Comité de sécurité de l'information
Chambre sécurité sociale et santé

CSI/CSSS/18/324

DÉLIBÉRATION N° 18/184 DU 4 DÉCEMBRE 2018 PORTANT SUR L'ÉCHANGE DE DONNÉES À CARACTÈRE PERSONNEL ENTRE LES ACTEURS DU RÉSEAU DE LA SÉCURITÉ SOCIALE ET LES ORGANISATIONS DES COMMUNAUTÉS ET RÉGIONS À L'INTERVENTION DES INTÉGRATEURS DE SERVICES DE CES COMMUNAUTÉS ET RÉGIONS

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, notamment son article 15, § 1er ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier l'article 114;

Vu la loi du 5 septembre 2018 *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, notamment l'article 97;

Vu le rapport de la Banque Carrefour de la sécurité sociale;

Vu le rapport de monsieur Bart Viaene.

A. OBJET

1. Conformément à l'article 14 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, toute communication de données à caractère personnel par des institutions de sécurité sociale à des tiers (tels les organisations des Communautés et Régions) intervient en principe à l'intervention de la Banque Carrefour de la sécurité sociale. Ces dernières années, les communications de données à caractère personnel par des institutions de sécurité sociale à des organisations de Communautés et Régions interviennent cependant aussi souvent à l'intervention de l'intégrateur de services de l'entité fédérée concernée qui, sur son terrain, veille à l'accès sécurisé et intégré aux données à caractère personnel de sources authentiques.

2. Les intégrateurs de services suivants sont donc chargés de la collecte et de l'échange de données à caractère personnel électroniques issues des sources authentiques pour les besoins des Communautés et des Régions. Le « Vlaamse Dienstenintegrator » (VDI), institué par le Décret flamand du 13 juillet 2012, la Banque Carrefour d'échange de données (BCED),

institué par l'accord de coopération entre la Région wallonne et la Communauté française du 23 mai 2013 et FIDUS, créé par l'ordonnance bruxelloise du 8 mai 2014. Au niveau fédéral, c'est la direction générale Transformation digitale du service public fédéral Stratégie et Appui (l'ancien FEDICT) qui intervient comme intégrateur de services. Ces organisations font toutes office d'intermédiaire entre les fournisseurs de données et les utilisateurs de données.

B. PRINCIPES D'INTERVENTION DES INTÉGRATEURS DE SERVICES

3. Il relève de la responsabilité des intégrateurs de services de respecter et de faire respecter par les destinataires réels des données à caractère personnel les principes de limitation des finalités et de minimisation des données, tels que décrits dans le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*. La Banque Carrefour de la sécurité sociale n'effectue pas de filtrage spécifique des données à caractère personnel pour autant que l'intégrateur de services intervenant s'engage explicitement, au moyen d'une convention écrite signée, à (faire) respecter les principes précités et à réaliser les filtrages utiles, en vue de l'application correcte des délibérations du comité de sécurité de l'information. Seules les données à caractère personnel dont le destinataire final a effectivement besoin dans le cadre de la réalisation de ses missions, et qui sont donc mentionnées en tant que telles dans la délibération applicable du comité de sécurité de l'information, peuvent être mises à sa disposition. L'intégrateur de services supprime les données à caractère personnel superflues (les données à caractère personnel qui ne sont pas pertinentes sur le plan du contenu pour le destinataire final ou qui ont trait à des personnes concernant lesquelles le destinataire final ne gère pas de dossier) et veille à ce qu'elles ne soient pas transmises au destinataire final. Par ailleurs, l'intégrateur de services de la Communauté ou de la Région ne peut pas conserver les données à caractère personnel issues du réseau de la sécurité sociale de manière structurelle, ni dans une banque de données de contenu, ni dans les loggings qu'il doit conserver afin de permettre la traçabilité de bout-en-bout lors de l'échange de données à caractère personnel (les loggings ne contiennent par conséquent pas les données à caractère personnel échangées proprement dites mais uniquement un renvoi au message applicable et au type de données à caractère personnel). Outre la source authentique du réseau de la sécurité sociale, seul le destinataire final peut (temporairement) conserver les données à caractère personnel reçues, aussi longtemps que ceci est nécessaire pour l'exécution de certaines de ses missions (ces missions et le délai de conservation approprié seront en règle générale définies par la chambre sécurité sociale et santé du comité de sécurité de l'information dans la délibération qu'elle rend en application de l'article 15 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, à l'occasion de l'évaluation du respect du principe de limitation des finalités et du principe de limitation de la conservation). L'engagement écrit précité de l'intégrateur de services doit aussi avoir trait à ce dernier aspect.

