertu de l'article 51 du règlement (UE) 2016/679.

## 3.17 Responsabilité

Processus permanent et dynamique qui consiste à la fois en l'obligation de rendre des comptes en ce qui concerne le respect des exigences légales et réglementaires et en un mécanisme capable de démontrer l'efficacité des mesures prises et l'efficacité de la protection des données à caractère personnel.

## 3.18 Analyse d'impact relative à la protection des données

L'analyse d'impact relative à la protection des données est un process qui aide les responsables de traitement à identifier, à évaluer et réduire au minimum les risques liés à la protection des données à caractère personnel de nouveaux projets ou politiques et des actions à entreprendre.

## 3.19 Protection des données dès la conception

Chaque nouveau service ou processus d'affaires qui utilise des données à caractère personnel doit prendre en compte la protection de ces données. Une organisation doit être en mesure de démontrer qu'elle dispose d'une sécurité adéquate et que la conformité est surveillée. En pratique cela signifie que les aspects des données à caractère personnel doivent être pris en compte tout au long du cycle de vie du système ou du développement du processus.

## 3.20 Protection des données par défaut

Obligation de s'assurer que, par défaut, les fonctionnalités des fichiers et des applications avec des données à caractère personnel garantissent un niveau élevée de protection des données. Les paramètres de confidentialité les plus stricts s'appliquent automatiquement lorsqu'un client acquiert un nouveau produit ou service. En d'autres termes, aucune modification manuelle des paramètres de confidentialité ne devrait être requise de la part de l'utilisateur. Il y a ainsi un élément temporel à ce principe, car les informations à caractère personnel ne doivent, par défaut, être conservées que pendant la durée necessaire pour fournir ce produit ou service.

## 3.21 Règles d'entreprise contraignantes

Les règles internes relatives à la protection des données à caractère personnel qu'appliquent un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe.

## 3.22 Cycle de vie

Cf. ISO 14001:2015

# 4.Organisation et **structure**

## 4.1 Leadership et engagement

La direction doit démontrer son leadership et son engagement dans la mise en œuvre des exigences de ce référentiel et des processus qui facilitent l'amélioration continue de la gestion de la protection des données à caractère personnel.

L'organisme doit mettre en oeuvre des mesures techniques et organisationnelles appropriées pour garantir et démontrer que les traitements de données à caractère personnel sont conformes avec les principes relatifs aux traitements de données à caractère personnel.
En particulier ces mesures doivent :

A. être appropriées aux finalités du traitement;

B. être définies dès la conception et mises en œuvre au moment du traitement tout au long du cycle de vie du produit ou service.

Ces mesures sont évaluées à intervalles réguliers et mises à jour si nécessaire.

NOTE : Les principes relatifs au traitement des données à caractère personnel sont ceux décrits dans l'article 5 du règlement (UE) 2016/679

## 4.2 Politique

### 4.2.1 Etablissement de la politique de protection des données à caractère personnel

La direction doit établir, documenter, mettre en œuvre et maintenir une politique indiquant son engagement à fournir des produits et/ou des services conformes au règlement (UE) 2016/679 et à rendre compte de sa conformité aux clients et aux personnes physiques.

La politique doit inclure un engagement :

A. en matière de protection des données à caractère personnel, y compris la prévention des situations de violation des données à caractère personnel;

B. à satisfaire à ses obligations de conformité (cf.5.3);

C. à mettre en œuvre des mesures organisationnelles et techniques au sein de l'organisation pour assurer la conformité au règlement (UE) 2016/679.

### 4.2.2 Communication de la politique de protection des données à caractère personnel

**La politique doit être:**

- disponible, communiquée, comprise et appliquée au sein de l'organisme;
- disponible vis-à-vis des parties intéressées, le cas échéant.

## 4.3 Organisation, rôles , responsabilités et autorités

### 4.3.1 Organisation et responsabilités

L'organisation doit avoir une structure organisationnelle documentée pour assurer la conformité des produits et/ou services (cf 5.3).

La direction doit s'assurer que les responsabilités et les autorités liées à la gestion et au traitement des données à caractère personnel sont identifiées, affectées et comprises.Les suppléances en cas d'absence de la personne responsable doivent être documentées.

### 4.3.2 Délégué à la protection des données

Un délégué à la protection des données doit être nommé pour assurer la conformité du système de gestion de protection des données à caractère personnel et des processus associés.

Ce délégué à la protection des données doit être désigné sur la base des qualités professionnelles et de la connaissance de la législation et des pratiques en matière de protection des données et doit reporter au niveau le plus élevé de la direction de l'organisme

L'organisation doit veiller à ce que le délégué à la protection des données soit impliqué dans tous les sujets liés à la protection des données à caractère personnel et doit allouer un budget et des ressources appropriés.
L'organisme doit veiller à ce que le délégué à la protection des données puisse exercer ses tâches avec la nécessaire indépendance et confidentialité. Dans le cas où le délégué à la protection des données est en charge d'autres missions et tâches, l'organisme doit veiller à ce que cela n'entraîne pas de conflit d'intérêts.

**Les missions du délégué à la protection des données sont les suivantes:**

A. Informer et conseiller l'organisme ainsi que les employés qui procèdent au traitement de données à caratère personnel sur les obligations de conformité en matière (cf. 5.3);

B. Contrôler le respect des obligations du présent règlement (cf. 5.3) avec les règles internes de l'organime en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ; en particulier le responsable de la protection des données doit organiser la réalisation des revues de management;

C. Dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci;

D. Etre le point de contact pour l'autorité de contrôle et coopérer avec l'autorité de contrôle sur les questions relatives aux données à caratère personnel, le cas échéant.

L'organisme doit publier les coordonnées du responsable de la protection des données et les communiquer à l'autorité de contrôle si nécessaire.

NOTE : Le délégué à la protection des données peut être un employé ou une personne sous contrat. Les qualités et expériences professionnelles doivent couvrir les aspects management IT/IS mais également la connaissance des produits et services de l'organisme.

