LIGNES DIRECTRICES POUR LA SÉCURITÉ DE L'INFORMATION DES DONNÉES À CARACTÈRE PERSONNEL DANS LES VILLES ET LES COMMUNES, LES INSTITUTIONS FAISANT PARTIE DU RÉSEAU GÉRÉ PAR LA BANQUE-CARREFOUR DE LA SÉCURITÉ SOCIALE ET DANS LE CADRE DE L'INTÉGRATION CPAS-COMMUNE

Version : 2.0

Répartition des normes en deux parties :

- partie A – normes et mesures globales liées à la politique, consistant en des normes et mesures générales et des normes et mesures spécifiques pour les institutions de sécurité sociale, pour les villes et les communes et dans le cadre de l'intégration d'un CPAS avec une commune ;
- partie B – normes de mise en œuvre spécifiques/techniques, consistant en des normes générales de mise en œuvre et des normes spécifiques de mise en œuvre pour les institutions de sécurité sociale et dans le cadre de l'intégration d'un CPAS avec une commune.

1 Préambule

Le document “Lignes directrices pour la sécurité de l'information des données à caractère personnel dans les villes et les communes, les institutions faisant partie du réseau géré par la Banque-carrefour de la Sécurité sociale et dans le cadre de l'intégration CPAS-commune” établit les objectifs de sécurité que doit respecter chacune de ces institutions. Ce document s'inspire de la norme ISO 27002.

Vu la tendance d'une collaboration de plus en plus fréquent entre les communes et les centres publics d'action sociale (CPAS), tant sur le plan logistique que sur le plan pratique, on attire l'attention sur le fait que dans de tels cas, outre les lignes directrices pour la sécurité de l’information des données à caractère personnel qui s'appliquent de manière générale, il faut également respecter les exigences spécifiques de sécurité qui sont imposées aux institutions qui souhaitent obtenir et conserver un accès au réseau de la Banque-carrefour de la Sécurité sociale (ci-après la BCSS ou Banque-carrefour).

Certaines institutions sont hébergées dans différents bâtiments ou disposent d'entités décentralisées. Dans chacune de ces entités, les lignes directrices pour la sécurité doivent être respectées, en particulier au niveau de la sécurité physique (sécurisation des accès, sécurité incendie, …).

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 conservées, 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, technique ou au niveau de la gestion, que juridique.

Conseiller en sécurité de l'information

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 connaissent spécifiquement bien le secteur pour lequel le Comité est compétent. Actuellement, il existe six 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 de l'information doit parfois être communiquée au comité sectoriel compétent et/ou validée par lui.

Le conseiller en sécurité de l'information 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 l'organe ultime de décision.

Porte unique

L'expression "porte unique" définit le concept par lequel des guichets de différents services communaux sont accessibles à un seul endroit pour les citoyens, comme (liste non exhaustive) :

- le service population ;
- le service état civil ;
- les centres publics d'action sociale ;
- l'agence locale pour l'emploi ;
- le logement social ;
- le service de la police locale ;
- …

Cette initiative n'est évidemment approuvée qu'à condition que les mesures définies dans le présent document soient respectées par toutes les organisations qui disposeront d'un guichet.

Sur le site Internet de la Commission de la protection de la protection de la vie privée, davantage de termes sont expliqués dans le lexique (voir http://www.privacycommission.be/fr/lexicon).

3 Champ d'application et interprétation des lignes directrices

3.1 Application des lignes directrices pour la sécurité de l'information

Les lignes directrices pour la sécurité expliquées ci-après s'appliquent à tous les services de villes et de communes qui utilisent et traitent des données à caractère personnel, aux institutions de sécurité sociale, telles que mentionnées 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* (ci-après la loi Banque-carrefour) et dans le cadre de l'intégration d'un CPAS et d'une commune ou d'une ville.

La mise en œuvre et la vérification des lignes directrices pour la sécurité auprès de tiers qui traitent des données de nature personnelle pour le compte d'une des institutions susmentionnées relèvent tout d'abord de la responsabilité de l'institution qui confie des tâches à ce tiers.

Sécurité de l'information dans les villes et les communes

Étant donné que les villes et communes sont connectées au Registre national, les exigences de sécurité de 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) s'appliquent. Les villes et communes peuvent également relever d'autres domaines de compétence auxquels d'autres dispositions légales complémentaires s'appliquent éventuellement. Les mesures de référence de la Commission de la protection de la vie privée s'appliquent de toute façon. Ces normes/directives "*Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel*" ainsi que les *« Lignes directrices pour la sécurité de l'information de données à caractère personnel* » sont disponibles sur le site Internet de la Commission.

Les administrations communales et celles des villes doivent désigner un conseiller en sécurité de l'information et disposer d'une politique de sécurité. La communication de données à caractère personnel par des villes et des communes requiert également l'autorisation préalable du comité sectoriel compétent de la Commission de la protection de la vie privée.

Sécurité de l'information dans les institutions de sécurité sociale et dans les CPAS en particulier

L'organisation de la politique de sécurité de l'information au sein du réseau de la Banque-carrefour de la Sécurité sociale se base sur l'application obligatoire des normes minimales de sécurité par ses partenaires. Ces normes sont disponibles sur le site Internet de la Banque-carrefour et doivent être obligatoirement respectées par les institutions de sécurité sociale si elles souhaitent obtenir et conserver un accès au réseau de la Banque-carrefour. Le contrôle du respect de ces normes effectué par le Comité sectoriel de la Sécurité Sociale et de la Santé se base sur un questionnaire qui est transmis chaque année via la Banque-carrefour. En cas de non-respect, conformément à l'article 46, premier alinéa, 1° de la loi Banque-carrefour, l'accès au réseau peut être retiré aux institutions concernées, après mise en demeure.

Les normes minimales de sécurité s'appliquent donc aux institutions de sécurité sociale, telles que mentionnées à l'article 2, premier alinéa, 2° de la loi Banque-carrefour et aux instances qui ont adhéré au réseau de la BCSS, conformément à l'article 18 de la loi susmentionnée. D'autres instances peuvent également être soumises au respect des normes minimales de sécurité via une autorisation du Comité sectoriel de la Sécurité Sociale. Ces normes s'appliquent aussi aux CPAS.

La mise en œuvre et la vérification des normes minimales de sécurité auprès de tiers qui traitent des données de nature personnelle pour le compte d'une institution de sécurité sociale relèvent de la responsabilité de l'institution qui confie des tâches au tiers.