4. Lors de l'échange de données à caractère personnel du réseau de la sécurité sociale, il est fait usage d'un répertoire des références (actualisé en permanence) qui indique quelles organisations tiennent à jour un dossier concernant une personne déterminée (avec mention

de la période de validité). Le système créé sur la base de l'article 6 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* permet de mettre une personne en rapport avec une organisation et de décrire ce rapport en détail (la finalité qui justifie le traitement des données à caractère personnel de la personne et le type de dossier traité par l'organisation). Le répertoire des références permet de communiquer automatiquement des modifications de données (appelées mutations) aux parties mandatées et permet de contrôler que le fournisseur et l'utilisateur des données à caractère personnel gèrent tous les deux effectivement un dossier concernant l'intéressé (si tel n'est pas le cas, l'échange de données à caractère personnel perd sa justification).

5. Tout intégrateur de services doit être en mesure de distribuer un message électronique provenant du réseau de la sécurité sociale, reçu de la Banque Carrefour de la sécurité sociale, aux demandeurs compétents, sur la base d'un répertoire des références propre (inspiré ou non du répertoire des références de la Banque Carrefour de la sécurité sociale). Dans le répertoire des références de la Banque Carrefour de la sécurité sociale, il n'est dès lors pas repris de renvoi pour les personnes concernées jusqu'au niveau des diverses organisations compétentes (les destinataires finaux), mais uniquement un renvoi à la Communauté et à la Région compétente, ainsi qu'un contexte d'intégration et un groupe cible auquel sont liés certains messages électroniques (à cet égard, un regroupage est réalisé par besoin similaire). Si l'intégrateur de services ne s'est pas engagé par écrit vis-à-vis de la Banque Carrefour de la sécurité sociale à créer et gérer pareil répertoire des références (l'instrument nécessaire au respect des principes de limitation des finalités et de minimisation des données), les données à caractère personnel du réseau de la sécurité sociale peuvent uniquement être communiquées aux organisations des Communautés et des Régions dans la mesure où les personnes concernées (les personnes concernant lesquelles les destinataires finaux doivent pouvoir traiter des données à caractère personnel pour réaliser leurs missions) sont intégrées dans le répertoire des références de la Banque Carrefour de la sécurité sociale sous un code qualité approprié renvoyant à l'organisation en question. En d'autres termes, si l'intégrateur de services ne s'engage pas explicitement à développer un répertoire des références propre, la Banque Carrefour de la sécurité sociale assumera cette tâche, comme dans le passé. Lors du traitement de données à caractère personnel, il y a lieu de se mettre concrètement d'accord sur l'utilisation des répertoires des références. Il convient de déterminer de manière univoque, par organisation concernée, dans quel répertoire des références il est indiqué que cette organisation gère un certain type de dossier concernant une personne déterminée et pour une période déterminée, soit le répertoire des références de la Banque Carrefour de la sécurité sociale, un répertoire des références sectoriel existant ou le répertoire des références de l'intégrateur de services de l'entité fédérée. Les répertoires des références sont considérés comme des sources authentiques et il ne peut donc pas y avoir de redondance à ce niveau: l'indication selon laquelle une personne est connue auprès d'une organisation, ne peut donc être conservée qu'à un seul endroit (si l'affiliation auprès d'une institution de sécurité sociale déterminée est déjà indiquée dans un répertoire des références déterminé, cette affiliation ne doit pas être reprise une deuxième fois dans les répertoires des références des intégrateurs de services des Communautés et des Régions).