## 4.4 Objectifs

L'organisme doit s'assurer que des objectifs sont clairement définis pour maintenir et améliorer la conformité et la réalisation des produits et/ou services en cohérence avec ce référentiel. Ces objectifs doivent être :

- documentés, mesurables;
- communiqués aux fonctions et niveaux concernés;
- surveillés et mis à jour autant que besoin.

Les objectifs doivent être établis en prenant en compte l'analyse d'impact relative à la protection des données et les obligations de conformité associées (cf. 5.3).

# 5. Gestion des risques relatifs aux **données à caractère personnel**

## 5.1 Généralités

L'organisme doit mettre en oeuvre un plan d'action efficace en considérant les enjeux et exigences en matière de protection des données à caractère personnel.

## 5.2 Analyse d'impact relative à la protection des données

L'organisme doit déterminer les activités, produits et/ou services que peuvent affecter la confidentialité et l'intégrité des données à caractère personnel et les situations potentielles de violation des données à caractèrer personnel, dans une perspective de cycle de vie.

Lors de la détermination de ces aspects, l'organisme doit prendre en compte :

A. une description systématique des opérations de traitement envisagées et des finalités du traitement;

B. une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard de leurs finalités ;

C. une évaluation des risques pour les droits et libertés des personnes concernées ;

D. les niveaux de risque des données à caractère personnel ;

E. les conditions anormales et les situations prévisibles qui pourraient conduire à des cas de violation de données à caractère personnel ;

F. les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect des exigences règlementaires, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

G. tout changement, y compris les évolutions nouvelles ou planifiées et les activités, produits et/ou services nouveaux ou modifiés ;

Cette analyse d'impact relative à la protection des données doit être développée et gérée par une équipe multidisciplinaire qui comprend les responsables du marketing, du commerce, des opérations, de l'ingénierie, des technologies de l'information et de la sécurité, de la qualité et d'autres fonctions pertinentes.

Les analyses d'impact relatives à la protection des données doivent être documentées y compris les situations potentielles de violation des données à caractère personnel.

L'organisme doit communiquer les conclusions de ces analyses d'impact aux différents niveaux et fonctions de l'organisme, de façon appropriée.

## 5.3 Obligations de conformité

L'organisme doit déterminer toutes les obligations de conformité relatives aux données à caractère personnel incluant :

A. les exigences réglementaires;

B. les codes de conduite imposés ou les règles d'entreprise contraignantes;

C. les exigences client spécifiques relatives à la protection des données à caractère personnel.

L'organisme doit prendre en considération ces obligations de conformité pour l'établissement, la mise en œuvre, la maintenance et l'amélioration continue du système de management et doit maintenir à jour des informations documentées sur es obligations de conformité.

NOTE : Les exigencies réglementaires comprennent le réglement (UE) 2016/679, les dispositions de tout état membre de l'Union Européenne relatives à la protection des données à caractère personnel et les politiques du responsable de traitement et de ses sous-traitants en matière de protection des données à caractère personnel.

## 5.4 Plan d'actions

L'organisme doit planifier d'entreprendre des actions pour traiter ses:

A. résultats de l'analyse d'impact relative à la protection des données à caractère personnel ;

B. obligations de conformité.

Lors de la planification de ces actions, l'organisme doit

- prendre en considération ses options technologiques ainsi que ses exigences financières, opérationnelles et commerciales ;
- évaluer l'efficacité de ces actions en selectionnant des mesures techniques adaptées aux risques identifiés ;
- garantir l'établissement de processus pour amener l'efficacité des actions mises en œuvre.

## 5.5 Gestion des situations de violation de données

L'organisme doit établir, mettre en œuvre et maintenir à jour le ou les processus nécessaire(s) pour se préparer et répondre aux situations de violation de données à caractère personnel potentielles identifiées (5.2).

Notamment l'organisme doit :

A. préparer sa réponse en planifiant des actions pour prévenir ou atténuer les violations des données à caractère personnel et leurs conséquences, de manière appropriée à l'ampleur de l'urgence et à l'impact potentiel ;

B. répondre aux situations réelles de violation de données à caractère personnel ;

C. tester périodiquement les actions de réponse planifiées lorsque cela est réalisable ;

D. revoir et réviser périodiquement le ou les processus ainsi que les actions de réponse planifiées, notamment après la survenue de situations les violations des données à caractère personnel ou la réalisation de tests;

E. fournir des informations et des formations pertinentes relatives à la préparation et à la réponse aux situations de violations des données à caractère personnel, de façon appropriée, aux parties intéressées pertinentes, y compris les personnes effectuant un travail sous le contrôle de l'organisme.

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, l'organisme doit communiquer la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

En complément, en cas de violation de données à caractère personnel, l'organisme doit notifier la violation en question à l'autorité de contrôle, dans les meilleurs délais, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

La communication à la personne concernée et/ou à l'autorité de contrôle doit être conforme aux exigences des articles 33 et 34 du règlement (UE) 2016/679.

# 6. Système de **management**

## 6.1 Manuel et procédures

L'organisme doit établir, mettre en œuvre, tenir à jour et améliorer en continu un système de management en accord avec les exigences de ce référentiel qui assure la mise en œuvre effective et la maintenance des processus relatifs à la protection des données à caractère personnel. Le système de management doit être approprié au type, gamme et volume des produits et/ou services.

Le système de management doit documenter les processus opérationnels, et leurs interactions en assurant que les données à caractère personnel sont collectées, traitées et conservées ou archivées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

Le système de management doit permettre à l'organisme:

1. d'assurer que le traitement de données à caractère personnel est conforme avec les exigences de conformité contractuelles ou réglementaire;
2. d'assurer que les responsabilités sont assurées en conformité avec le Réglement (UE) 2016/679;
3. de surveiller la conformité et l'adéquation des procédures documentées du système.

NOTE : Un système de management de la qualité (ISO 9001: 2015) ou de la sécurité de l'information (ISO 27001: 2013) de l'organisme peut être utilisé pour répondre aux exigences minimales du système de management défini dans ce référentiel

## 6.2 Informations documentées

Le système de management de l'organisme doit inclure les informations documentées relatives aux traitements et processus liés à la protection des données à caractère personnel.