Sécurité de l'information dans le cadre d'un partenariat entre villes et communes et CPAS

La Banque-carrefour de la Sécurité Sociale a également imposé des mesures de sécurité de l'information claires aux acteurs de son réseau, dont les centres publics d'action sociale (ci-après les CPAS) pour garantir l'intégrité de la vie privée des citoyens concernés. Dans le respect de la politique relative à la sécurité de l'information de la sécurité sociale et de la vie privée, le CPAS peut élaborer des protocoles de collaboration avec l'administration communale/de la ville.

Toute forme de collaboration au niveau communal/de la ville entre l'administration communale ou celle de la ville et le CPAS doit être pleinement étayée. Cela peut conduire à un meilleur service intégré au citoyen et à une plus grande efficacité des parties concernées. La condition pour ce faire est que cette collaboration ne porte pas atteinte aux principes repris dans la Loi vie privée ou aux autres dispositions pertinentes relatives à la protection des données (à caractère personnel).

À la lumière de la loi susmentionnée, il faut en outre signaler qu'au sein d'une commune/ville, l'administration communale ou celle de la ville et le CPAS sont tous deux responsables du traitement de données à caractère personnel. Ils assument chacun leur propre responsabilité et doivent élaborer chacun leur propre politique de sécurité de l'information avec les contrôles y afférents.

Le fait que les deux organisations collaborent, par exemple en faisant appel aux mêmes membres du personnel et à la même infrastructure, est autorisé pour autant que chaque organisation respecte ses obligations propres à ses activités. En ce qui concerne le CPAS, le respect des normes minimales de sécurité est imposé comme c'est aussi le cas pour toutes les institutions qui sont connectées au réseau de la BCSS.

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

La Commission de la protection de la vie privée 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. Les lignes dierctrices ne s'appliquent en principe que lors du traitement de données à caractère personnel, elles doivent toutefois également 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.

Pour les institutions qui font partie du réseau qui est géré par la BCSS, le contrôle du respect des normes s'effectue en complétant un questionnaire qui est soumis pour évaluation au Comité sectoriel de la Sécurité Sociale et de la Santé via la Banque-carrefour. Il relève de la responsabilité de l'institution de compléter correctement le questionnaire et de veiller au respect des normes. Le Comité sectoriel de la Sécurité Sociale et de la Santé peut, le cas échéant, (faire) effectuer des contrôles afin d'analyser sur le terrain le respect des normes minimales de sécurité par les institutions de la sécurité sociale.

Si le Comité sectoriel de la Sécurité Sociale et de la Santé constate qu'une institution de la sécurité sociale manque à son devoir en matière de respect de ces normes, il peut demander à la Banque-carrefour de ne plus donner suite aux demandes envoyées par cette institution.

Toutefois, il va de soi qu'avant de prendre cette mesure, le Comité sectoriel de la Sécurité Sociale et de la Santé doit interroger la personne chargée de la gestion journalière de l'institution concernée.

3.2 Interprétation et révision des lignes directrices pour la sécurité de l'information

Les lignes directrices sont divisées en une partie A qui reprend les normes et mesures globales liées à la politique avec un volet "villes et communes", un volet "institutions faisant partie du réseau qui est géré par la Banque-carrefour de la Sécurité Sociale" et un volet qui s'applique spécifiquement dans le cadre d'un accord de coopération entre un CPAS et une ville ou une commune et en une partie B qui reprend ces mêmes subdivisions en ce qui concerne les normes de mise en œuvre spécifiques/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 sont sujettes à révision. Elles seront donc adaptées en fonction de l'évolution qui survient 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 pour les villes et les communes, les institutions faisant partie du réseau qui est géré par la Banque-carrefour de la Sécurité Sociale et dans le cadre de l'intégration d'un CPAS et d'une commune 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 l'organe ultime 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 l'organe ultime de décision.

Pour ce groupe cible, ces lignes directrices pour la sécurité veulent être une spécification des mesures générales de référence et des « *lignes directrices pour la sécurité de l'information de données à caractère personnel* » que la Commission de la protection de la vie privée a édictées.

À la fin du point 12 "Conformité", elles rappellent en particulier toutes les prescriptions légales que les villes et les communes ainsi que les institutions faisant partie du réseau qui est géré par la BCSS doivent remplir lors de l'utilisation et du traitement de données à caractère personnel.

5 Lignes directrices – structure ISO 27002

La structure de ces lignes directrices s'inspire de la norme ISO 270002 (voir notamment http://www.iso27001security.com/html/27002.html). Elle est subdivisée en 11 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, le mode de mise en œuvre technique de la sécurité de l'information est repris dans la partie B.

La modification des normes minimales du BCSS donne lieu à l'envoi des normes minimales de sécurité modifiées et approuvées aux responsables de la gestion journalière des institutions de la sécurité sociale qui en informent leur comité de direction.

6 Abréviations utilisées

- GLO = s'applique de manière globale
- SP KSZ-BCSS = s'applique spécifiquement aux institutions de la sécurité sociale
- SP SG-VC = s'applique spécifiquement aux villes et communes
- SP INT = s'applique spécifiquement lors d'une collaboration villes/communes et CPAS et pour l'intégration et l'utilisation partagée de l'ICT par les villes/communes et les CPAS

PARTIE A – NORMES ET MESURES GLOBALES LIÉES À LA POLITIQUE

1 RISQUE ***(voir ISO 27002 – 4 Appréciation et traitement du risque)***		
1.1 APPRÉCIATION DU RISQUE LIÉ À LA SÉCURITÉ ***(voir ISO 27002 – 4.1 Appréciation du risque lié à la sécurité)***		
A-1.1.1	**GLO**	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 et de présenter cette appréciation à l'organe ultime de décision au sein de votre organisation en vue d'actions ultérieures.
1.2 TRAITEMENT DU RISQUE LIÉ À LA SÉCURITÉ ***(voir ISO 27002 – 4.2 Traitement du risque lié à la sécurité)***		
A-1.2.1	**GLO**	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 Politique de sécurité)***		
2.1 POLITIQUE DE SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 5.1 Politique de sécurité de l'information)***		
A-2.1.1	**GLO**	Votre organisation doit disposer d'une politique de sécurité de l'information ("*information security policy*") formelle, actualisée et approuvée par l'organe ultime de décision de votre organisation qui doit régulièrement être communiquée à toutes les parties concernées.

