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

CSI/CSSS/24/114

DÉLIBÉRATION N° 24/044 DU 5 MARS 2024 RELATIVE AUX BONNES PRATIQUES À APPLIQUER EN CAS D'UTILISATION DE SERVICES CLOUD PUBLICS

Le Comité de sécurité de l'information, chambre sécurité sociale et santé ;

Vu le Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (Règlement général relatif à la protection des données ou RGPD);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* ;

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, en particulier l'article 46 ;

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

Vu le rapport du président,

Émet, après délibération, la décision suivante, le 5 mars 2024:

I. OBJET DE LA DEMANDE

1. Le besoin des organisations et des institutions de sécurité sociale de recourir à des services de cloud public ne cesse de croître. Lors de l'utilisation de ces services, le responsable du traitement doit s'assurer que la protection des données soit correctement mise en place et que les opérations de traitement sur cette plateforme soient réalisées en conformité avec le RGPD.

II. COMPÉTENCE

2. En vertu de l'article 46, § 1er, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, la chambre sécurité sociale et santé du Comité de sécurité de l'information peut formuler les bonnes pratiques qu'elle juge utiles pour l'application et le respect de la présente loi et de ses mesures d'exécution et des dispositions fixées par ou en vertu de la loi visant à la protection de la vie privée à l'égard des traitements de données à caractère personnel relatives à la sécurité sociale.

3. Le Comité de sécurité de l'information s'estime par conséquent compétent.

III. BONNES PRATIQUES

4. Compte tenu des principes du Règlement général sur la protection des données (RGPD) et des dispositions de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, la chambre sécurité sociale et santé du Comité de sécurité de l'information formule les pratiques suivantes qui doivent au minimum être appliquées lors de l'utilisation de services de cloud public.

5. En vertu de l'article 5 du RGPD, le responsable du traitement veille à ce que les données à caractère personnel soient traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité). Ces mesures doivent assurer un niveau de protection adéquat compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraînent l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

6. Lors de l'établissement de la liste de bonnes pratiques, on part du principe que le fournisseur de service Cloud public ne peut pas avoir accès aux informations traitées sur la plateforme. Ceci est réalisé grâce à l'informatique confidentielle (« *confidential computing* ») qui permet de garantir, au moyen du chiffrement, que le fournisseur de service n'a pas accès à des données et codes lisibles, dans la mémoire et dans le processeur. Cet environnement sécurisé est aussi appelé enclave.

7. Lors du recours à l'informatique confidentielle, les conditions suivantes doivent au moins être remplies:

a. Le fournisseur de service Cloud public ne peut pas avoir accès aux informations traitées.

   i. Les données au repos « data at rest » doivent être protégées, peuvent uniquement être déchiffrées dans l'enclave sécurisée et doivent à nouveau être chiffrées avant de quitter l'enclave.
   ii. Les données en transit « data in transit » doivent être protégées, peuvent uniquement être déchiffrées dans une enclave sécurisée et doivent à nouveau être chiffrées avant de quitter l'enclave.
   iii. Les informations ne peuvent pas être transférées, de manière lisible, sur les réseaux Cloud, y compris au sein de la plateforme mise en place par l'utilisateur. Ceci s'applique donc aussi à la communication entre deux serveurs au sein de la même plateforme.
   iv. L'échange d'informations avec la plateforme de cloud doit avoir lieu de manière sécurisée.

b. L'attestation de l'informatique confidentielle de la plateforme de cloud public

   i. Avant que le logiciel ne traite des informations sensibles sur la plateforme d'informatique confidentielle, il doit être certain que la plateforme offre les garanties utiles au niveau de la protection. Ceci a lieu au moyen d'une attestation de l'informatique confidentielle.
   ii. L'attestation doit permettre de vérifier que l'environnement d'exécution est confidentiel et véridique, doit être réalisée de manière fiable et doit aussi être protégée. L'attestation doit pouvoir être exécutée indépendamment du fournisseur de service Cloud public.

c. Moyens de chiffrement et secrets

   i. Les clés de chiffrement et les secrets sont protégés jusque dans l'enclave et ne quitteront jamais l'enclave sous forme lisible.
   ii. Les clés de chiffrement et les secrets sont gérés sur un système auquel le fournisseur de service Cloud public n'a pas accès.

d. Moyens d'authentification

   i. Les moyens d'authentification doivent être traités de la même manière que les secrets.
   ii. Le fournisseur de service Cloud public n'a pas accès au système gérant les moyens d'authentification ou au système réalisant l'authentification.
   iii. Le fournisseur de service Cloud public n'a pas d'accès logique aux serveurs ou aux enclaves, ni même avec des moyens d'authentification propres.

e. Moyens d'autorisation

i. Le fournisseur de service Cloud public n'a pas accès au système gérant les autorisations.

f. Suppression des données

i. Le fournisseur de service Cloud public offre les garanties utiles que les données seront effectivement supprimées dans les systèmes de stockage lorsque l'utilisateur donne l'ordre à cet effet et fait régulièrement attester ces procédures par une partie externe.

g. Surveillance de la technologie utilisée

i. L'utilisateur doit conclure un contrat avec le fournisseur de service Cloud public selon lequel l'utilisateur est immédiatement informé de vulnérabilités éventuelles de la plateforme ou de ses composants de sorte que l'utilisateur puisse prendre des mesures adéquates pour limiter le risque.

h. Service level agreement

i. La relation avec le fournisseur de service Cloud public doit comprendre un service level agreement qui offre des garanties suffisantes que le fournisseur de service Cloud public réagira, de manière adéquate, aux menaces éventuelles susceptibles d'avoir un impact sur la protection des informations.

i. Réglementation applicable et litiges

i. Les contrats avec le fournisseur de service Cloud public doivent être conclus sous le droit belge ou le droit d'un autre pays européen. Les litiges relatifs au RGPD doivent être traités par l'Autorité de protection des données belge.

8. Le Comité de sécurité de l'information rappelle qu'en vertu de l'article 9 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, le responsable du traitement prend les mesures suivantes lors du traitement de données génétiques, biométriques ou des données concernant la santé :

1° les catégories de personnes ayant accès aux données à caractère personnel sont désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données à caractère personnel visées;

2° la liste des catégories des personnes ainsi désignées est tenue à la disposition de l'autorité de contrôle compétente par le responsable du traitement ou, le cas échéant, par le sous-traitant;

3° il veille à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

La présente délibération entre en vigueur le 20 mars 2024.

Michel DENEYER
Président