L'organisme doit avoir une procédure pour gérer les informations documentées, incluant selon le cas les activités suivantes:

- identification, description, revue et approbation;
- distribution, accès et utilisation;
- stockage et protection;
- maîtrise des modifications;
- conservation et élimination.

L'organisme doit conserver des enregistrements pour démontrer le contrôle effectif de la conformité des produits et/ou des services.

Les enregistrements doivent être lisibles, conservés en bon état et récupérables.

Les enregistrements doivent être conservés pour une période définie en tenant compte des exigences légales ou contractuelles.

## 6.3 Analyse et évaluation

L'organisme doit déterminer:

A. ce qui doit être contrôlé et surveillé, et quand;
B. les méthodes de suivi, de mesure, d'analyse et d'évaluation;
C. les critères de performance et les indicateurs appropriés.

En complément, l'organisme doit établir, mettre en oeuvre et tenir à jour les processus nécessaires à l'évaluation du respect de ses obligations de conformité.

En particulier l'organisme doit:

A. déterminer la fréquence à laquelle la conformité sera évaluée;
B. évaluer la conformité et entreprendre des actions si nécessaire;
C. déterminer les risques de violation des données à caractère personnel ou de non-conformité et l'efficacité du processus de détection des non-conformités et des mesures prises;
D. maintenir la connaissance et la compréhension de son état de conformité ;
E. communiquer les informations pertinentes sur la performance tant en interne qu'en externe.

L'organisme doit conserver des informations documentées comme prevue du suivi de la conformité de ses opérations.

## 6.4 Audit interne

L'organisme doit réaliser des audits internes au moins annuellement couvrant toutes les exigences de ce référentiel pour fournir des informations permettant de déterminer:

- la conformité aux exigences de ce référentiel ;
- sa mise en œuvre de manière efficace et son maintien à jour.

Le périmètre et la fréquence des audits doivent tenir compte des risques des processus et activités relatifs à la protection des données à caractère personnel et des résultats des audits précédents.
Les audits internes doivent être réalisés par des auditeurs dûment formés et compétents. L'impartialité des auditeurs doit être assurée.

Les rapports d'audits doivent détailler tout écart significatif par rapport à ce référentiel. En particulier les rapports d'audits doivent identifier les enjeux liés aux technologies ou processus qui pourraient impacter les obligations de la conformité (cf.5.3).

## 6.5 Revue de direction

A des intervalles planifiés la direction doit conduire des revues du système de management, a minima annuellement, pour évaluer la performance vis à vis du référentiel et des objectifs (4.4).

La revue de direction doit inclure les sujets suivants:

- état d'avancement des actions issues des revues de direction précédentes;
- résultats des audits internes et externes;
- satisfaction des clients et retours d'information des parties intéressées y compris les réclamations ;
- incidents, violations, non conformités et plans d'actions associés;
- efficacité des actions mises en œuvre suite aux analyses d'impact relatives à la protection des données; résultats de contrôle et de surveillance;
- performance des sous-traitants et des prestataires de service;
- tout changement relatif à l'analyse d'impact relative à de la protection des données;
- toute évolution au niveau des obligations de conformité.

Les éléments de sortie de la revue de direction doivent inclure:

- opportunités d'amélioration;
- plan d'action y compris les besoins en ressources;
- actions d'amélioration, si besoin, au cas où les objectifs n'ont pas été atteints;
- toute implication pour l'orientation stratégique de l'organisme.

Les enregistrements de revue de direction doivent être documentés et utilisés pour réviser les objectifs. La conclusion des revues de direction et les plans d'action associés doivent être communiqués efficacement au personnel approprié et mis en œuvre.

## 6.6 Non conformité et action corrective

L'organisme doit déterminer les opportunités d'amélioration et mettre en œuvre les mesures nécessaires pour répondre aux exigences de conformité (cf.5.3) et prévenir la récurrence.

Lorsqu'une non- conformité se produit, l'organisme doit:

A. prendre des mesures pour maîtriser le problème immédiat;

B. évaluer les actions en identifiant les causes de la non conformité pour prévenir d'autres occurrences ailleurs;

C. mettre en œuvre le plan d'action, vérifier que les corrections ont été effectivement mises en œuvre.

L'organisation doit conserver une information documentée comme preuve de la nature des non-conformités et des mesures correctives associées.

## 6.7 Réclamations

L'organisme doit s'assurer que les réclamations des clients et des parties intéressées sont effectivement traitées.

L'organisme doit publier le processus de traitement des réclamations.

Dès réception de la réclamation, l'organisme doit:

A. accuser réception de la réclamation auprès du plaignant;

B. collecter et analyser toutes les informations nécessaires pour évaluer et valider la réclamation et décider des suites à donner sur la réclamation,

C. informer officiellement le plaignant sur la décision relative à la réclamation;

D. s'assurer que toutes les mesures correctives et préventives appropriées sont mises en oeuvre.

## 6.8 Communication

### 6.7.1 Généralités

En établissant son processus de communication, l'organisme doit:

A. prendre en compte ses obligations de conformité (cf.5.3);

B. s'assurer que les informations communiquées relatives à la protection des données à caractère personnel sont cohérentes avec les exigencies de ce référentiel et sont fiables.

L'organisme doit conserver, de façon appropriée, des informations documentées comme preuves de ses communications.

### 6.7.2 Communication interne

L'organisme doit:

A. communiquer en interne les informations pertinentes relatives au système de management relatif à la protection des données aux différents niveaux et fonctions de l'organisme, en particulier les changements apportés au système de management, de façon appropriée;

B. s'assurer que son ou ses processus de communication permettent aux personnes effectuant un travail sous le contrôle de l'organisme de contribuer à l'amélioration continue.