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	**GLO**	Il faut un soutien clair de l'organe ultime 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.
A-3.1.2	**GLO**	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 de l'information. 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 de l'information 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-3.1.3	**GLO**	Le conseiller en sécurité de l'information doit toujours disposer de toutes les informations nécessaires pour exécuter sa mission correctement et en temps opportun.
A-3.1.4	**GLO**	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-3.1.5	**SP KSZ-BCSS**	Chaque institution de la sécurité sociale connectée au réseau de la Banque-carrefour doit communiquer à la Banque-carrefour le nombre d'heures qu'elle a accordées officiellement au conseiller en sécurité de l'information et à ses éventuels adjoints pour l'exécution de leurs tâches.
A-3.1.6	**SP KSZ-BCSS**	Chaque institution de la sécurité sociale connectée au réseau de la Banque-carrefour doit organiser les informations au conseiller en sécurité de l'information de manière à ce que ce dernier dispose des données pour l'exécution de la mission de sécurité qui lui a été confiée et de manière à ce qu'une concertation entre les différentes parties concernées puisse être organisée afin d'impliquer ainsi plus étroitement le conseiller en sécurité de l'information dans les activités de l'institution.
A-3.1.7	**SP KSZ-BCSS**	Chaque institution de gestion d'un réseau secondaire est tenu d'échanger au moins une fois par semestre des informations pertinentes avec son réseau secondaire en organisant une réunion du sous-groupe "Sécurité de l'information" pour les institutions qui font partie de son réseau.
A-3.1.8	**SP INT**	Une collaboration entre la ville/commune et le CPAS en matière de hardware et de technologie ICT est permise. Cette collaboration doit garantir le respect de toutes les normes et de toutes les règles auxquelles est tenue toute organisation intrinsèquement et en raison de cette collaboration. Avant que du hardware, des lignes de télécommunication, … ainsi que toute gestion commune ne puissent être regroupés, un accord de coopération doit être conclu entre les différentes organisations partenaires. Cet accord doit mentionner les compétences de chaque organisation ainsi que les responsabilités.

		Si une part de cette gestion est confiée à un tiers (un sous-traitant), il est nécessaire que ce tiers ait conclu un contrat avec l'organisation. Ce contrat doit mentionner toutes les obligations du sous-traitant en matière de confidentialité mais également ses obligations en matière de protection des données à caractère personnel, telles que définies dans la Loi vie privée - article 16).
3.2 TIERS ET SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 6.2 Tiers)***		
A-3.2.1	**GLO**	Il convient d'identifier clairement les risques liés à la sécurité de l'information concernant des tiers et de mettre en œuvre les mesures de gestion appropriées avant d'accorder à ces tiers (organisations ou citoyens) un accès à des données à caractère personnel.

4 BIENS ***(voir ISO 27002 – 7 Gestion des biens)***		
4.2 CLASSIFICATION DES INFORMATIONS ***(voir ISO 27002 – 7.2 Classification des informations)***		
A-4.2.1	**GLO**	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-4.2.2	**GLO**	Tous les utilisateurs qui utilisent/traitent des données à caractère personnel doivent connaître cette distinction.

5 RESSOURCES HUMAINES ***(voir ISO 27002 – 8 Sécurité liée aux ressources humaines)***		
5.1 SÉCURITÉ DE L'INFORMATION AVANT LE RECRUTEMENT ***(voir ISO 27002 – 8.1 Avant le recrutement)***		
A-5.1.1	**GLO**	Lors du processus de recrutement, votre organisation doit clairement signaler aux candidats potentiels l'importance de la sécurité de l'information.

A-5.1.2	**GLO**	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.
5.2 SÉCURITÉ DE L'INFORMATION PENDANT LA DURÉE DU CONTRAT ***(voir ISO 27002 – 8.2 Pendant la durée du contrat)***		
A-5.2.1	**GLO**	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 appropriée et d'un recyclage régulier.
A-5.2.2	**GLO**	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 concernant les obligations de confidentialité et de sécurité, en signant un document contractuel reprenant des clauses contractuelles claires.
5.3 SÉCURITÉ DE L'INFORMATION EN CAS DE FIN OU DE MODIFICATION DE CONTRAT ***(voir ISO 27002 – 8.3 Fin ou modification de contrat)***		
A-5.3.1	**GLO**	Il faut élaborer des procédures claires et appropriées et veiller à l'application de celles-ci concernant la restitution du matériel et la suppression de tous les droits d'accès lors du départ d'un salarié, d'un contractant ou d'un utilisateur tiers.

6 ENVIRONNEMENT PHYSIQUE ***(voir ISO 27002 – 9 Sécurité physique et environnementale)***		
6.1 SÉCURITÉ ENVIRONNEMENTALE ***(voir ISO 27002 – 9.1 Zones sécurisées)***		
A-6.1.1	**GLO**	Votre organisation doit réaliser une analyse des risques. Sur la base des résultats, les zones sécurisées doivent être définies et les sécurisations d'accès appropriées doivent être apportées pour sécuriser toutes les zones où se trouvent des informations et du matériel IT avec des données à caractère personnel.
A-6.1.2	**GLO**	Votre organisation doit définir les mesures nécessaires pour éviter toute forme de dommage pouvant compromettre les données à caractère personnel.
6.2 MATÉRIEL SÉCURISÉ ***(voir ISO 27002 – 9.2 Sécurité du matériel)***		
A-6.2.1	**GLO**	Sur la base d'une analyse des risques, votre organisation doit définir les mesures de gestion adéquates concernant le matériel, le câblage et les équipements de support afin d'empêcher la perte, les dommages, le vol et la modification non souhaitée de données à caractère personnel (même lorsque ce matériel est

6 ENVIRONNEMENT PHYSIQUE ***(voir ISO 27002 – 9 Sécurité physique et environnementale)***		
6.1 SÉCURITÉ ENVIRONNEMENTALE ***(voir ISO 27002 – 9.1 Zones sécurisées)***		
		utilisé/placé hors site).
A-6.2.2	**GLO**	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.

7 PROCÉDURES OPÉRATIONNELLES ET DE COMMUNICATION ***(voir ISO 27002 – 10 Gestion de l'exploitation et des télécommunications)***		
7.1 PROCÉCURES OPÉRATIONNELLES ET RESPONSABILITÉS CONCERNANT LA SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 10.1 Procédures et responsabilités liées à l'exploitation)***		
A-7.1.1	**GLO**	Votre organisation doit prévoir une séparation des tâches afin d'éviter qu'une seule personne n'ait le contrôle exclusif d'un traitement de données à caractère personnel.
7.2 PROTECTION CONTRE LES CODES MALVEILLANTS ET MOBILES ***(voir ISO 27002 – 10.4 Protection contre les codes malveillants et mobiles***		
A-7.2.1	**GLO**	Votre organisation doit disposer de procédures et de directives appropriées de protection contre les codes malveillants et de contrôle des codes mobiles pour augmenter la sensibilisation des utilisateurs du système et des utilisateurs finaux. Exemples de directives et de procédures possibles : • interdire l'utilisation de programmes automatisés ; • 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 codes malveillants.
7.3 SAUVEGARDE ***(voir ISO 27002 – 10.5 Sauvegarde)***		
A-7.3.1	**GLO**	Votre organisation doit rédiger une politique de sauvegarde adéquate et en assurer le suivi afin d'empêcher la perte, les dommages, le vol et la modification non souhaitée de données à caractère personnel.

