CPVP
Commission de la protection de la vie privée

LIGNES DIRECTRICES POUR LA SÉCURITÉ DE L'INFORMATION DE DONNÉES À CARACTÈRE PERSONNEL

Décembre 2014

Version : 2.0

Répartition des normes en deux parties :

- partie A – normes et mesures globales liées à la politique de gestion
- partie B – normes de mise en œuvre spécifiques/techniques

1 Champ d'application

1.1 Champ d'application général

Le document "Lignes directrices pour la sécurité de l'information de données à caractère personnel" définit les finalités de sécurité à respecter pour chaque institution – personne morale, entreprise ou administration – qui conserve, utilise, traite ou communique des données à caractère personnel et dont le traitement nécessite une autorisation préalable. Il promeut la culture de la sécurité telle que préconisée par l'OCDE dans son document "Lignes directrices régissant la sécurité des systèmes et réseaux d'information" et il s'inspire de la norme ISO 27002:2013[1], de la norme ISO 27005:2011[2] et de la norme ISO 27018:2014[3]. Il constitue un développement des mesures de référence de la Commission de la protection de la vie privée pour tous les traitements de données à caractère personnel soumis à une autorisation préalable. Les "*Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel*" sont disponibles sur le site Internet de la Commission vie privée et s'appliquent à tous les traitements de données à caractère personnel.

La mise en œuvre et la vérification des lignes directrices pour la sécurité auprès de tiers qui traitent des données à caractère personnel pour le compte d'une institution relèvent en premier lieu de la responsabilité de l'institution qui confie des tâches à ce tiers.

La loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après la Loi vie privée ou LVP) définit très précisément les conditions et les circonstances d'un traitement ou d'une transmission de données à caractère personnel. L'exécution de certains traitements, vu le caractère sensible des données, n'est toutefois pas possible sans autorisation préalable du comité sectoriel compétent de la Commission de protection de la vie privée. Chaque institution qui introduit une demande d'autorisation doit disposer d'une politique de sécurité qui repose sur ces lignes directrices pour la sécurité de l'information de données à caractère personnel et doit, le cas échéant, désigner un conseiller en sécurité de l'information (ci-après conseiller en sécurité).

[1] Code de bonne pratique pour le management de la sécurité de l'information.
[2] Gestion des risques liés à la sécurité de l'information.
[3] Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII.

1.2 Champs d'application particuliers

Pour les organismes de la sécurité sociale et les organismes qui recourent à l'intégrateur de services fédéral, les présentes lignes directrices sont applicables à la sécurité de l'information au sens large, telle que définie dans l'arrêté royal du 17 mars 2013 *relatif aux conseillers en sécurité institués par la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral* : "*stratégie, règles, procédures et moyens de protection de tout type d'information tant dans les systèmes de transmission que dans les systèmes de traitement en vue de garantir la confidentialité, la disponibilité, l'intégrité, la fiabilité, l'authenticité et l'irréfutabilité de l'information*". Autrement dit, cette définition ne concerne pas uniquement les données à caractère personnel, mais toutes les données.

En outre, conformément à l'article 2, premier alinéa, 2° de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, les organismes de la sécurité sociale sont obligés de respecter les normes minimales, telles que définies par la Banque-carrefour de la sécurité sociale.

2 Quelques définitions

Qu'est-ce que la sécurité de l'information ?

La sécurité de l'information est l'ensemble de mesures de gestion qui veillent à ce que la confidentialité, l'intégrité et la disponibilité de toutes les formes d'information – tant sous la forme électronique (numérique) que papier – soient maintenues, dans le but d'assurer la continuité des informations et de l'information et de limiter à un niveau acceptable prédéfini les éventuelles conséquences d'incidents en matière de sécurité de l'information.

Il y a lieu d'entendre par "mesure de gestion" toutes les mesures relatives à la politique, aux procédures, aux directives, aux méthodes et aux structures organisationnelles. Ces mesures peuvent être de nature aussi bien administrative ou technique que juridique ou relever de la gestion.

Conseiller en sécurité

Des comités sectoriels sont instaurés au sein de la Commission de la protection de la vie privée. Ils sont composés de membres de la Commission et d'experts qui sont spécifiquement familiarisés avec le secteur pour lequel le Comité est compétent. Actuellement, il existe cinq comités sectoriels. Pour pouvoir traiter certaines données à caractère personnel, une autorisation d'un ou de plusieurs de ces comités sectoriels est requise. Dans le cadre de ces procédures d'autorisation, la désignation d'un conseiller en sécurité doit parfois être communiquée au comité sectoriel compétent et/ou validée par lui.

Le conseiller en sécurité est l'instigateur et le moteur de la politique de sécurité de l'information. C'est lui qui fait des propositions, qui fixe les objectifs à atteindre, qui suit et conseille les différentes personnes qui interviennent lors de la mise en place du système de sécurisation, …. Il analyse et étudie les incidents de sécurité et propose des mesures de gestion. Il rapporte directement à la direction ou à la plus haute instance de décision.

Le site Internet de la Commission de la protection de la protection de la vie privée comporte un lexique où davantage de termes sont expliqués(voir http://www.privacycommission.be/fr/lexicon).

3 Interprétation des lignes directrices

3.1 Contrôle du respect des lignes directrices pour la sécurité de l'information

La Commission de la protection de la vie privée, la Commission de contrôle flamande, la Commission de contrôle bruxelloise, la Commission Wallonie-Bruxelles de contrôle des échanges de données et/ou chaque comité sectoriel compétent en la matière peuvent effectuer des contrôles ou faire effectuer par une instance externe des contrôles portant sur le respect d'aspects spécifiques des lignes directrices pour la sécurité de l'information de données à caractère personnel. Ces lignes directrices doivent être appliquées dans le cadre d'autorisations octroyées par chacun des comités sectoriels institués au sein de la Commission de la protection de la vie privée.

3.2 Interprétation et révision des lignes directrices pour la sécurité

Les lignes directrices pour la sécurité sont divisées en une partie A qui reprend les normes et mesures globales liées à la politique et en une partie B qui se compose des normes de mise en œuvre spécifiques et techniques.

Les institutions assument la responsabilité de mettre en œuvre les moyens de sécurité les plus indiqués en fonction de leur situation spécifique et selon l'importance des moyens de fonctionnement à sécuriser.

Enfin, il faut signaler que ces lignes directrices peuvent être révisées. Elles seront donc adaptées en fonction des évolutions sur le plan légal, technique, en particulier en ce qui concerne les risques en matière de sécurité, ou sur d'autres plans, en particulier les normes ISO.