L'organisme doit s'assurer que toute politique client spécifique ou exigence, tout code de conduite ou toutes règles d'entreprise contraigantes, méthodes opérationnelles sont comprises, mises en œuvre et clairement communiquées aux différents niveaux et fonctions de l'organisme, et aux sous-traitants et prestataires, le cas échéant.

### 6.7.3 Communication externe

L'organisme doit communiquer en externe les informations pertinentes relatives à la protection de données, comme établi par le ou les processus de communication de l'organisme et requis par ses obligations de conformité.

En particulier, le responsable de traitement prend des mesures appropriées pour fournir aux personnes concernées toute information relative aux droits et libertés des personnes physiques conformément aux articles 12 à 23 (chapitre III: droits de la personne concernée) du Réglement (UE) 2016/679.

# 7. Maîtrise des **produits et/ou services**

## 7.1 Exigences relatives aux produits et services

L'organisme doit s'assurer que les exigences relatives aux produits et/ou services sont définies y compris:

A. les exigences de conformité et les exigences client relatives à la protection des données à caractère personnel;

B. les exigences internes jugées nécessaires par l'organisme ou imposées par un code de conduite ou des règles d'entreprise contraignantes.

L'organisme doit conduire une revue pour s'assurer de son aptitude à répondre aux exigences relatives aux produits et/ou services proposés aux clients.

L'organisme doit, le cas échéant, conserver des informations documentées des résultats de la revue. Cette revue doit être mise à jour en cas de changements des exigences relatives aux produits et/ou services.

## 7.2 Conception et développement des produits et/ou services

L'organisme doit établir, mettre en oeuvre et maintenir un processus de conception et développement qui assure une conformité en continu, aux exigences en matière de protection des données à caractère personnel tout au long du cycle de vie des produits et services, y compris le traitement en fin de vie, et à l'élimination finale de ses produits et services.

L'organisme doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir que :

- les exigences relatives aux produits et services sont prises en compte pour la conception et le développement;
- Les conséquences potentielles d'une défaillance potentielle liée à la nature des produits et services au travers de la réalisation de l'analyse d'impact relative à la protection des données (5.2);
- par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité;
- la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples;
- les traitements de données sont conformes avec les intérêts ou les droits fondamentaux et libertés des personnes physiques et en particulier pour les personnes vulnérables incluant les enfants.

L'organisme doit maîtriser le processus de conception et développement pour garantir que les produits et services résultants satisfont les exigences pour l'application spécifiée ou l'usage prévu.
La conception et le développement de produits ou services ne sont validés qu'après un examen de la clôture appropriée des non-conformités relatives à la protection des données à caractère personnel.

L'organisme doit conserver des informations documentées relatives aux activités de conception et de développement.

NOTE : Les droits et libertés des personnes physiques sont décrites dans les articles 12 à 23 (chapitre III: droits de la persone concernée) du Réglement (UE) 2016/679.

## 7.3 Libération des produits et/ou services

Lorsque les produits et/ou services requièrent une approbation avant mise en service, des procédures doivent être mises en place pour garantir que la mise en service n'intervient pas tant que les exigences de mise en service n'ont pas été remplies et la mise en service autorisée.

Conformément à l'article 30 du Réglement (UE) 2016/679, l'organisme doit maintenir un registre des activités de traitement effectuées sous sa responsabilité. Ce registre doit comporter toutes les informations suivantes:

A. les finalités et catégories du traitement;
B. une description des catégories de personnes concernées et des catégories de données à caractère personnel;
C. les catégories de destinataires;
D. le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale;
E. dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données.

L'organisme doit mettre le registre à la disposition de l'autorité de contrôle sur demande.

# 8. Maîtrise **opérationnelle**

L'organisme doit élaborer et mettre en œuvre des procédures documentées et/ou des instructions de travail qui garantissent la conformité de ses opérations.

## 8.1 Maîtrise des traitements

Compte tenu 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, l'organisme met en oeuvre des mesures techniques et organisationnelles appropriées pour garantir et démontrer que le traitement est effectué conformément à ses obligations de conformité.

Les procédures et ou instructions doivent être disponibles et spécifier comment les données à caractère personnel sont traitées en respectant les principes de l'article 5 du Réglement (UE) 2016/679.

En cohérence avec la perspective du cycle de vie, l'organisme doit conserver des informations documentées pour démontrer que les processus ont été mis en œuvre conformément aux dispositions et la conformité des produits et/ou services aux exigences.

NOTE : Les moyens de maîtrise peuvent inclure des moyens techniques et des procédures. Les moyens de maîtrise peuvent être mis en oeuvre suivant une hiérarchie (par exemple, élimination, substitution, gestion administrative) et peuvent être utilisés séparément ou par combinaison.

NOTE : Il est fortement recommandé de cartographier les processus relatifs à la protection des données à caractère personnel.

## 8.2 Maîtrise des sous-traitants et des prestataires externes

L'organisme doit s'assurer que les processus externalisés sont maîtrisés ou influencés en conformité avec l'article 27 du règlement (UE) 2016/679. Le type et le degré de maîtrise ou d'influence à appliquer au(x) processus doivent être définis.
En particulier:

- L'organisme doit faire uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en oeuvre de mesures techniques et organisationnelles appropriées, de manière à ce que le traitement réponde aux exigences de conformité (cf. 5.3) et garantisse la protection des droits de la personne concernée ;
- Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique qui définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits de l'organisme.

**Ce contrat doit prévoir, notamment, que le sous-traitant**:

A. ne traite les données à caractère personnel que sur instruction documentée de l'organisme, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale;

B. veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité;

C. selon le choix de l'organisme, supprime toutes les données à caractère personnel ou les renvoie au terme de la prestation de services relatifs au traitement;

D. met à la disposition de l'organisme toutes les informations nécessaires pour démontrer le respect des obligations et pour contribuer aux audits, y compris des inspections, conduits par l'organisme ou un autre auditeur mandaté par ce dernier;

E. ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement ;

F. notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

Le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que si le transfert respecte l'une des dispositions détaillées dans les articles 44, 45 et 46 du règlement (UE) 2016/679.