7.4 SÉCURITÉ DES RÉSEAUX ***(voir ISO 27002 – 10.6 Gestion de la sécurité des réseaux)***		
A-7.4.1	**GLO**	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 quitter votre organisation.
A-7.4.2	**SP KSZ-BCSS**	Pour leurs connexions TCP/IP externes à la sécurité sociale, les institutions de la sécurité sociale du réseau primaire doivent utiliser l'Extranet de la sécurité sociale. Cette mesure ne s'applique pas si l'institution en question utilise, pour ses connexions TCP/IP externes à la sécurité sociale une configuration informatique qui n'est pas utilisée pour le traitement de données à caractère personnel sociales ou qui n'est en aucune façon reliée au(x) système(s) d'information utilisé(s) pour le traitement de données à caractère personnel sociales. Pour toute dérogation à cette règle, une demande motivée doit être introduite via le service de sécurité de la BCSS.
A-7.4.3	**SP KSZ-BCSS**	Pour leurs connexions TCP/IP externes à la sécurité sociale, les institutions de la sécurité sociale du réseau secondaire peuvent utiliser l'Extranet de la sécurité sociale. Cette mesure ne s'applique pas si l'institution en question utilise, pour ses connexions TCP/IP externes à la sécurité sociale une configuration informatique qui n'est pas utilisée pour le traitement de données à caractère personnel sociales ou qui n'est en aucune façon reliée au(x) système(s) d'information utilisé(s) pour le traitement de données à caractère personnel sociales. Pour les connexions directes avec leurs réseaux TCP/IP externes à la sécurité sociale : • les institutions du réseau secondaire impliquées doivent mettre en œuvre des mesures de sécurité qui sont et restent conformes aux mesures prises au niveau de l'Extranet de la sécurité sociale ; • les institutions de gestion concernées doivent adopter des dispositifs de sécurité qui sont et restent conformes aux dispositifs adoptés au niveau de l'Extranet de la sécurité sociale.
7.5 MANIPULATION DES SUPPORTS IT PHYSIQUES ***(voir ISO 27002 – 10.7 Manipulation des supports)***		
A-7.5.1	**GLO**	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 multifonction. Exemples de supports IT amovibles : - disques optiques (CD, DVD, Blu-ray, etc.) ; - cartes mémoire (clé USB, stick mémoire, carte digitale, carte SD, mini-carte SD, carte CompactFlash, smart card, etc.) ; - floppy disk et zip disk ; - bandes magnétiques/tapes.

A-7.5.1	**SP INT**	Supports d'information Le niveau de sécurité le plus élevé imposé aux deux organisations s'applique à chaque support d'information partagé et ce, aussi bien pour les supports d'information actifs que pour ceux utilisés pour les sauvegardes et l'archivage. L'accès à ces supports d'information doit être accordé en fonction des besoins par le service habilité (compétent ?). Les accès à ces supports doivent pouvoir être contrôlés.
7.6 ÉCHANGE D'INFORMATIONS ***(voir ISO 27002 – 10.8 Échange des informations)***		
A-7.6.1	**GLO**	Votre organisation doit disposer d'une politique de messagerie électronique et d'une politique Internet (*"e-mail policy et Internetpolicy"*) formelles, actualisées et approuvées par l'organe ultime de décision de votre organisation qui doivent régulièrement être communiquées à toutes les parties concernées et qui consacrent une attention à l'utilisation de données à caractère personnel dans un courrier électronique.
A-7.6.2	**SP INT**	Services communs villes/communes et CPAS D'un point de vue juridique, nous avons à faire à deux organisations différentes disposant de leur propre réglementation spécifique. Des dossiers qui contiennent des données à caractère personnel ne peuvent pas être partagés à moins qu'une autorisation spécifique du Comité sectoriel compétent n'ait été accordée.

8 ACCÈS À DES DONNÉES À CARACTÈRE PERSONNEL ***(voir ISO 27002 – 11 Contrôle d'accès)***		
8.1 EXIGENCES RELATIVES AU CONTRÔLE D'ACCÈS ***(voir ISO 27002 – 11.1 Exigences métier relatives au contrôle d'accès)***		
A-8.1.1	**GLO**	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 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.
8.2 RESPONSABLE DES DROITS D'ACCÈS DES UTILISATEURS ***(voir ISO 27002 – 11.2 Gestion de l'accès utilisateur)***		
A-8.2.1	**GLO**	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.

8.3 RESPONSABILITÉS UTILISATEURS ***(voir ISO 27002 – 11.3 Responsabilités utilisateurs)***		
A-8.3.1	**GLO**	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.
8.4 CONTRÔLE D'ACCÈS AUX RÉSEAUX ***(voir ISO 27002 – 11.4 Contrôle d'accès aux réseaux)***		
A-8.4.1	**GLO**	Votre organisation doit définir des mesures de protection appropriées si un accès en ligne est accordé (par exemple via Internet ou un réseau sans fil) à des données à caractère personnel.
8.5 CONTRÔLE D'ACCÈS AUX APPLICATIONS ET À L'INFORMATION ***(voir ISO 27002 – 11.6 Contrôle d'accès aux applications et à l'information)***		
A-8.5.1	**GLO**	Les mesures de sécurité nécessaires doivent être définies afin de limiter l'accès aux données à caractère personnel.
A-8.5.2	**GLO**	Votre organisation doit limiter l'accès des gestionnaires d'informations (gestionnaires de systèmes, également appelés "superusers") aux systèmes informatiques sur lesquels les données à caractère personnel sont utilisées/traitées.
A-8.5.3	**SP INT**	Lors de l'utilisation d'une infrastructure informatique commune par plusieurs organisations, il faut veiller à prévoir les mesures techniques et organisationnelles nécessaires afin que seules les personnes habilitées aient accès aux données à caractère personnel nécessaires à l'exercice de leur fonction au sein ou pour le compte de leur(s) organisation(s) respective(s). Lors de l'accès aux données, une identification formelle doit avoir lieu. Il faut pouvoir faire une distinction entre l'accès au nom de la commune ou du CPAS. Cela signifie pour chaque utilisateur que des droits d'accès distincts aux données à caractère personnel doivent être accordés en fonction du rôle au sein de l'organisation pour laquelle il exécute une tâche.
8.6 TRAVAILLER À DISTANCE ***(voir ISO 27002 – 11.7 Informatique mobile et télétravail)***		
A-8.6.1	**GLO**	Votre organisation doit disposer d'une politique formelle en matière d'utilisation de matériel informatique mobile qui doit tenir compte des risques que comporte le travail dans des environnements non protégés. En matière de télétravail, il faut conclure des accords et définir des mesures de sécurité qui soient conformes à la politique de sécurité de votre organisation. Le personnel qui utilise du matériel informatique portable ou qui fait du télétravail doit recevoir des instructions pour le conscientiser aux risques supplémentaires de cette manière de travailler et aux mesures de gestion qui sont prises.