6. L'intégrateur de services doit, par ailleurs, participer à la réalisation de la traçabilité de bout-en-bout lors de l'échange de données à caractère personnel. Il doit donc pouvoir retracer à tout moment le trajet accompli par les données à caractère personnel issues du réseau de la

sécurité sociale depuis qu'elles lui ont été transmises par la Banque Carrefour de la sécurité sociale. Il doit développer à cet effet une gestion des loggings efficace et se mettre d'accord avec les divers destinataires finaux de données à caractère personnel sur la répartition des tâches en ce qui concerne la conservation des loggings (contenu, accès, durée de conservation, ...). Toute communication de données à caractère personnel du réseau de la sécurité sociale doit, par la suite, pouvoir être complètement retracée, depuis la source authentique jusqu'au destinataire final, et il y a lieu de pouvoir vérifier, éventuellement en combinaison avec les loggings des différentes parties (dans le cas d'un système graduel qui permet de se mettre mutuellement d'accord selon le principe des cercles de confiance), à tout moment quel collaborateur de quelle organisation a traité quel type de données à caractère personnel relatives à quel assuré social, à quel moment et pour quelles finalités (cela suppose une identification sure et unique des messages électroniques, de bout-en-bout). Ces mesures sont notamment prises pour satisfaire au droit de consultation de la personne concernée et pour, le cas échéant, offrir aux organes de contrôle compétents la possibilité de traiter des plaintes relatives au traitement de données à caractère personnel. Les loggings sont conservés pendant dix ans au moins, d'une manière sécurisée (avec restriction d'accès et sous la surveillance du délégué à la protection des données), et sont par ailleurs aussi traités conformément à la réglementation relative à la protection de la vie privée. Les loggings ne peuvent pas contenir le contenu réel du message mais uniquement un renvoi au message applicable (seul le type de données à caractère personnel peut être conservé et non les données à caractère personnel mêmes). L'engagement relatif à la gestion des loggings est également repris dans la convention écrite précitée qui est conclue entre l'intégrateur de services et la Banque Carrefour de la sécurité sociale.

7. Tout intégrateur de services doit, en outre, respecter les règles et directives relatives à la protection de la vie privée, en particulier le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* et la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, et les normes minimales de sécurité de l'information du réseau de la sécurité sociale, qui ont été rédigées par le Comité général de coordination de la Banque Carrefour de la sécurité sociale.

8. L'intégrateur de services informe la Banque Carrefour de la sécurité sociale sur les modalités de mise en application des mesures précitées. Il précise en particulier comment il réalisera la traçabilité de bout-en-bout du traitement des données à caractère personnel et comment il développera, mettra en place et gèrera le répertoire des références propre. Ces éléments sont également repris dans la convention précitée qui est conclue entre l'intégrateur de services et la Banque Carrefour de la sécurité sociale et font intégralement partie de l'engagement pris par l'intégrateur de services. Cette même convention fixe aussi les responsabilités respectives et indique qui est le responsable du traitement pour quel traitement partiel.

Par ces motifs,

la chambre sécurité sociale et santé du comité de sécurité de l'information

conclut que si la communication de données à caractère personnel du réseau de la sécurité sociale à une organisation d'une Communauté ou d'une Région se fait à l'intervention de l'intégrateur de services de cette Communauté ou Région, cet intégrateur de services est toujours tenu de respecter les mesures précitées. Il fixe son engagement (unique) dans une convention écrite avec la Banque Carrefour de la sécurité sociale.

Cette délibération ne porte nullement préjudice à la compétence du comité de sécurité de l'information pour se prononcer, au cas par cas, sur les communications de données à caractère personnel du réseau de la sécurité sociale, en application de l'article 15 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque Carrefour de la sécurité sociale*.

Bart VIAENE

Le siège de la chambre sécurité sociale et santé du comité de sécurité de l'information est établi dans les bureaux de la Banque Carrefour de la sécurité sociale, à l'adresse suivante: Quai de Willebroeck 38 - 1000 Bruxelles