# 9. Ressources

L'organisme doit déterminer et fournir les ressources nécessaires à la mise en œuvre de mesures techniques et organisationnelles pour assurer le respect des exigences en matière de protection des données à caractère personnel.

## 9.1 Infrastructure

L'organisme doit mettre en oeuvre des mesures techniques et organisationnelles appropriées pour mettre en œuvre les principes de protection de données de manière effective et intégrer les niveaux de sécurité nécessaires au niveau des traitements, et appropriés au type et nature des traitements ainsi qu'aux conclusions de l'analyse d'impact relative des données à caractère personnel.
En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

L'organisme doit mettre en oeuvre les processus appropriés visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe précédent comprennent la mise en oeuvre de politiques appropriées en matière de protection des données par l'organisme. Ces mesures doivent définir les dispositions de sécurité appropriées lors des phases de collecte, détention, conservation et transfert des données.

L'organisme doit mettre en oeuvre des procédures pour garantir que l'accès par son personnel à des données personnelles est limité au personnel qui doit avoir un tel accès.

NOTE : Le cas échéant, l'organisme peut considerer une conformité vis à vis de la norme ISO/IEC 27001.

NOTE : ISO/IEC 27002:2013 peut être utilisée comme un guide pour identifier les mesures adéquates à mettre en oeuvre.

NOTE : Une attention particulière doit être portée sur le stockage des données à caractère personnel sur les équipements mobiles.

## 9.2 Personnel

### 9.2.1 Compétence

L'organisme doit:

A. déterminer les compétences nécessaires de la ou des personnes effectuant un travail qui a une incidence sur la protection des données à caractère personnel et sur sa capacité à satisfaire à ses obligations de conformité;

B. s'assurer que ces personnes sont compétentes sur la base d'une formation initiale ou professionnelle ou d'une expérience appropriées;

C. déterminer les besoins de formation liés à l'analyse d'impact relative aux données à caractère personnel ;

D. maintenir les compétences de son personnel impliqué dans la protection des données à caractère personnel en fonction des changements des technologies et pratiques;

E. le cas échéant, mener des actions pour acquérir les compétences nécessaires et évaluer l'efficacité de ces actions.

En particulier, le personnel en charge de la mise en œuvre du système de management au sein de l'organisme doit être formé sur les aspects de la réglementation relative à la protection des données.

Les enregistrements de toute formation doivent être disponibles. Cela doit inclure au minimum:

A. le nom du stagiaire et l'attestation de présence

B. la date et la durée de la formation

C. le titre ou le contenu du cours, selon le cas

D. le fournisseur de formation

### 9.2.2 Sensibilisation

L'organisme doit s'assurer que son personnel est sensibilisé:

A. à la politique de protection de données à caractère personnel ;

B. violations réelles ou potentielles de données à caractère peronnel associées à leur travail;

C. aux répercussions d'un non-respect des exigences du système de management, y compris le non-respect des obligations de conformité de l'organisme.

### 9.2.3 Maintien des connaissances

L'organisme doit veiller à ce que le développement des technologies de l'information et de la communication et les évolutions des pratiques commerciales soient suivis et pris en compte.

# Annexe 1 - Introduction

## 0.1 Généralités

Les avantages potentiels pour une organisation de mettre en œuvre un système de gestion lié à la protection des données à caractère personnel sur la base de ce référentiel sont:

A. la capacité de fournir de façon constante des produits et des services qui répondent aux exigences réglementaires et aux exigences légales des clients;

B. la prise en compte des risques et des opportunités liés à son contexte et à ses objectifs;

C. la capacité de démontrer les exigences de conformité réglementaire.

Ce référentiel utilise l'approche par processus, qui intègre le cycle Plan-Do-Check-Act (PDCA) et l'approche basée sur le risque.

Elle comprend notamment :

- l'adoption de règles internes;
- la conservation du dossier de tout traitement effectué sous la responsabilité du responsable de traitement ou du sous-traitant, c'est-à-dire une description de chaque traitement mis en œuvre;
- la mise en œuvre d'une analyse d'impact pour les traitements présentant des risques particuliers en ce qui concerne les droits et libertés des personnes physiques;
- le respect du principe de transparence dans les transactions décisives relatives à la protection des données à caractère personnel;
- la mise en œuvre des approches «par-conception» et «par-défaut» dans les projets;
- la nomination d'un délégué à la protection des données;
- la documentation et les dossiers des mesures de conformité.

## 0.2 Objectif du référentiel

Le but de ce référentiel est de fournir aux organisations un cadre de mesures organisationnelles et techniques et processus pour se conformer au règlement (UE) 2016/679 relatif à la protection des données à caractère personnel et répondre aux progrès technologiques.

Une approche systématique de la gestion de la protection des données à caractère personnel peut fournir à la direction générale de l'information pour réussir sur le long terme et créer des conditions permettant d'atteindre la conformité en:

- protégeant les données à caractère personnel en prévenant ou en atténuant les violations de données à caractère personnel;
- aidant l'organisation à s'acquitter de ses obligations en matière de conformité;
- contrôlant ou influençant la façon dont les produits et services de l'organisation sont conçus, développés, traités et disposés en utilisant une perspective de cycle de vie qui peut prévenir les atteintes à la protection des données à caractère personnel;
- communiquant les informations appropriées aux parties intéressées pertinentes.

# 0.3 Approche processus

## 0.3.1 Généralités

1. Principe de responsabilisation. Il s'agit d'un principe général de responsabilité envers le responsable du traitement des données à caractère personnel qu'il effectue lui-même ou qui est exécuté en son nom.

2. Par conséquent, cette obligation l'oblige à mettre en œuvre des mesures techniques et organisationnelles appropriées pour effectuer le traitement conformément aux exigences du règlement.

3. Règles internes. Par conséquent, afin de se conformer à cette obligation, le responsable du traitement doit décrire en détail les obligations incombant au titulaire pour se conformer au règlement et fournir des éléments de preuve, notamment en adoptant des règles et des mécanismes internes.