9 ACQUISITION, DÉVELOPPEMENT ET MAINTENANCE DES SYSTÈMES D'INFORMATION ***(voir ISO 27002 – 12 Acquisition, développement et maintenance des systèmes d'information)***		
9.1 EXIGENCES DE SÉCURITÉ APPLICABLES AUX SYSTÈMES D'INFORMATION ***(voir ISO 27002 – 12.1 Exigences de sécurité applicables aux systèmes d'information)***		
A-9.1.1	**GLO**	Votre organisation doit disposer d'une approche structurée pour garantir intégralement les exigences de sécurité des données à caractère personnel lors du développement de systèmes d'information (lors de l'input, du traitement et de l'output).
9.2 SÉCURITÉ EN MATIÈRE DE DÉVELOPPEMENT ET D'ASSISTANCE TECHNIQUE ***(voir ISO 27002 – 12.5 Sécurité en matière de développement et d'assistance technique)***		
A-9.2.1	**GLO**	Votre organisation doit appliquer des procédures de modification formelles et claires afin de limiter au minimum le risque de modifications erronées ou la perte de données à caractère personnel.
A-9.2.2	**GLO**	Votre organisation doit disposer de procédures pour le développement de nouveaux systèmes ou d'importantes évolutions de systèmes existants de manière à ce que le responsable du projet tienne compte des exigences de sécurité nécessaires.

10 INCIDENTS LIÉS À LA SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 13 Gestion des incidents liés à la sécurité de l'information)***		
10.1 SIGNALEMENT DES ÉVÉNEMENTS ET DES FAILLES LIÉS À LA SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 13.1 Signalement des événements et des failles liés à la sécurité de l'information)***		
A-10.1.1	**GLO**	Votre organisation doit veiller à ce que la cellule de sécurité de l'information soit toujours directement informée d'événements et d'incidents pouvant compromettre ou ayant compromis la sécurité de l'information de données à caractère personnel.
A-10.1.2	**GLO**	Votre organisation doit veiller à ce que la cellule de sécurité de l'information soit toujours directement informée des failles détectées dans la sécurité des systèmes ou des services concernés par le traitement de données à caractère personnel.
A-10.1.3	**GLO**	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 d'escalade pour les incidents impliquant des données à caractère personnel.
10.2 GESTION DES AMÉLIORATIONS ET INCIDENTS LIÉS À LA SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 13.2 Gestion des améliorations et incidents liés à la sécurité de l'information)***		
A-10.2.1	**GLO**	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-10.2.2	**GLO**	La cellule de sécurité de l'information doit être systématiquement informée 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.

11 CONTINUITÉ DE L'ACTIVITÉ ***(voir ISO 27002 – 14 Gestion du plan de continuité de l'activité)***		
11.1 ASPECTS DE LA SÉCURITÉ DE L'INFORMATION EN MATIÈRE DE GESTION DE LA CONTINUITÉ DE L'ACTIVITÉ ***(voir ISO 27002 – 13 Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité)***		
A-11.1.1	**GLO**	Votre organisation doit prendre toutes les mesures possibles pour garantir la continuité de la disponibilité des données à caractère personnel (sur la base d'une analyse des risques).

12 CONFORMITÉ ***(voir ISO 27002 – 15 Conformité)***		
12.1 CONFORMITÉ AVEC LES EXIGENCES LÉGALES ***(voir ISO 27002 – 15.1 Conformité avec les exigences légales)***		
A-12.1.1	**GLO**	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 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 10 août 2005 *instituant le système d'information Phenix* ; • Loi du 4 juillet 1962 *relative à la statistique publique* ; • 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-12.1.2	**GLO**	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 de l'information 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-12.1.3	**GLO**	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-12.1.4	**GLO**	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.
A-12.1.5	**SP KSZ-BCSS**	Chaque institution de la sécurité sociale doit respecter la législation spécifique suivante : • Loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* ; • les autorisations génériques et individuelles en vigueur.
A-12.1.6	**SP KSZ-BCSS**	Chaque institution de la sécurité sociale connectée au réseau de la Banque-carrefour doit communiquer l'identité de son conseiller en sécurité de l'information et de ses éventuels adjoints au Comité sectoriel de la Sécurité Sociale et de la Santé. Pour les institutions du réseau secondaire, l'identité doit être communiquée à l'institution de gestion.
A-12.1.7	**SP KSZ-BCSS**	Chaque institution de la sécurité sociale connectée au réseau de la Banque-carrefour doit s'assurer de l'existence des autorisations nécessaires du Comité sectoriel de la Sécurité Sociale et de la Santé pour l'accès à des données sociales à caractère personnel gérées par une autre institution.
A-12.1.8	**SP SG-VC**	Chaque ville ou commune doit respecter la législation spécifique suivante : • *Arrêté du 18 décembre 2003du Gouvernement wallon portant le Code de la fonction publique wallonne* (M.B. du 31/12/2003) notamment l'article 3 §2 et l'annexe « charte de bonne conduite administrative »; • les autorisations génériques et individuelles en vigueur.
A-12.1.9	**SP SG-VC**	Chaque ville ou commune doit communiquer l'identité de son conseiller en sécurité de l'information et de ses éventuels adjoints au Comité sectoriel du Registre national (voir l'article 10 de la Loi sur le Registre national).
A-12.1.1O	**SP KSZ-BCSS** **SP INT**	Comptabilité Si des données à caractère personnel figurent dans la comptabilité (par ex. au sein des CPAS), les normes minimales du Comité sectoriel de la Sécurité Sociale et de la Santé sont d'application. Cette règle reste d'application dans le cas d'un système commun de comptabilité.
A-12.1.11	**SP INT**	Fichier d'adresses commun La règle générale stipule que pour tout échange de données à caractère personnel sociales, une autorisation du Comité sectoriel de la Sécurité Sociale et de la Santé est requise et que cet échange de données doit se faire par l'intermédiaire de la Banque-carrefour de la Sécurité Sociale. Cela implique que le fichier d'adresses commun ne peut contenir aucune donnée à caractère personnel sociale sans autorisation du Comité sectoriel de la Sécurité Sociale et de la Santé.