4 Finalités poursuivies

Les lignes directrices pour la sécurité des données à caractère personnel constituent un fil conducteur qui permet de définir et de gérer un Information Security Management System (ci-après ISMS) documenté, c'est-à-dire constater, exécuter, contrôler, évaluer, tenir à jour et améliorer dans le cadre des activités et des risques d'exploitation liés au traitement de données à caractère personnel de l'institution. L'ISMS doit se baser sur le cercle de qualité de Deming qui consiste en quatre activités cycliques : PLAN (= regarder le fonctionnement actuel et projeter un plan d'amélioration du fonctionnement, toujours définir des finalités), DO (= exécuter l'amélioration envisagée), CHECK (= mesurer le résultat de l'amélioration et le confronter aux finalités prévues), ACT (= rectifier à l'aide des résultats trouvés dans Check). Dans ce contexte, la direction ou la plus haute instance de décision doit pouvoir fournir la preuve de son implication concernant la constatation, la mise en œuvre, l'exécution, le contrôle, l'évaluation, la mise à jour et l'amélioration de l'ISMS. L'efficacité de l'ISMS doit être continuellement améliorée en utilisant la politique de sécurité de l'information, les objectifs de la sécurité de l'information, les résultats d'audit, l'analyse d'événements contrôlés, des mesures de correction et de prévention et l'évaluation de la direction ou celle de la plus haute instance de décision.

Ces lignes directrices pour la sécurité veulent être pour tous les traitements à caractère personnel soumis à une autorisation préalable, une précision des mesures générales de référence que la Commission de la protection de la vie privée a édictées à l'égard de toutes les instances qui traitent des données à caractère personnel.

5 Lignes directrices – structure

Les lignes directrices pour la sécurité des données à caractère personnel s'inscrivent tant dans les buts que dans les principes des lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information. Elles s'inspirent de la norme ISO 27002:2013 (voir notamment http://www.iso27001security.com/html/27002.html), de la norme ISO 27005:2011 et de la norme ISO 27018:2014.
Les présentes lignes directrices sont subdivisées en 15 chapitres. Chaque chapitre traite d'un aspect déterminé de la sécurité de l'information et chaque point vise spécifiquement la sécurité de l'information lors de l'utilisation et du traitement de données à caractère personnel.

Une distinction est établie entre d'une part les normes globales et d'autre part le contenu technique de ces normes globales. Les concepts de base ou les normes et mesures globales liées à la politique sont repris dans la partie A, les modalités de mise en œuvre technique de la sécurité de l'information sont reprises dans la partie B.

PARTIE A – NORMES ET MESURES GLOBALES LIÉES À LA POLITIQUE

1 RISQUE ***(voir ISO 27005 – Gestion des risques liés à la sécurité de l'information)***	
1.1 APPRÉCIATION DU RISQUE LIÉ À LA SÉCURITÉ ***(voir ISO 27005 – 8 Appréciation du risque lié à la sécurité)***	
A-1.1.1	Après identification et analyse, il convient de réaliser régulièrement une appréciation du risque et des besoins liés à la sécurité relative aux informations qui sont propres à votre organisation et qui concernent l'utilisation et le traitement de données à caractère personnel, ce en concertation avec la plus haute instance de décision de votre organisation.
1.2 TRAITEMENT DU RISQUE LIÉ À LA SÉCURITÉ ***(voir ISO 27005 – 9 Traitement du risque lié à la sécurité)***	
A-1.2.1	Pour chaque risque pertinent relatif à l'utilisation et au traitement de données à caractère personnel constaté à l'issue de la phase d'appréciation du risque lié à l'information, les mesures de gestion nécessaires doivent être prises et un suivi doit être assuré.

2 POLITIQUE ***(voir ISO 27002 – 5 Politiques de sécurité de l'information)***	
2.1 POLITIQUE DE SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 5.1 Orientations de la direction en matière de sécurité de l'information)***	
A-2.1.1	Votre organisation doit disposer d'une politique de sécurité de l'information ("*information security policy*") formelle, actualisée et approuvée par la plus haute instance de décision de votre organisation, qui doit régulièrement être communiquée à toutes les parties concernées.
A-2.1.2	Il faut un soutien clair de la plus haute instance de décision de votre organisation pour initialiser, contrôler, entretenir et, au besoin, adapter la mise en œuvre de la sécurité de l'information au sein de votre organisation. Exemples de documents concernant la sécurité de l'information :

	- un rapport annuel en matière de sécurité de l'information ; - un plan pluriannuel en matière de sécurité de l'information.

3 ORGANISATION ***(voir ISO 27002 – 6 Organisation de la sécurité de l'information)***	
3.1 ORGANISATION INTERNE CONCERNANT LA SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 6.1 Organisation interne)***	
A-3.1.1	Votre organisation doit mettre à disposition les crédits et moyens de fonctionnement nécessaires afin de pouvoir assurer la coordination et l'exécution correctes de la politique de sécurité de l'information. Le suivi de l'exécution de la politique de sécurité doit être assuré par la cellule de sécurité de l'information, dirigée par un conseiller en sécurité. Ces tâches peuvent également être confiées à un service externe spécialisé et agréé. La cellule de sécurité de l'information a une mission de conseil, de stimulation, de documentation et de contrôle au sein de votre organisation. À cet effet, le conseiller en sécurité doit se charger : - de fournir des avis experts à la personne chargée de la gestion journalière et responsable du traitement des données ; - d'exécuter des missions qui lui sont confiées par la personne chargée de la gestion journalière et responsable du traitement des données.
A-3.1.2	Le conseiller en sécurité doit toujours disposer des compétences et des informations nécessaires pour exécuter sa mission correctement et en temps opportun.
A-3.1.3	Votre organisation doit disposer d'une plate-forme de décision active qui se réunit régulièrement pour la validation et l'approbation des mesures de gestion pour la sécurité de l'information, proposées par la cellule de sécurité de l'information.
A-3.1.4	Quel que soit le type de projet, votre organisation doit toujours intégrer la sécurité de l'information dans la ou les méthodes de gestion de projet afin d'identifier et d'aborder les risques en matière de sécurité de l'information.

3.2 Travail mobile ***(voir ISO 27002 – 6.2 Appareils mobiles et télétravail)***	
A-3.2.1	Votre organisation doit disposer d'une politique formelle en matière d'utilisation d'appareils mobiles, en tenant compte des risques du travail dans des environnements non protégés. Les collaborateurs qui utilisent des appareils mobiles doivent être formés afin (1) qu'ils soient conscients des risques supplémentaires qu'entraîne cette manière de travailler et (2) qu'ils sachent quelles mesures de gestion doivent être prises.
A-3.2.2	Les organisations qui accordent le télétravail doivent édicter une politique définissant les conditions et restrictions relatives au télétravail.