4. En outre, le responsable de traitement doit adopter une approche proactive. En d'autres termes, il doit pouvoir démontrer sa conformité sans attendre que des irrégularités lui soient signalées. Il adopte des règles internes et met en œuvre les mesures appropriées pour assurer et pouvoir démontrer que le traitement des données est effectué conformément au règlement.

5. La portée de ces obligations tient compte:

- du but des traitements;
- des risques de porter atteinte aux droits et libertés des personnes physiques.

6. En fonction des risques liés au traitement et aux types de données traitées, les mesures à mettre en œuvre vont de la documentation à la mise en œuvre des obligations de sécurité et à la mise en œuvre d'une analyse d'impact.

7. Transparence. Le responsable de traitement est soumis à une obligation de transparence et de traçabilité des documents afin de pouvoir être tenu responsable. Il doit à tout moment pouvoir identifier et documenter les mesures prises pour se conformer aux exigences du règlement et être en mesure de démontrer qu'il a rempli ses obligations en matière de protection des données à caractère personnel. Il est tenu de documenter toutes les actions de sa politique de protection des données afin de démontrer aux autorités de contrôle comment elles sont réalisées.

8. Protection des données par conception. Le principe de la «protection des données par conception» exige que les organisations tiennent compte du respect de la vie privée dans la conception des produits, des services et des systèmes utilisant des données à caractère personnel.

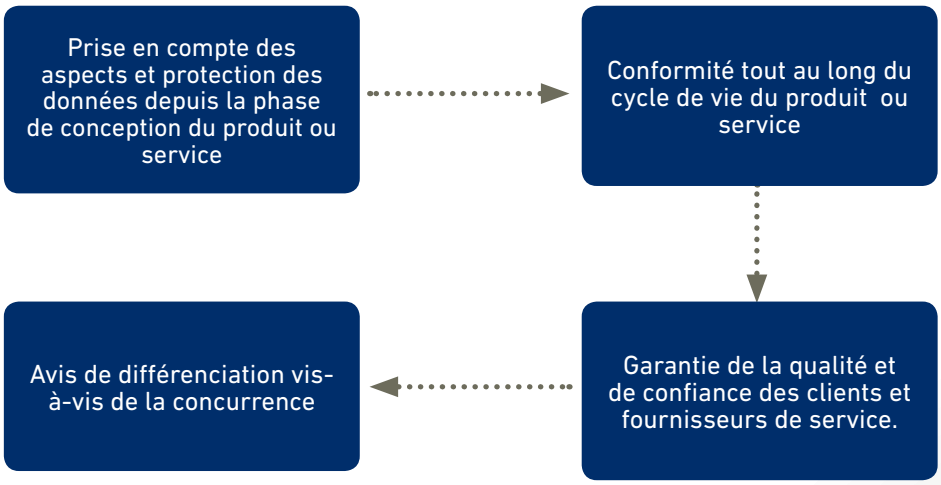
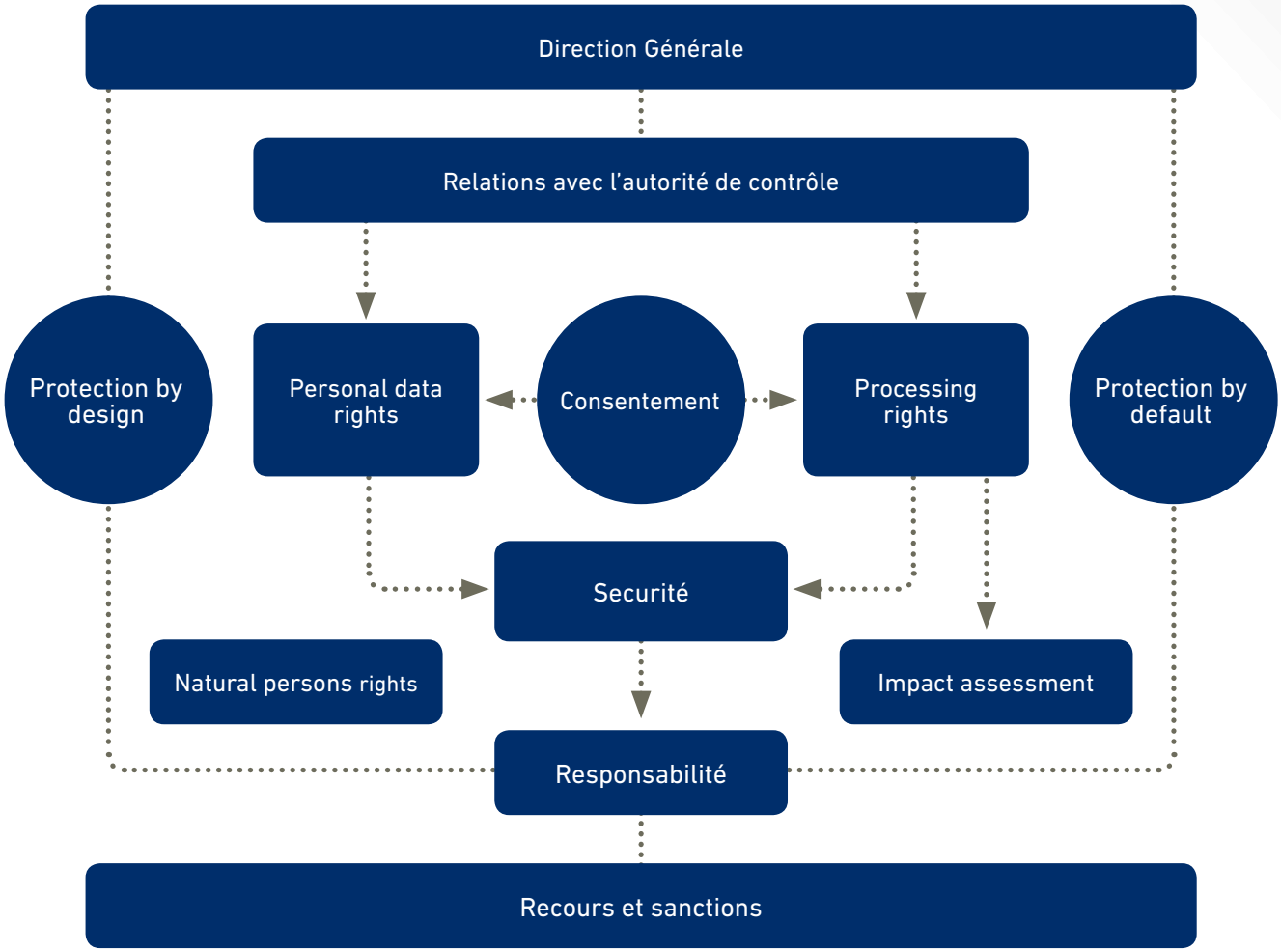