A-12.1.12	**SP INT**	Une autorisation du Comité sectoriel de la Sécurité Sociale et de la Santé est requise pour l'échange de données à caractère personnel entre la commune/ville et le CPAS.
12.2 CONFORMITÉ AVEC LES POLITIQUES ET NORMES DE SÉCURITÉ ET CONFORMITÉ TECHNIQUE ***(voir ISO 27002 – 15.2 Conformité avec les politiques et normes de sécurité et conformité technique)***		
A-12.2.1	**GLO**	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 : - politique liée à la sécurité de l'information ; - organisation de la sécurité de l'information ; - gestion des biens ; - exigences de sécurité concernant le personnel ; - sécurité physique ; - gestion opérationnelle ; - sécurité logique des accès ; - entretien et développement des systèmes d'information ; - gestion des incidents liés à la sécurité de l'information ; - processus de gestion de la continuité de l'activité ; - conformité.
A-12.2.2	**SP KSZ-BCSS**	Chaque institution de la sécurité sociale connectée au réseau de la Banque-carrefour doit organiser au moins une fois tous les quatre ans un audit externe concernant la situation de la sécurité logique et physique.

PARTIE B – NORMES DE MISE EN OEUVRE SPÉCIFIQUES/TECHNIQUES

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)***		
B-3.1.1	**SP KSZ-BCSS**	Les conseillers en sécurité de l'information concernés veillent, au sein de l'institution propre, à l'utilisation sécurisée de la carte professionnelle soins de santé telle que définie aux articles 42 à 50 inclus de l'arrêté Royal du 22 février 1998 *portant des mesures d'exécution de la carte d'identité sociale*.

4 BIENS ***(voir ISO 27002 – 7 Gestion des biens)***		
4.1 RESPONSABILITÉS RELATIVES AUX BIENS ***(voir ISO 27002 – 7.1 Responsabilités relatives aux biens)***		
B-4.1.1	**GLO**	Un inventaire actualisé des moyens 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-4.1.2	**GLO**	Dans cet inventaire, chaque moyen pertinent relatif à un traitement de données à caractère personnel doit être couplé à une fonction/personne déterminée au sein de votre organisation (responsabilité).

4.2 CLASSIFICATION DES INFORMATIONS ***(voir ISO 27002 – 7.2 Classification des informations)***		
B-4.2.1	**GLO**	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 RESSOURCES HUMAINES ***(voir ISO 27002 – 8 Sécurité liée aux ressources humaines)***		
5.2 SÉCURITÉ DE L'INFORMATION PENDANT LA DURÉE DU CONTRAT ***(voir ISO 27002 – 8.2 Pendant la durée du contrat)***		
B-5.2.1	**GLO**	Votre organisation doit prendre toutes les mesures adéquates 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 de l'organisation.
5.3 SÉCURITÉ DE L'INFORMATION EN CAS DE FIN OU DE MODIFICATION DE CONTRAT ***(voir ISO 27002 – 8.3 Fin ou modification de contrat)***		
B-5.3.1	**GLO**	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 programmes fournis, les documents appartenant à la société, le matériel et les cartes 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.
B-5.3.2	**GLO**	Les droits d'accès des travailleurs, contractants et utilisateurs externes aux informations et au matériel doivent être bloqués lors de la fin du contrat.
B-5.3.3	**GLO**	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 5.3.1 et 5.3.2.

6 ENVIRONNEMENT PHYSIQUE ***(voir ISO 27002 – 9 Sécurité physique et environnementale)***		
6.1 SÉCURITÉ ENVIRONNEMENTALE ***(voir ISO 27002 – 9.1 Zones sécurisées)***		
B-6.1.1	**GLO**	L'accès aux locaux (où des données à caractère personnel se trouvent ou sont utilisées/traitées) doit être strictement limité aux personnes habilitées désignées par votre organisation. Cet aspect doit faire l'objet d'un contrôle régulier, aussi bien pendant qu'en dehors des heures de travail normales (journal de bord ou dossier de journalisation).
B-6.1.2	**GLO**	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.
6.2 MATÉRIEL SÉCURISÉ ***(voir ISO 27002 – 9.2 Sécurité du matériel)***		
B-6.2.1	**GLO**	Le matériel doit être protégé contre des menaces physiques et des dangers de l'extérieur (même si ce matériel est utilisé/placé hors site). Une attention doit être accordée : • 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-6.2.2	**GLO**	Tout matériel équipé de supports de stockage doit être contrôlé pour la mise au rebut et le recyclage afin que toutes les données à caractère personnel soient transférées et 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.
B-6.2.3	**SP KSZ-BCSS**	Chaque institution de la sécurité sociale connectée au réseau de la Banque-carrefour doit disposer d'une alimentation électrique alternative pour garantir le service attendu.

7 PROCÉDURES OPÉRATIONNELLES ET DE COMMUNICATION ***(voir ISO 27002 – 10 Gestion de l'exploitation et des télécommunications)***		
7.2 PROTECTION CONTRE LES CODES MALVEILLANTS ET MOBILES ***(voir ISO 27002 – 10.4 Protection contre les codes malveillants et mobiles***		
B-7.2.1	**GLO**	Votre service informatique doit utiliser des systèmes actualisés de protection (prévention, détection et suppression) contre les codes malveillants et de contrôle des codes mobiles au niveau de : - tous les utilisateurs finaux, par exemple sur l'ordinateur, et générer des rapports périodiques, et - tous les composants du réseau, par exemple via Internet, et générer des rapports périodiques.
7.3 SAUVEGARDE ***(voir ISO 27002 – 10.5 Sauvegarde)***		
B-7.3.1	**GLO**	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-7.3.2	**GLO**	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.
B-7.3.3	**SP INT**	L'introduction de mesures de cryptage est nécessaire si les supports contiennent les sauvegardes de plusieurs organisations. Dans ce cas, les mesures de cryptage doivent être appliquées de manière à ce que chaque organisation ne puisse lire que ses propres données.
7.4 SÉCURITÉ DES RÉSEAUX ***(voir ISO 27002 – 10.6 Gestion de la sécurité des réseaux)***		
B-7.4.1	**GLO**	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-7.4.2	**GLO**	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-7.4.3	**SP KSZ-BCSS**	Chaque institution de la sécurité sociale connectée au réseau de la Banque-carrefour doit mettre en œuvre les mesures techniques efficaces et appropriées nécessaires pour garantir le niveau le plus élevé de disponibilité pour la connexion avec le réseau de la Banque-carrefour afin d'assurer une accessibilité maximale des données consultées et rendues disponibles. Cela suppose que cette connexion doit au moins être dédoublée vers différents points de connexion de l'Extranet qui soutiennent la transmission d'informations et intègrent les aspects de sécurité.