4 RESSOURCES HUMAINES ***(voir ISO 27002 – 7 (La sécurité des ressources humaines)***	
4.1 SÉCURITÉ DE L'INFORMATION AVANT L'EMBAUCHE ***(voir ISO 27002 – 7.1 Avant l'embauche***	
A-4.1.1	Lors du processus de recrutement, votre organisation doit clairement signaler aux candidats potentiels l'importance de la sécurité de l'information.
A-4.1.2	Tous les candidats doivent signer leur contrat de travail dans lequel figurent également des clauses relatives à leurs responsabilités en matière de sécurité de l'information des données à caractère personnel.
4.2 SÉCURITÉ DE L'INFORMATION PENDANT LA DURÉE DU CONTRAT ***(voir ISO 27002 – 7.2 Pendant la durée du contrat)***	
A-4.2.1	Pour garantir que tous les collaborateurs internes s'engagent à respecter leurs obligations en matière de confidentialité et de sécurité des données à caractère personnel, votre organisation doit informer tous les collaborateurs internes impliqués dans l'utilisation et le traitement des données à caractère personnel quant aux obligations de confidentialité et de sécurité sous la forme : - d'un code de bonne conduite ; - et/ou de la mention de ce code de bonne conduite dans le règlement de travail ; - et/ou d'une description de fonction avec mention des obligations de confidentialité et de sécurité ; - et/ou de clauses contractuelles ; - et en outre, sous la forme d'une formation et d'une sensibilisation appropriées et d'un recyclage régulier.

A-4.2.2	Votre organisation doit informer tous les collaborateurs externes (contractants et utilisateurs tiers) chargés de l'utilisation et/ou du traitement des données à caractère personnel de leurs obligations de confidentialité et de sécurité par le biais d'un code de conduite et en leur demandant de signer un document contractuel reprenant des clauses contractuelles claires.
A-4.2.3	Votre organisation doit disposer d'une procédure disciplinaire formelle et connue de tous destinée à prendre des mesures à l'encontre de collaborateurs ayant enfreint les règles liées à la sécurité de l'information.
4.3 SÉCURITÉ DE L'INFORMATION EN CAS DE RUPTURE, TERME OU MODIFICATION DU CONTRAT DE TRAVAIL ***(voir ISO 27002 – 7.3 Rupture, terme ou modification du contrat de travail)***	
A-4.3.1	Votre organisation doit définir les responsabilités et les missions liées à la sécurité de l'information qui restent valables à l'issue de la rupture, du terme ou de la modification du contrat de travail, en informer le salarié ou le contractant et veiller à leur application.

5 ACTIFS ***(voir ISO 27002 – 8 Gestion des actifs)***	
5.1 CLASSIFICATION DE L'INFORMATION ***(voir ISO 27002 – 8.2 Classification de l'information)***	
A-5.1.1	Lors des traitements de données à caractère personnel, votre organisation doit établir une distinction claire entre les types de données suivants : - données anonymes : ce sont les données qui ne peuvent être mises en relation avec une personne identifiée ou identifiable et qui ne sont donc pas des données à caractère personnel ; - données à caractère personnel : une donnée à caractère personnel est toute information concernant une personne physique identifiée ou identifiable ; - données à caractère personnel sensibles : il s'agit de données relatives à la race, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, à la santé, à la vie sexuelle, à des suspicions, des poursuites ou des condamnations pénales ou administratives. Il est en principe interdit de traiter de telles données ; - données à caractère personnel codées, sensibles ou non : ce sont des données à caractère personnel qui ne peuvent être reliées à une personne identifiée ou identifiable qu'au moyen d'un code.
A-5.1.2	Tous les utilisateurs qui utilisent/traitent des données à caractère personnel doivent connaître cette distinction.

5.2 MANIPULATION DES SUPPORTS ***(voir ISO 27002 – 8.3 Manipulation des supports)***	
A-5.2.1	Votre organisation doit disposer de procédures pour la gestion de supports amovibles sur lesquels sont stockées des données à caractère personnel et qui peuvent quitter le périmètre de sécurité de votre organisation. Pensez ici aussi aux supports amovibles dans le matériel comme les imprimantes et les photocopieuses multifonctions.
A-5.2.2	Votre organisation doit définir les mesures nécessaires pour protéger durant leur transport les supports physiques (en ce compris les documents papier) comportant des données à caractère personnel contre les accès non autorisés, les abus ou la corruption.

6 ACCÈS À DES DONNÉES À CARACTÈRE PERSONNEL ***(voir ISO 27002 – 9 Contrôle d'accès)***	
6.1 EXIGENCES RELATIVES AU CONTRÔLE D'ACCÈS ***(voir ISO 27002 – 9.1 Exigences métier en matière de contrôle d'accès)***	
A-6.1.1	Votre organisation doit disposer d'une politique de contrôle des accès approuvée et actualisée concernant l'octroi, la modification et la suppression de droits d'accès à des applications et à des systèmes qui utilisent/traitent des données à caractère personnel. Cette politique doit être établie, documentée et examinée sur la base de la classification des données à caractère personnel.
A-6.1.2	En ce qui concerne les réseaux ou services de réseau, votre organisation doit définir les mesures de sécurité adéquates afin que chacun n'ait accès qu'aux données à caractère personnel pour lesquelles il a expressément reçu une autorisation.
6.2 RESPONSABLE DES DROITS D'ACCÈS DES UTILISATEURS ***(voir ISO 27002 – 9.2 Gestion de l'accès utilisateur)***	
A-6.2.1	Votre organisation doit désigner un responsable chargé de la gestion de toutes les demandes relatives à l'accès à des données à caractère personnel. Ce responsable doit être différent de la personne qui octroie, adapte ou supprime les droits d'accès au niveau technique dans les systèmes.

6.3 RESPONSABILITÉS DES UTILISATEURS ***(voir ISO 27002 – 9.3 Responsabilités des utilisateurs)***	
A-6.3.1	Les utilisateurs doivent être informés de leur responsabilité dans le cadre d'une sécurisation des accès efficace, notamment concernant l'utilisation de mots de passe et la sécurité du matériel sur lequel des données à caractère personnel sont utilisées/traitées.
6.4 CONTRÔLE DE L'ACCÈS AU SYSTÈME ET AUX APPLICATIONS ***(voir ISO 27002 – 9.4 Contrôle de l'accès au système et aux applications)***	
A-6.4.1	Votre organisation doit définir des mesures de protection appropriées pour limiter l'accès aux données à caractère personnel.
A-6.4.2	Votre organisation doit limiter l'accès des gestionnaires d'informations (gestionnaires de systèmes, également appelés "superusers") aux systèmes et applications sur lesquels les données à caractère personnel sont utilisées/traitées.