Figure 1: Protection des données

9. Protection des données par défaut. Le principe de la «protection des données par défaut» exige que les organisations disposent d'un système d'information garantissant un niveau élevé de protection des données à tous les stades (enregistrement, exploitation, administration, intégrité et mise à jour). La sécurité du système d'information doit être assurée dans tous ses éléments physiques ou logiques. En outre, cette règle implique que l'état de la sécurité du système d'information peut être connu à tout moment, en fonction des spécifications du fabricant, des aspects vulnérables et des mises à jour.

10. L'approche du règlement peut être formalisée comme suit



# **Annexe 2** – Tableaux de **références croisées**

## Matrice de correspondance entre le Référentiel de certification et l'ISO 9001 et le RGPD

| Contenu de la norme de certification | | ISO 9001:2015 | RÈGLEMENT UE 2016/679 |
|---|---|---|---|
| 0 | Introduction | | Article 1 ; Article 2 ; Article 40 ; Article 42 |
| 1 | Domaine d'application | | Article 24 (3) ; 25(3) ; 28(5) ; 42 |
| 2 | Références normatives | | ISO 9001:2015 ; ISO 14001:2015 ; RÈGLEMENT UE 2016/679 |
| 3 | Termes et définitions | | |
| 4 | Organisme et structure | | |
| 4.1 | Leadership et engagement | 5.1 | Article 25 ; Article 23 |
| 4.2 | Politique | 5.2 | |
| 4.2.1 | Établissement de la politique relative aux données à caractère personnel | 5.2.1 | |
| 4.2.2 | Communication de la politique relative aux données à caractère personnel | 5.2.2 | |
| 4.3 | Rôles, responsabilités et autorités au sein de l'organisme | 5.3 (1 et 2) | Article 37 ; Article 38 ; Article 39 |
| 4.3.1 | Organisme et responsabilités | | |
| 4.3.2 | Délégué à la protection des données | | |
| 4.4 | Objectifs | 6.2.1 | |
| 5 | Management du risque relatif aux données à caractère personnel | 6.1 | |
| 5.1 | Généralités | 6.1.1 | Article 34 |
| 5.2 | Analyse d'impact relative à la protection des données | 6.1.2 | Article 35 (7) |
| 5.3 | Obligations de conformité | 6.1.3 | Article 31 |
| 5.4 | Plan d'action | 6.1.4 | |
| 5.5 | Gestion des violations de données à caractère personnel | 8.7 | Article 33 ; 34 |
| 6 | Système de management | | |

| Contenu de la norme de certification | | ISO 9001:2015 | RÈGLEMENT UE 2016/679 |
|---|---|---|---|
| 6.1 | Manuel et procédures | 4.4 | Article 5 |
| 6.2 | Informations documentées | 7.5 | Article 15 |
| 6.3 | Évaluation des performances | 9.1.1 9.1.2 9.1.3 | |
| 6.4 | Audit interne | 9.2 | |
| 6.5 | Revue de direction | 9.3 | |
| 6.6 | Non-conformités et actions correctives | 10.2 | |
| 6.7 | Réclamations | | |
| 6.8 | Communication | 7.4 | |
| 6.8.1 | Généralités | | |
| 6.8.2 | Communication interne | | |
| 6.8.3 | Communication externe | | Article 7 ; Article 12 ; Article 13 ; Article 14 ; Article 15 ; Article 16 ; Article 17 ; Article 18 ; Article 19 ; Article 20 ; Article 21 ; Article 22 ; Article 23 |
| 7 | Maîtrise des produits et/ou des services | | |
| 7.1 | Exigences relatives aux produits et services | 8.2 | |
| 7.2 | Conception et développement de produits et services | 8.3 | Article 25 ; 32 ; Article 7 |
| 7.3 | Libération des produits et / ou des services | 8.6 | Article 30 |
| 8 | Maîtrise opérationnelle | | |
| 8.1 | Maîtrise des processus | 8.1 | Article 5 ; Article 24 (1) ; Article 35 |
| 8.2 | Maîtrise de la sous-traitance et des prestataires de service | 8.4 | Article 28 ; 45 ; 46 |
| 9 | Ressources | 7.1 | |
| 9.1 | Infrastructure | 7.1.3 | Article 25 (1) (2) ; Article 24 (2) ; Article 32 1(d) |
| 9.2 | Personnel | 7.1.2 | |
| 9.2.1 | Compétences | 7.2 | Article 37 |
| 9.2.2 | Sensibilisation | 7.3 | Article 32 (4) |
| 9.2.3 | Gestion des connaissances | | |