B-7.4.4	**SP INT**	Si l'organisation (les organisations) est (sont) dispersée(s) sur plusieurs sites, il faut prendre les mesures nécessaires afin que la connexion entre ces sites soit correctement sécurisée. Pour ce faire, il existe plusieurs possibilités : • une solution consiste à avoir une ligne directe (virtuelle) entre les différents lieux ; • dans certaines circonstances, une connexion sans fil peut être installée. Toutefois, il faut faire remarquer que ces équipements sans fil peuvent uniquement communiquer entre eux. Dans le cas de l'utilisation de la technologie sans fil, la politique de sécurité sur les réseaux sans fil est d'application (voir le site Internet de la Banque-carrefour de la Sécurité Sociale) ; • une autre solution consiste à installer une connexion VPN entre les sites via Internet. La solution standard recommandée par la Banque-carrefour de la Sécurité Sociale est la connexion VPN "IPsec" LAN-to-LAN.
7.5 MANIPULATION DES SUPPORTS IT PHYSIQUES ***(voir ISO 27002 – 10.7 Manipulation des supports)***		

B-7.5.1	**GLO**	Lors de l'utilisation de supports amovibles sur lesquels sont stockées des données à caractère personnel, il faut prendre les mesures de gestion adéquates. En voici quelques exemples :
		• si le support amovible quitte le périmètre de sécurité :
		  ○ les données à caractère personnel stockées doivent être supprimées si elles ne sont plus nécessaires ;
		  ○ avec des 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.

7.6 ÉCHANGE D'INFORMATIONS ***(voir ISO 27002 – 10.8 Échange des informations)***		
B-7.6.1	**SP KSZ-BCSS**	Toute transmission de données sociales au sein du réseau de la sécurité sociale doit être traitée aussi rapidement que possible par toutes les parties concernées, qu'elles soient intermédiaires ou destinataires/receveurs. Les institutions qui envoient des données sociales au sein du réseau de la sécurité sociale, en particulier lorsqu'elles sont la source authentique, doivent traiter en temps opportun les messages de suivi qu'elles doivent recevoir des destinataires ou des intermédiaires. Chaque partie impliquée dans l'envoi, aussi bien le destinataire/receveur que l'intermédiaire ou l'expéditeur, doit prendre dans les plus brefs délais les mesures appropriées lors du traitement des messages de suivi. Toute anomalie ou lacune dans l'envoi électronique des données doit être signalée le plus rapidement possible aux parties concernées, qu'elles soient receveur, intermédiaire ou expéditeur.

B-7.6.2	**SP KSZ-BCSS**	Lorsque l'institution dans la zone "USERID" du préfixe d'un message à la Banque-carrefour reprend le numéro de programme qui est à la base du message qu'elle envoie à la Banque-carrefour, bien que ce soit une personne physique qui soit à l'origine du message, la Banque-carrefour peut, a posteriori, retrouver le numéro de programme. La Banque-carrefour ne connaît toutefois pas l'identité de la personne physique qui a envoyé le message. Dans ce cas, l'institution de la sécurité sociale doit donc établir elle-même la relation entre le numéro de programme qu'elle reprend dans la partie préfixe du message qu'elle envoie à la Banque-carrefour et l'identité de la personne physique qui envoie le message.
B-7.6.3	**SP INT**	Les collaborateurs au service de plusieurs organisations doivent disposer d'une adresse e-mail distincte au sein de chaque organisation.
7.7 MONITORING ***(voir ISO 27002 – 10.10 Surveillance)***		
B-7.7.1	**GLO**	Pour l'utilisation et le traitement de données à caractère personnel, votre organisation doit constituer des rapports d'audit clairement protégés (activités, exceptions, événements), conformément aux mesures de référence de la Commission de la protection de la vie privée.
B-7.7.2	**GLO**	Votre organisation doit disposer d'une liste actualisée de toutes les personnes et de leurs niveaux d'accès respectifs aux données à caractère personnel.
B-7.7.3	**SP KSZ-BCSS**	Chaque institution de la sécurité sociale connectée au réseau de la Banque-carrefour doit tenir à jour la liste des flux ouverts sur l'Extranet de la sécurité sociale.
B-7.7.4	**SP INT**	Tout accès à un système d'information qui contient des données à caractère personnel doit pouvoir être tracé de manière à pouvoir également répondre à la question "pour quelle organisation ?", en plus des questions "qui a accédé, quand, à quoi et pourquoi ?". L'intégrité et la confidentialité ainsi que la séparation par organisation de ces loggings doivent être garanties et ils doivent pouvoir être consultés par les autorités habilitées.

8 ACCÈS À DES DONNÉES À CARACTÈRE PERSONNEL ***(voir ISO 27002 – 11 Contrôle d'accès)***		
8.4 CONTRÔLE D'ACCÈS AUX RÉSEAUX ***(voir ISO 27002 – 11.4 Contrôle d'accès aux réseaux)***		
B-8.4.1	**GLO**	Vos gestionnaires de réseaux doivent prendre des mesures de protection appropriées si un accès en ligne est accordé (par exemple via Internet ou via un réseau sans fil) à des données à caractère personnel
B-8.4.2	**SP INT**	Séparation des organisations Même si plusieurs organisations collaborent, il est nécessaire de réaliser une séparation physique et logique entre ces organisations. Au niveau du réseau, une

		séparation logique doit être réalisée, si une séparation physique n'est pas possible, de manière à ce que chaque utilisateur n'ait accès qu'à ses propres moyens.
8.5 CONTRÔLE D'ACCÈS AUX APPLICATIONS ET À L'INFORMATION ***(voir ISO 27002 – 11.6 Contrôle d'accès aux applications et à l'information)***		
B-8.5.1	**GLO**	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-8.5.2	**GLO**	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 ?).
B-8.5.3	**SP INT**	Séparation des organisations : • au niveau du système d'exploitation, les organisations doivent être séparées sur le plan logique ; • le système des droits d'accès doit pouvoir faire une distinction entre les collaborateurs des différentes organisations. Si un collaborateur travaille pour plusieurs organisations, il doit disposer d'un compte au sein de chaque organisation pour garantir une séparation de ses droits et de ses accès.
B-8.5.4	**SP INT**	Utilisation d'un progiciel commun L'utilisation d'un logiciel commun est autorisée. Lors de l'accès au logiciel et aux données stockées par ce progiciel, il faut toutefois pouvoir distinguer si cet accès a lieu au nom de la commune ou du CPAS (via un système pointu de gestion des utilisateurs et des accès). Il faut veiller à ce qu'il y ait une séparation logique des données (stockage).
B-8.5.5	**SP INT**	Système commun pour la comptabilité L'utilisation d'un seul logiciel comptable est autorisée à condition d'utiliser des comptes et des encodages distincts pour les deux entités. Cela sera d'ailleurs nécessaire dans le cadre d'audits externes et de documents comptables.
B-8.5.6	**SP INT**	Système commun pour la gestion du personnel Concernant la sécurité de l'information, pour le bon fonctionnement des organisations, un certain nombre de rôles et de fonctions doivent être définis au sein