7 CRYPTOGRAPHIE ***(voir ISO 27002 – 10 Cryptographie)***	
7.1 MESURES CRYPTOGRAPHIQUES ***(voir ISO 27002 – 10.1 Mesures cryptographiques)***	
A-7.1.1	En fonction des résultats de l'analyse des risques, votre organisation doit élaborer une politique pour une utilisation correcte et efficace de la cryptographie afin de protéger la confidentialité, l'authenticité et/ou l'intégrité des données à caractère personnel.
A-7.1.2	Votre organisation doit élaborer une politique pour l'utilisation, la protection et la longévité de clés cryptographiques tout au long de leur cycle de vie.

8 SÉCURITÉ PHYSIQUE ***(voir ISO 27002 – 11 Sécurité physique et environnementale)***	
8.1 SÉCURITÉ ENVIRONNEMENTALE ***(voir ISO 27002 – 11.1 Zones sécurisées)***	
A-8.1.1	En fonction des résultats de l'analyse des risques, des zones sécurisées ainsi que les contrôles d'accès appropriés doivent être définis afin de protéger tous les espaces où se trouvent des informations ainsi que des dispositifs de traitement d'informations contenant des données à caractère personnel.
A-8.1.2	Votre organisation doit définir les mesures nécessaires relatives aux zones sécurisées afin d'éviter toute forme de dommage pouvant mettre en péril les données à caractère personnel.
8.2 MATÉRIEL SÉCURISÉ ***(voir ISO 27002 – 11.2 Matériels)***	
A-8.2.1	Votre organisation doit définir, sur la base de l'analyse des risques, les mesures de gestion appropriées relatives au matériel, au câblage et aux équipements de support afin d'empêcher la perte, les dommages, le vol et la modification non souhaitée de données à caractère personnel. À cet égard, il convient d'accorder une attention particulière au matériel qui se trouve ou qui est utilisé hors du site de l'organisation.
A-8.2.2	Votre organisation doit élaborer une procédure spécifique pour la mise au rebut ou le recyclage de tout le matériel équipé de supports de stockage sur lesquels sont utilisées/traitées des données à caractère personnel.

9 SÉCURITÉ OPÉRATIONNELLE ***(voir ISO 27002 – 12 Sécurité liée à l'exploitation)***	
9.1 PROCÉCURES OPÉRATIONNELLES ET RESPONSABILITÉS CONCERNANT LA SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 12.1 Procédures et responsabilités liées à l'exploitation)***	
A-9.1.1	Votre organisation doit définir les procédures et responsabilités nécessaires lors de changements dans l'organisation, les processus d'exploitation, les équipements de traitement des informations et les systèmes qui ont une influence sur la sécurité de l'information de données à caractère personnel.

A-9.1.2	Votre organisation doit prévoir une séparation de fonctions afin d'éviter qu'une seule personne obtienne le contrôle exclusif d'un traitement de données à caractère personnel.
9.2 PROTECTION CONTRE LES LOGICIELS MALVEILLANTS ***(voir ISO 27002 – 12.2 Protection contre les logiciels malveillants)***	
A-9.2.1	Votre organisation doit disposer de procédures et de directives appropriées de protection contre les logiciels malveillants pour augmenter la sensibilisation des utilisateurs du système et des utilisateurs finaux. Quelques exemples de directives et de procédures possibles : • interdire l'utilisation de programmes non-autorisés ; • définir une politique en matière de réception de fichiers et de programmes provenant de réseaux externes ou reçus via ces réseaux ou via tout autre support ; • établir les responsabilités en matière de protection contre les logiciels malveillants.
9.3 SAUVEGARDE ***(voir ISO 27002 – 12.3 Sauvegarde)***	
A-9.3.1	Votre organisation doit rédiger une politique de sauvegarde appropriée et en assurer le suivi afin de garantir une restauration adéquate après une perte, des dommages, un vol ou une modification non souhaitée de données à caractère personnel.

10 SÉCURITÉ DES COMMUNICATIONS ***(voir ISO 27002 – 13 Sécurité des communications)***	
10.1 SÉCURITÉ DES RÉSEAUX ***(voir ISO 27002 – 13.1 Management de la sécurité des réseaux)***	
A-10.1.1	La sécurité des réseaux doit constituer un élément de votre plan global de sécurité de l'information qui doit consacrer une attention particulière aux flux d'informations au cours desquels des données à caractère personnel peuvent sortir de votre organisation.
10.2 TRANSFERT DE L'INFORMATION ***(voir ISO 27002 – 13.2 Transfert de l'information)***	
A-10.2.1	Votre organisation doit disposer d'une politique formelle, actualisée et approuvée par la plus haute instance de décision de votre organisation en matière de moyens de communication (comme l'e-mail, l'Internet, la vidéo, le fax et le téléphone) qui est régulièrement communiquée à toutes les

	parties concernées et dans laquelle on consacre une attention particulière à l'utilisation de données à caractère personnel. Nous renvoyons également à cet égard à la recommandation n° 8/2012 de la Commission vie privée *relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail*.
A-10.2.2	Votre organisation doit définir, évaluer régulièrement et documenter les exigences pour les engagements de confidentialité ou de non-divulgation qui reflètent les besoins de votre organisation quant à la protection des données à caractère personnel.

11 ACQUISITION, DÉVELOPPEMENT ET MAINTENANCE DES SYSTÈMES D'INFORMATION ***(voir ISO 27002 – 14 Acquisition, développement et maintenance des systèmes d'information)***	
11.1 EXIGENCES DE SÉCURITÉ APPLICABLES AUX SYSTÈMES D'INFORMATION ***(voir ISO 27002 – 14.1 Exigences de sécurité applicables aux systèmes d'information)***	
A-11.1.1	Votre organisation doit veiller à ce que les exigences de sécurité pour les données à caractère personnel restent toujours garanties lors de l'acquisition ou du développement de nouveaux systèmes d'information ou en cas d'extensions de systèmes d'information existants. On entend par systèmes d'information des applications, services, moyens IT ou autres éléments de traitement de l'information.
11.2 SÉCURITÉ DES PROCESSUS DE DÉVELOPPEMENT ET D'ASSISTANCE TECHNIQUE ***(voir ISO 27002 – 14.2 Sécurité des processus de développement et d'assistance technique)***	
A-11.2.1	Votre organisation doit disposer de procédures pour le développement de nouveaux systèmes ou pour des évolutions importantes de systèmes existants afin que le responsable de projet tienne compte des exigences de sécurité impérieuses relatives à la protection des données à caractère personnel.
A-11.2.2	Votre organisation doit appliquer des procédures de modification formelles et claires afin de limiter au minimum le risque de modifications erronées ou la fuite de données à caractère personnel.