# Matrice de correspondance entre le RGPD et le Référentiel de certification

| Chapitre | Section | Article | | Norme de certification |
|---|---|---|---|---|
| Dispositions générales | | Article premier | Objets et objectifs | Annexe 1 |
| | | Article 2 | Champ d'application matériel | Annexe 1 |
| | | Article 3 | Champ d'application territorial | 8.2 Maîtrise de la sous-traitance et des prestataires de service |
| | | Article 4 | Définitions | 3 Termes et définitions |
| Principes | | Article 5 | Principes relatifs au traitement des données à caractère personnel | 6.1 Manuel et procédures<br>8.1 Maîtrise du traitement |
| | | Article 6 | Licéité du traitement | 6.8.3 Communication externe + Annexe 1 |
| | | Article 7 | Conditions applicables au consentement | 6.8.3 Communication externe<br>7.2 Conception et développement de produits et / ou des services |
| | | Article 8 | Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information | 5.2 Analyse d'impact relative à la protection des données (Définitions 3.8 et 3.9) |
| | | Article 9 | Traitement portant sur des catégories particulières de données à caractère personnel | |
| | | Article 10 | Traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions | |
| | | Article 11 | Traitement ne nécessitant pas l'identification | |
| Droits de la personne concernée | Transparence et modalités | Article 12 | Transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée | 6.8.3 Communication externe |
| | Information et accès aux données à caractère personnel | Article 13 | Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée | 6.8.3 Communication externe |
| | | Article 14 | Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée | 6.8.3 Communication externe |
| | | Article 15 | Droit d'accès de la personne concernée | 6.8.3 Communication externe<br>6.2 Informations documentées |
| | Rectification | Article 16 | Droit de rectification | 6.8.3 Communication externe |

| Chapitre | Section | Article | | Norme de certification |
|---|---|---|---|---|
| | et effacement | Article 17 | Droit à l'effacement (« droit à l'oubli ») | 6.8.3 Communication externe |
| | | Article 18 | Droit à la limitation du traitement | 6.8.3 Communication externe |
| | | Article 19 | Obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement | 6.8.3 Communication externe |
| | | Article 20 | Droit à la portabilité des données | 6.8.3 Communication externe |
| | Droit d'opposition et prise de décision individuelle automatisée | Article 21 | Droit d'opposition | 6.8.3 Communication externe |
| | | Article 22 | Décision individuelle automatisée, y compris le profilage | 6.8.3 Communication externe |
| | Limitations | Article 23 | Limitations | 6.8.3 Communication externe |
| Responsable du traitement et sous-traitant | Obligations générales | Article 24 | Responsabilité du responsable du traitement | 8.1 Maîtrise du traitement<br>9.1 Infrastructure |
| | | Article 25 | Protection des données dès la conception et protection des données par défaut | 7.2 Conception et développement de produits et / ou de services<br>9.1 Infrastructure |
| | | Article 26 | Responsables conjoints du traitement | |
| | | Article 27 | Représentants des responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union | |
| | | Article 28 | Sous-traitant | 8.2 Maîtrise de la sous-traitance et des prestataires de service |
| | | Article 29 | Traitement effectué sous l'autorité du responsable du traitement ou du sous-traitant | |
| | | Article 30 | Registre des activités de traitement | 7.3 Libération des produits et / ou des services |
| | | Article 31 | Coopération avec l'autorité de contrôle | 5.3 Obligations de conformité |
| | Sécurité des données à caractère personnel | Article 32 | Sécurité du traitement | 7.2 Conception et développement de produits et / ou de services<br>9.1 Infrastructure<br>9.2.2 Sensibilisation |
| | | Article 33 | Notification à l'autorité de contrôle d'une violation de données à caractère personnel | 5.5 Gestion des violations de données à caractère personnel |

| Chapitre | Section | Article | | Norme de certification |
|---|---|---|---|---|
| | | Article 34 | Communication à la personne concernée d'une violation de données à caractère personnel | 5.1 Management du risque relatif aux données à caractère personnel / Généralités<br>5.5 Gestion des violations de données à caractère personnel |
| | Analyse d'impact relative à la protection des donnés et consultation préalable | Article 35 | Analyse d'impact relative à la protection des données | 5.2 Analyse d'impact relative à la protection des données<br>8.1 Maîtrise du traitement |
| | | Article 36 | Consultation préalable | 4.3.2 Délégué à la protection des données |
| | Délégué à la protection des données | Article 37 | Désignation du délégué à la protection des données | 4.3 Rôles, responsabilités et autorités au sein de l'organisme<br>9.2.1 Compétences |
| | | Article 38 | Fonction du délégué à la protection des données | 4.3 Rôles, responsabilités et autorités au sein de l'organisme |
| | | Article 39 | Missions du délégué à la protection des données | 4.3 Rôles, responsabilités et autorités au sein de l'organisme |
| | Codes de conduite et certification | Article 40 | Codes de conduite | 0 |
| | | Article 41 | Suivi des codes de conduite approuvés | 1 ; 7.2 ; 6.8.2 ; 7.1.1 |
| | | Article 42 | Certification | 0 (Annexe 1) ; 1 |
| | | Article 43 | Organismes de certification | |
| Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales | | Article 44 | Principe général applicable aux transferts | 8.2 Maîtrise de la sous-traitance et des prestataires de service |
| | | Article 45 | Transferts fondés sur une décision d'adéquation | 8.2 Maîtrise de la sous-traitance et des prestataires de service |
| | | Article 46 | Transferts moyennant des garanties appropriées | 8.2 Maîtrise de la sous-traitance et des prestataires de service |
| | | Article 47 | Règles d'entreprise contraignantes | 6.8.2 / 7.1.1 / 7.2 + 3 Termes et définitions |
| | | Article 48 | Transferts ou divulgations non autorisés par le droit de l'Union | |
| | | Article 49 | Dérogations pour des situations particulières | |
| | | Article 50 | Coopération internationale dans le domaine de la protection des données à caractère personnel | |

## A propos de Bureau Veritas

Bureau Veritas est un leader mondial de l'inspection, de la certification et des essais en laboratoire. Créé en 1828, le Groupe emploie plus de 74000 collaborateurs dans environ 1400 bureaux et laboratoires situés dans le monde entier. Bureau Veritas aide ses clients à améliorer leurs performances, en offrant des services et des solutions innovantes pour s'assurer que leurs actifs, produits, infrastructures et processus répondent aux normes et réglementations relatives à la qualité, la santé, la sécurité, la protection de l'environnement et la responsabilité sociale.

BUREAU VERITAS CERTIFICATION HOLDING
Le Triangle de l'Arche - 8, Cours du Triangle, CS 900%
92937 Paris La Defense CEDEX
France