		de chaque organisation séparément, en tenant compte des règles, des obligations et des limitations (restrictions ?) qui lui sont applicables. Des paquets pour l'enregistrement du temps, le règlement des vacances, l'enregistrement de la carrière, les salaires etc. peuvent être partagés, à nouveau à condition que l'accès et le stockage des données soient séparés.
B-8.5.7	**SP INT**	Afin de garantir une sécurité optimale du réseau, un simple utilisateur ne peut pas non plus disposer de droits d'administrateur sur son poste de travail dans un accord de coopération entre une ville/commune et un CPAS. Cette limitation des droits a pour but d'éviter que le poste de travail et le réseau ne soient infectés par du malware ou que le poste de travail de l'utilisateur ne soit mal configuré. Cette limitation a pour but que l'utilisateur ne dispose pas de toutes les fonctions sur son poste de travail. L'utilisateur ne sera par exemple pas autorisé à installer de nouvelles applications ou à modifier les paramètres du réseau ou du système. Cette mesure vaut aussi bien pour les postes de travail fixes ("desktops") que pour les postes de travail mobiles ("laptops"). Dans le cas de nouvelles Technologies (smartphones, tablettes, …), une analyse des risques doit être effectuée afin de pouvoir appliquer les mesures de sécurité appropriées.
B-8.5.8	**SP INT**	L'accès aux systèmes d'information doit pouvoir être accordé de manière granulaire. Il doit donc être possible d'accorder à un utilisateur uniquement les droits qui sont nécessaires à l'exécution de sa mission au sein de la commune/ville ou au sein du CPAS.
8.6 TRAVAILLER À DISTANCE ***(voir ISO 27002 – 11.7 Informatique mobile et télétravail)***		
B-8.6.1	**GLO**	Votre organisation doit instaurer les mesures de gestion nécessaires pour permettre l'utilisation de matériel informatique mobile (y compris d'autres supports mobiles) et le télétravail de manière sécurisée. Il peut notamment s'agir : • de techniques cryptographiques ; • de sauvegardes ; • d'un anti-virus; • d'une sécurisation des accès dans le cas de l'accès externe à des données à caractère personnel ; • d'une sécurité physique du matériel informatique portable (y compris des supports mobiles) et du lieu de télétravail contre le vol.
B-8.6.2	**SP KSZ-BCSS** **SP INT**	La seule solution autorisée pour accorder à un utilisateur un accès via Internet au réseau interne de l'organisation est d'utiliser une connexion sécurisée et contrôlée dont le concept a été approuvé par la Banque-carrefour de la Sécurité Sociale. Cette connexion doit remplir les conditions suivantes : • une authentification efficace de l'utilisateur et de l'ordinateur ; • un contrôle du niveau de sécurité du poste de travail avant de permettre la connexion ; • les connexions doivent être journalisées ; • il ne peut pas être possible de mettre en place simultanément des connexions avec différents réseaux. Des informations plus détaillées peuvent être obtenues dans la politique de sécurité relative à l'utilisation d'une connexion VPN publiée sur le site Internet de la Banque-carrefour de la Sécurité Sociale.

9 ACQUISITION, DÉVELOPPEMENT ET MAINTENANCE DES SYSTÈMES D'INFORMATION ***(voir ISO 27002 – 12 Acquisition, développement et maintenance des systèmes d'information)***		
9.1 EXIGENCES DE SÉCURITÉ APPLICABLES AUX SYSTÈMES D'INFORMATION ***(voir ISO 27002 – 12.1 Exigences de sécurité applicables aux systèmes d'information)***		
B-9.1.1	**GLO**	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.
9.2 SÉCURITÉ LORS DES PROCESSUS DE DÉVELOPPEMENT ET DE MAINTENANCE ***(voir ISO 27002 – 12.5 Sécurité en matière de développement et d'assistance technique)***		
B-9.2.1	**GLO**	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.

10 INCIDENTS LIÉS À LA SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 13 Gestion des incidents liés à la sécurité de l'information)***		
10.1 SIGNALEMENT DES ÉVÉNEMENTS ET DES FAILLES LIÉS À LA SÉCURITÉ DE L'INFORMATION ***(voir ISO 27002 – 13.1 Signalement des événements et des failles liés à la sécurité de l'information)***		
B-10.1.1	**GLO**	Votre organisation doit installer un système qui permet de : - détecter ; - assurer le suivi ; - et réparer des failles de sécurité relatives aux données à caractère personnel utilisées/traitées. Dans ce contexte, il faut accorder une attention aux processus appropriés de feed-back, aux formulaires pour le signalement de failles liées à la sécurité de l'information.

11 CONTINUITÉ DE L'ACTIVITÉ ***(voir ISO 27002 – 14 Gestion du plan de continuité de l'activité)***		
11.1 ASPECTS DE LA SÉCURITÉ DE L'INFORMATION EN MATIÈRE DE GESTION DE LA CONTINUITÉ DE L'ACTIVITÉ ***(voir ISO 27002 – 14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité)***		
B-11.1.1	**GLO**	Les procédures nécessaires doivent être mises en œuvre pour la récupération de vos processus d'exploitation 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-11.1.2	**GLO**	Vos mesures pour la continuité de la disponibilité des données à caractère personnel doivent être régulièrement testées et adaptées.
B-11.1.3	**SP KSZ-BCSS**	Chaque institution de la sécurité sociale connectée au réseau de la Banque-carrefour doit prévoir un centre de repli informatique en cas de catastrophe limitée ou totale.

12 CONFORMITÉ ***(voir ISO 27002 – 15 Conformité)***		
12.3 PRISES EN COMPTE DE L'AUDIT DU SYSTÈME D'INFORMATION ***(voir ISO 27002 – 15.3 Prises en compte de l'audit du système d'information)***		
B-12.3.1	**GLO**	Votre organisation doit 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.
B-12.3.2	**SP INT**	Système commun pour la comptabilité Dans le cas d'un audit externe de la comptabilité, il est nécessaire que les données qui n'appartiennent pas à l'organisation faisant l'objet de l'audit soient anonymisées si celles-ci doivent être transmises à l'auditeur.