12 RELATIONS AVEC LES FOURNISSEURS ***(voir ISO 27002 – 15 Relations avec les fournisseurs)***	
12.1 SÉCURITÉ DE L'INFORMATION DANS LES RELATIONS AVEC LES FOURNISSEURS ***(voir ISO 27002 – 15.1 Sécurité de l'information dans les relations avec les fournisseurs)***	
A-12.1.1	En cas de collaboration avec des fournisseurs, votre organisation doit s'assurer que le fournisseur offre suffisamment de garanties en matière de sécurité de l'information des données à caractère personnel et que les obligations relatives à l'utilisation et au traitement de données à caractère personnel soient établies contractuellement (cf. l'article 16, § 1 de la loi vie privée).
A-12.1.2	Si votre organisation envisage, pour le stockage, l'utilisation et/ou le traitement de données à caractère personnel, de recourir aux services d'un fournisseur du "cloud", elle doit réaliser une analyse des risques relative à la conformité de la sécurité de l'information proposée avec les présentes lignes directrices et les conditions contractuelles (en particulier un éventuel accès aux données à caractère personnel par des tiers ainsi que des garanties contractuelles minimales relatives par exemple à des règles d'audit, la continuité et la qualité du service, l'interopérabilité et la réversibilité/la transmissibilité).

13 GESTION DES INCIDENTS LIÉS À LA SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 16 Gestion des incidents liés à la sécurité de l'information)***	
13.1 GESTION DES INCIDENTS LIÉS À LA SÉCURITÉ DE L'INFORMATION ET AMÉLIORATIONS ***(voir ISO 27002 – 16.1 Gestion des incidents liés à la sécurité de l'information et améliorations)***	
A-13.1.1	Les responsabilités et les procédures doivent être définies concernant la détection et le traitement d'incidents liés à la sécurité de l'information et de failles impliquant des données à caractère personnel qui sont rapportés.
A-13.1.2	Votre organisation doit veiller à ce que la cellule de sécurité de l'information/le responsable du traitement soit toujours directement informé(e) d'événements et d'incidents pouvant compromettre ou ayant compromis la sécurité de l'information de données à caractère personnel.
A-13.1.3	Votre organisation doit veiller à ce que la cellule de sécurité de l'information/le responsable du traitement soit toujours directement informé(e) des failles détectées ou supposées dans la sécurité des systèmes ou des services concernés par le traitement de données à caractère personnel.
A-13.1.4	Votre organisation doit disposer d'une procédure formelle et actualisée pour le signalement d'événements liés à la sécurité de l'information, combinée à une procédure de réaction et de remontée d'information pour les incidents impliquant des données à caractère personnel. En cas d'incident public, il est

	recommandé de procéder à un signalement auprès des instances compétentes, conformément à la recommandation n° 01/2013 de la Commission vie privée. Il convient plus particulièrement, conformément à la loi du 13 juin 2005 *relative aux communications électroniques*, de veiller au respect de l'obligation de notification s'il s'agit d'un incident public dans le secteur des télécommunications.
A-13.1.5	La cellule de sécurité de l'information/le responsable du traitement doit être systématiquement informé(e) de toutes les mesures qui sont prises pour faire face aux incidents liés à la sécurité de l'information et aux failles impliquant des données à caractère personnel.

14 CONTINUITÉ DE L'ACTIVITÉ ***(voir ISO 27002 – 17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité)***	
14.1 CONTINUITÉ DE LA SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 17.1 Continuité de la sécurité de l'information)***	
A-14.1.1	Sur la base d'une évaluation des risques, votre organisation doit définir les mesures nécessaires pour garantir la continuité de la sécurité de l'information des données à caractère personnel.
14.2 REDONDANCES	
A-14.2.1	En fonction des exigences de votre organisation, il convient de mettre en œuvre des moyens de traitement de l'information avec suffisamment de redondances pour garantir la disponibilité des données à caractère personnel. Il faut à cet égard tenir compte de risques supplémentaires en matière de sécurité de l'information suite à la redondance.

15 CONFORMITÉ ***(voir ISO 27002 – 18 Conformité)***	
15.1 RESPECT DES PRESCRIPTIONS LÉGALES ***(voir ISO 27002 – 18.1 Conformité aux obligations légales et contractuelles)***	
A-15.1.1	Votre organisation doit toujours respecter toutes les lois et les règles en vigueur concernant le traitement et la protection des données à caractère personnel. Il faut au moins respecter les dispositions reprises dans la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (Loi vie privée) et son arrêté d'exécution (AR du 13 février 2001). En fonction du traitement de données, ce cadre légal est complété par une législation spécifique :

	• Arrêté royal du 17 décembre 2003 *fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la Commission de la protection de la vie privée* ; • Loi du 8 août 1983 *organisant un registre national des personnes physiques* ; • Loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* ; • Loi du 16 janvier 2003 *portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses dispositions* ; • Loi du 4 juillet 1962 *relative à la statistique publique* ; • Loi du 13 juin 2005 *relative aux communications électroniques* ; • Loi du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral* ; • Loi du 5 mai 2014 *garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier* ; • Arrêté royal du 12 août 1993 *relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale* ; • Arrêté royal du 17 mars 2013 *relatif aux conseillers en sécurité institués par la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral* ; • Arrêté royal du 7 juin 2007 *fixant les modalités relatives à la composition et au fonctionnement du Comité de surveillance statistique institué au sein de la Commission de la protection de la vie privée* ; • Circulaire du 9 janvier 2002 *relative à l'accès aux informations enregistrées dans le Registre national des personnes physiques et aux mesures en vue de garantir la sécurité des données* ; • Circulaire du 24 septembre 2007 : *Obligations incombant aux responsables de traitement* ; • Circulaire du 12 mars 2008 : *Protection de la vie privée à l'égard des traitements de données à caractère personnel - Accès aux informations du Registre national - Mesures de sécurité visant à garantir la confidentialité et l'intégrité des données, l'authentification des utilisateurs et la conservation de la trace des activités exécutées sur les systèmes d'information* ; • Circulaire du 10 juillet 2008 : *Protection de la vie privée à l'égard des traitements de données à caractère personnel - Accès aux informations du Registre national – Respect des finalités pour lesquelles l'autorisation d'accéder aux informations du Registre national ou d'en obtenir communication a été accordée.*
A-15.1.2	Avant d'acquérir ou de développer un système qui utilise/traite des données à caractère personnel, votre organisation doit systématiquement vérifier si une autorisation (sous la forme ou non d'une adhésion) est requise. Si tel est le cas, elle doit prendre des mesures pour satisfaire à toutes les obligations, en particulier la mention de l'identité du conseiller en sécurité et la description de la politique de sécurité à l'égard du comité sectoriel en question et au moyen des formulaires prescrits par ce même comité.

A-15.1.3	Votre organisation doit disposer de procédures actualisées pour l'élaboration et l'entretien de la documentation qui concerne la (les) autorisation(s) accordée(s).
A-15.1.4	Votre organisation doit disposer d'une approche approuvée pour vérifier que l'autorisation reste respectée lors de toute modification de l'application qui utilise/traite des données à caractère personnel pour laquelle cette autorisation a été accordée.
15.2 ÉVALUATIONS DE LA SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 18.2 Revue de la sécurité de l'information)***	
A-15.2.1	Votre organisation doit régulièrement organiser un audit de qualité concernant la sécurité de l'information des données à caractère personnel. Cet audit doit porter sur les domaines suivants des présentes lignes directrices : - analyse des risques ; - politique liée à la sécurité de l'information ; - organisation de la sécurité de l'information ; - exigences de sécurité concernant le personnel ; - gestion des actifs ; - sécurité logique des accès ; - mesures cryptographiques ; - sécurité physique ; - gestion opérationnelle ; - entretien et développement des systèmes d'information ; - sécurité de l'information dans les relations avec les fournisseurs ; - gestion des incidents liés à la sécurité de l'information ; - processus de gestion de la continuité de l'activité ; - conformité.

PARTIE B – NORMES DE MISE EN OEUVRE SPÉCIFIQUES/TECHNIQUES

3 ORGANISATION ***(voir ISO 27002 – 6 Organisation de la sécurité de l'information)***	
3.2 Travail mobile ***(voir ISO 27002 – 6.2 Appareils mobiles et télétravail)***	
B-3.2.1	Il convient de mettre en œuvre les mesures de gestion nécessaires permettant d'autoriser l'utilisation mobile des ordinateurs (y compris d'autres moyens mobiles) et le télétravail de manière sûre. Ces mesures peuvent notamment se rapporter à : • des techniques cryptographiques ; • des sauvegardes ; • la protection contre les logiciels malveillants ; • le contrôle des accès en cas d'accès externe à des données à caractère personnel ; • la protection physique contre le vol d'équipements informatiques portables (y compris les moyens mobiles) et des espaces de télétravail.

4 RESSOURCES HUMAINES ***(voir ISO 27002 – 7 La sécurité des ressources humaines)***	
4.2 SÉCURITÉ DE L'INFORMATION PENDANT LA DURÉE DU CONTRAT **(voir ISO 27002 – 7.2 Pendant la durée du contrat)**	
B-4.2.1	Toutes les mesures adéquates doivent être mises en œuvre afin d'empêcher que des données à caractère personnel ne quittent votre organisation sans contrôle et ne tombent entre des mains non autorisées. Notamment en : - protégeant les biens contre un accès, une diffusion, une modification, une destruction ou une intrusion non autorisés ; - exécutant des activités ou des processus de sécurité particuliers ; - garantissant que la responsabilité des actes posés soit toujours clairement attribuée à une personne ; - signalant des événements de sécurité ou des événements potentiels ou d'autres risques liés à la sécurité.

4.3 SÉCURITÉ DE L'INFORMATION LORS DU TERME OU DE LA MODIFICATION DU CONTRAT DE TRAVAIL ***(voir ISO 27002 – 7.3 Rupture, terme ou modification du contrat de travail)***	
B-4.3.1	Lors d'une modification des responsabilités dans le cadre de la participation au traitement de données à caractère personnel, il faut effectuer les adaptations nécessaires aux mesures de sécurité de l'information, telles que reprises aux points 5.1.3 et 6.1.2.

5 ACTIFS ***(voir ISO 27002 – 8 Gestion des actifs)***	
5.1 RESPONSABILITÉS RELATIVES AUX ACTIFS ***(voir ISO 27002 – 8.1 Responsabilités relatives aux actifs)***	
B-5.1.1	Un inventaire actualisé des actifs pertinents relatifs aux traitements de données à caractère personnel doit être établi en collaboration avec les services opérationnels concernés. Les moyens pertinents sont notamment : - l'information ; - les logiciels ; - les moyens physiques ; - les services ; - tous les utilisateurs (y compris les droits d'accès). -
B-5.1.2	Dans cet inventaire, chaque actif pertinent relatif à un traitement de données à caractère personnel doit être couplé à une fonction/personne déterminée au sein de votre organisation (responsabilité).
B-5.1.3	Lors de la fin d'un contrat avec un travailleur, un contractant ou un utilisateur externe, une procédure formelle doit être appliquée pour la restitution notamment de tous les actifs fournis (comme les programmes, les documents d'entreprise, les équipements et badges d'accès). Dans le cas de l'utilisation de matériel personnel, des mesures appropriées doivent être appliquées pour le transfert de toutes les informations pertinentes à l'organisation et la suppression correcte des informations figurant sur le matériel.
5.2 CLASSIFICATION DE L'INFORMATION ***(voir ISO 27002 – 8.2 Classification de l'information)***	
B-5.2.1	Lors de l'utilisation et du traitement de données à caractère personnel, il faut clairement tenir compte de la distinction entre les types de données suivants : • données anonymes ;

	• données à caractère personnel ; • données à caractère personnel sensibles ; • données à caractère personnel codées, sensibles ou non.
5.3 MANIPULATION DES SUPPORTS ***(voir ISO 27002 – 8.3 Manipulation des supports)***	

B-5.3.1	Lors de l'utilisation de supports amovibles ou d'autres supports sur lesquels sont stockées des données à caractère personnel, il faut prendre les mesures de gestion adéquates. En voici quelques exemples :
	• si les supports amovibles quittent le périmètre de sécurité :
	  o les données à caractère personnel stockées doivent être supprimées si elles ne sont plus nécessaires ;
	  o pour les données à caractère personnel, il faut obtenir au préalable un accord et tenir un registre ;
	• n'autoriser l'accès à des postes munis de supports amovibles que si cela est nécessaire pour des raisons de service ;
	• la conservation de données à caractère personnel sur des supports amovibles doit être conforme à la durée de vie du support. Si la durée de conservation dépasse la durée de vie, les données doivent également être stockées ailleurs.

B-5.3.2	Il convient de mettre en œuvre les mesures appropriées destinées à protéger, durant leur transport, les supports physiques (en ce compris les documents papier) comportant des données à caractère personnel contre les accès non autorisés, les abus ou la corruption. Voici des exemples de mesures : • recourir à des services de transport ou de courrier fiables ; • développer des procédures afin de vérifier l'identification des services de courrier ; • utiliser des emballages adéquats pour protéger le contenu contre des dommages physiques lors du transport ; • tenir une journalisation du transport, de la réception et de l'identification du contenu et de la protection du contenu qui a été appliquée.

6 ACCÈS À DES DONNÉES À CARACTÈRE PERSONNEL **(voir ISO 27002 – 9 Contrôle d'accès)**	
6.1 EXIGENCES EN MATIÈRE DE CONTRÔLE D'ACCÈS ***(voir ISO 27002 – 9.1 Exigences métier en matière de contrôle d'accès)***	
B-6.1.1	Vos gestionnaires de réseaux doivent mettre en œuvre les mesures de protection définies si un accès est accordé à des données à caractère personnel via des réseaux ou des services de réseau.

B-6.1.2	Les droits d'accès de tous les travailleurs et utilisateurs externes aux informations et aux équipements de traitement des informations doivent être supprimés ou adaptés, respectivement lors du terme ou de la modification du contrat de travail, du contrat ou de la convention.
6.4 CONTRÔLE DE L'ACCÈS AU SYSTÈME ET AUX APPLICATIONS ***(voir ISO 27002 – 9.4 Contrôle de l'accès au système et aux applications)***	
B-6.4.1	Par application de la société sur la base des exigences de sécurité, votre service informatique doit prendre les mesures de protection nécessaires pour limiter l'accès aux données à caractère personnel. Cela doit se faire au moyen d'un système : - d'identification (qui êtes-vous ?) ; - d'authentification (de quelle manière prouvez-vous qui vous êtes ?) ; - et d'autorisation (que pouvez-vous faire ?).
B-6.4.2	L'accès de vos gestionnaires d'informations (gestionnaires de systèmes, également appelés "superusers") aux systèmes informatiques sur lesquels les données à caractère personnel sont utilisées/traitées doit être limité au moyen d'une : - identification (qui êtes-vous ?) ; - authentification (de quelle manière prouvez-vous qui vous êtes ?) ; - et autorisation (que pouvez-vous faire en tant que superuser ?).

7 CRYPTOGRAPHIE ***(voir ISO 27002 – 10 Cryptographie)***	
7.1 MESURES CRYPTOGRAPHIQUES ***(voir ISO 27002 – 10.1 Mesures cryptographiques)***	
B-7.1.1	Les mesures cryptographiques établies doivent être mises en œuvre pour protéger la confidentialité, l'authenticité et l'intégrité des données à caractère personnel.
A-7.1.2	La politique relative à la gestion de clés cryptographiques doit être appliquée avec minutie toute au long du cycle de vie.

8 SÉCURITÉ PHYSIQUE ***(voir ISO 27002 – 11 Sécurité physique et environnementale)***	
8.1 SÉCURITÉ ENVIRONNEMENTALE ***(voir ISO 27002 – 11.1 Zones sécurisées)***	
B-8.1.1	L'accès aux espaces sécurisés (où des données à caractère personnel se trouvent ou sont utilisées/traitées) doit être strictement limité aux personnes habilitées désignées par votre organisation en appliquant les contrôles d'accès établis. Cet aspect doit faire l'objet d'un contrôle régulier par le responsable désigné, aussi bien pendant qu'en dehors des heures de travail normales (journal de bord ou dossier de journalisation).
B-8.1.2	Les mesures appropriées doivent être prises pour éviter les dégâts causés par le feu, les inondations, l'explosion,… bref, toute forme de calamités naturelles ou occasionnées par l'homme. Voici quelques exemples de mesures : • faire correspondre le compartimentage coupe-feu avec la détection de zones sécurisées ; • prévoir la détection incendie et les extincteurs adaptés et en contrôler régulièrement le fonctionnement ; • séparer l'entreposage des supports pour les sauvegardes et du matériel de réserve de la zone sécurisée.
8.2 MATÉRIEL SÉCURISÉ ***(voir ISO 27002 – 11.2 Matériels)***	
B-8.2.1	Le matériel doit être protégé contre des menaces physiques et des dangers de l'extérieur. Une attention particulière doit être accordée au matériel qui se trouve ou est utilisé hors du site de l'organisation. Il faut notamment faire attention : • au placement et à la protection du matériel de manière à ce qu'il soit protégé contre les risques de dommages et de pannes provenant de l'extérieur et à ce que l'accès par des personnes non habilitées soit évité ; • à la protection contre une panne de courant et d'autres pannes résultant d'une interruption des équipements d'utilité publique ; • à la sécurisation des câbles d'alimentation et de télécommunication contre une interception ou une dégradation ; • à l'entretien du matériel.
B-8.2.2	Tout matériel équipé de supports de stockage doit être contrôlé en cas de la mise au rebut ou de recyclage afin que toutes les données à caractère personnel soient écrasées ou supprimées de manière sécurisée. Si ce matériel contient des données à caractère personnel sensibles, des mesures spécifiques doivent être prises pour détruire physiquement ce matériel ou supprimer les informations au moyen de techniques qui rendent impossible toute récupération.

9 SÉCURITÉ OPÉRATIONNELLE ***(voir ISO 27002 – 12 Sécurité liée à l'exploitation)***	
9.1 PROCÉCURES OPÉRATIONNELLES ET RESPONSABILITÉS CONCERNANT LA SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 12.1 Procédures et responsabilités liées à l'exploitation)***	
B-9.1.1	Pour garantir une utilisation correcte et sûre des équipements de traitement des informations qui utilisent/traitent des données à caractère personnel, des procédures d'utilisation doivent être documentées et mises à disposition de tous les utilisateurs qui en ont besoin.
B-9.1.2	Conformément à la recommandation n° 01/2013 de la Commission vie privée, il doit y avoir une séparation stricte entre les environnements de développement, de test, d'acceptation/d'intégration et de production afin de réduire le risque d'accès non autorisé à l'environnement de développement ou de modifications de ce dernier. Cela implique notamment qu'aucun test ni développement ne soient effectués dans l'environnement de production. On ne peut déroger à cette règle que dans des cas exceptionnels à des fins de test, à condition que les mesures appropriées soient prises.
9.2 PROTECTION CONTRE LES LOGICIELS MALVEILLANTS ***(voir ISO 27002 – 12.2 Protection contre les logiciels malveillants)***	
B-9.2.1	Pour la protection contre les logiciels malveillants (prévention, détection et suppression/restauration), votre service informatique doit installer et mettre régulièrement à jour des logiciels anti-malware et de restauration, en scannant préventivement ou régulièrement les ordinateurs et médias. Le scan exécuté comporte notamment une vérification de la présence de logiciels malveillants : - dans tous les fichiers reçus via des réseaux ou via toute forme de média de stockage, et ce avant leur utilisation ; - dans des annexes et téléchargements, avant leur utilisation, et ce aux différents endroits cruciaux dans votre configuration réseau (serveurs mail, ordinateurs, accès réseau, …) ; - sur les pages Internet. Des messages d'avertissement donnant des informations précises en cas de réelle menace peuvent accroître la sensibilisation des utilisateurs.
9.3 SAUVEGARDE ***(voir ISO 27002 – 12.3 Sauvegarde)***	
B-9.3.1	Vos responsables de la gestion des sauvegardes doivent effectuer régulièrement des sauvegardes complètes et contrôlées des données à caractère personnel et doivent contrôler régulièrement s'ils sont en mesure de pouvoir réutiliser ces sauvegardes ("*restore*").

B-9.3.2	Vos responsables de la gestion des sauvegardes doivent prendre les mesures nécessaires pour garantir la confidentialité, l'intégrité et l'accessibilité relatives aux données de sauvegarde.
9.4 MONITORING ***(voir ISO 27002 – 12.4 Journalisation et surveillance)***	
B-9.4.1	Pour l'utilisation et le traitement de données à caractère personnel, des fichiers de journalisation clairs et protégés doivent être créés, conformément aux mesures de référence de la Commission vie privée. Les fichiers de journalisation doivent notamment contenir les activités, exceptions et événements.
B-9.4.2	Le responsable désigné par votre organisation doit disposer d'une liste actualisée de toutes les personnes et de leurs niveaux d'accès respectifs aux données à caractère personnel.
9.5 CONSIDÉRATIONS SUR L'AUDIT DU SYSTÈME D'INFORMATION ***(voir ISO 27002 – 12.7 Considérations sur l'audit du système d'information)***	
B-9.5.1	Il faut prendre les mesures de gestion et de sécurité appropriées pour éviter des fuites de données, une perte de données à caractère personnel, une dégradation des données et des perturbations des processus d'exploitation lors d'audits des systèmes d'information.

10 SÉCURITÉ DES COMMUNICATIONS ***(voir ISO 27002 – 13 Sécurité des communications)***	
10.1 SÉCURITÉ DES RÉSEAUX ***(voir ISO 27002 – 13.1 Management de la sécurité des réseaux)***	
B-10.1.1	Vos gestionnaires de réseaux doivent prendre des mesures de sécurité pour protéger les différents réseaux auxquels le matériel (qui traite les données à caractère personnel) est connecté.
B-10.1.2	Vos gestionnaires de réseaux doivent prendre les mesures de gestion nécessaires au niveau des réseaux de l'information pour : - garantir la confidentialité et l'intégrité concernant les données à caractère personnel, et - prévenir un accès non autorisé ; - répondre aux exigences de disponibilité et de capacité.

B-10.1.3	Vos gestionnaires de réseaux doivent tenir à jour une cartographie des flux de données au niveau du réseau, et toujours la mettre à disposition du conseiller en sécurité.

11 ACQUISITION, DÉVELOPPEMENT ET MAINTENANCE DES SYSTÈMES D'INFORMATION ***(voir ISO 27002 – 14 Acquisition, développement et maintenance des systèmes d'information)***	
11.1 EXIGENCES DE SÉCURITÉ APPLICABLES AUX SYSTÈMES D'INFORMATION ***(voir ISO 27002 – 14.1 Exigences de sécurité applicables aux systèmes d'information)***	
B-11.1.1	Vos exigences de sécurité doivent être clairement et formellement établies, convenues et documentées avant l'acquisition et/ou le développement et/ou l'amélioration du système d'information. Cette documentation doit toujours être actualisée dans le cadre du lancement d'une nouvelle version ou d'une version améliorée du système d'information.
11.2 SÉCURITÉ DES PROCESSUS DE DÉVELOPPEMENT ET D'ASSISTANCE TECHNIQUE ***(voir ISO 27002 – 14.2 Sécurité des processus de développement et d'assistance technique)***	
B-11.2.1	Avant la mise en production de nouvelles ou d'importantes évolutions de systèmes existants, le responsable du projet doit vérifier si les exigences de sécurité définies au début de la phase de développement sont remplies.

12 RELATIONS AVEC LES FOURNISSEURS ***(voir ISO 27002 – 15 Relations avec les fournisseurs)***	
12.1 SÉCURITÉ DE L'INFORMATION DANS LES RELATIONS AVEC LES FOURNISSEURS ***(voir ISO 27002 – 15.2 Gestion de la prestation du service)***	
B-12.1.1	La prestation de service des fournisseurs doit être régulièrement surveillée, jugée et auditée.

13 INCIDENTS LIÉS À LA SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 16 Gestion des incidents liés à la sécurité de l'information)***	
13.1 GESTION DES INCIDENTS LIÉS À LA SÉCURITÉ DE L'INFORMATION ET AMÉLIORATIONS ***(voir ISO 27002 – 16.1 Gestion des incidents liés à la sécurité de l'information et améliorations)***	
B-13.1.1	Il convient d'installer une procédure permettant : - de détecter ; - d'évaluer et, si d'application : - de suivre ; - et de restaurer des événements liés à la sécurité de l'information concernant les données à caractère personnel utilisées/traitées.
B-13.1.2	Le conseiller en sécurité désigné par votre organisation intervient en tant que point de contact pour la détection et le signalement d'incidents de sécurité.
B-13.1.3	Si un incident de sécurité de l'information dépasse les frontières de l'organisation, toutes les parties externes touchées doivent être suffisamment informées en temps opportun et de manière coordonnée par le conseiller en sécurité.

14 *CONTINUITÉ DE L'ACTIVITÉ* ***(voir ISO 27002 – 17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité)***	
14.1 CONTINUITÉ DE LA SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 17.1 Continuité de la sécurité de l'information)***	
B-14.1.1	Les procédures nécessaires doivent être mises en œuvre pour la récupération de vos processus d'exploitation, la garantie du niveau requis de sécurité de l'information et la remise à disposition des données à caractère personnel dans un délai défini au préalable. Les procédures peuvent comprendre des procédures d'urgence, de repli et de reprise, … Ces procédures doivent être documentées, testées et adaptées régulièrement et les personnes concernées doivent être formées. Les procédures concernant la continuité de l'activité doivent également être protégées contre les fuites et la dégradation, vu les informations sensibles qui y figurent (notamment de quelle manière l'organisation réagira en cas d'incident grave ou de catastrophe).

B-14.1.2	Vos mesures pour la continuité de la sécurité de l'information des données à caractère personnel doivent être régulièrement testées et au besoin mises à jour.

15 CONFORMITÉ ***(voir ISO 27002 – 18 Conformité)***	
15.1 RESPECT DES PRESCRIPTIONS LÉGALES ***(voir ISO 27002 – 18.1 Conformité aux obligations légales et contractuelles)***	
B-15.1.1	Le conseiller en sécurité communique en temps opportun à toutes les personnes impliquées dans le traitement de données à caractère personnel la législation et la réglementation pertinentes à respecter.