Comité de sécurité de l'information
Chambre autorité fédérale

DELIBERATION N° 20/057 DU 3 NOVEMBRE 2020 RELATIVE A LA COMMUNICATION DES DONNES A CARACTERE PERSONNEL PAR LE SPF FINANCES AU SPF BOSA DANS LE CADRE DES TESTS POUR LA MISE EN OEUVRE D'UN AUDIT TRAIL DE L'UTILISATION DE L'EBOX POUR LES PERSONNES FYSIQUES

Vu la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral, en particulier l'article 35/1, §1, premier alinéa, et §2;

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, en particulier les articles 111 et 114 ;

Vu la loi 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, en particulier l'article 98 ;

Vu la demande du service public fédéral Stratégie et Appui;

Vu le rapport de la présidente.

I. OBJET

1. Dans la délibération no 19/2008 du 7 mai 2008, l'ancien comité sectoriel du registre national a autorisé le service public fédéral des technologies de l'information et de la communication (ci-après «FEDICT») à avoir accès aux données d'information du registre national et à utiliser son numéro d'identification pour tester, corriger et tenir à jour les applications informatiques connectées au registre national par l'intermédiaire de l'UME, du FSB et des services Web.

2. Dans le cadre de la délibération susmentionnée, l'ancien comité sectoriel du registre national a établi que la FEDICT doit régulièrement tester, corriger et tenir à jour les applications informatiques connectées au Registre national et d'autres sources authentiques telles que la BCSS, par l'intermédiaire de l'UME, du FSB et des services Web, afin de fournir des services de qualité. Ce n'est qu'ainsi que le fonctionnement efficace, la sécurité et la disponibilité continue d'une application pourront être assurés. Dans ces tests, des applications informatiques sont utilisées et, par conséquent, l'accès à la source authentique, au moment où le Registre national est établi comme s'il s'agissait d'une transaction réelle. Le numéro

d'identification est également utilisé comme s'il s'agissait d'une transaction réelle avec la source authentique. Sans effectuer de véritables transactions, les essais ne sont pas efficaces et les applications ne peuvent être corrigées et maintenues. En conséquence, l'accès aux données du Registre national et l'utilisation du numéro du Registre national ont été autorisés, sous réserve de certaines conditions de sécurité strictes:
- le délégué à la protection des données (à l'époque le consultant en sécurité) du demandeur détermine la population sur laquelle les tests doivent être effectués avant les travaux internes de test, de correction et d'entretien;
- cette population compte jusqu'à 10 000 personnes;
- le délégué à la protection des données surveille de près le respect de ces paramètres par les personnes effectuant les travaux.

3. En application de l'arrêté royal du 22 février 2017 *portant création du Service public fédéral Stratégie et Appui* le SPF BOSA (ci-après «FOD Bosa») a repris et poursuivi les tâches et les pouvoirs de la FEDICT[1].

4. Conformément à la loi du 27 février 2019 *relative à l'échange électronique de messages par le biais de l'eBox*, le SPF BOSA a été chargé de fournir un eBox aux personnes physiques. L'eBox est une boîte aux lettres électronique sécurisée qui permet aux autorités publiques, d'une part, et aux citoyens et aux entreprises, d'autre part, d'échanger des messages.

5. Pour offrir et gérer l'eBox le SPF BOSA et les utilisateurs qui échangent des messages par la voie électronique par le biais de l'eBox sont autorisées à utiliser le numéro d'identification des personnes physiques inscrites au Registre national, à des fins d'identification et d'authentification de la personne physique et à des fins de communication entre les autorités et les utilisateurs (art. 8 de la loi du 27 février 2019 précitée).

6. Pour offrir et gérer l'eBox le SPF BOSA doit prendre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque et qui entre autres préservent l'origine et l'intégrité du contenu du message et garantissent la confidentialité du contenu du message. Le SPF BOSA utilise aussi des techniques informatiques sécurisées qui:
- permettent l'identification et l'authentification non équivoques de l'utilisateur et du destinataire, ainsi que la constatation non équivoque du moment de l'envoi et de la réception;
- enregistrent et mettent à disposition dans le système une preuve d'envoi et de réception du message;
- enregistrent l'identité de l'utilisateur et du destinataire, le moment de l'envoi et de la réception, la notification ainsi que le numéro unique attribué au message;
- identifient les erreurs de système et enregistrent les moments où les erreurs de système empêchent l'envoi ou la réception, et mettent ces informations à la disposition des intéressés.[2]

[1] Cfr. art. 7 et le Rapport au Roi de l'arrêté royal du 22 février 2017 précité.
[2] Art. 4 de la loi du 27 février 2019 précitée.

7. Un élément essentiel des mesures techniques et organisationnelles adéquates que doit prendre le SPF BOSA est l'établissement d'une piste de vérification (*audit trail*): Qui a eu accès au système d'information à quel moment et quel traitement a été effectué par ce système. On peut ainsi établir si une personne a fait un usage abusif d'un système d'information ou s'est efforcée de le faire, les utilisateurs compétents d'un système d'information peuvent être tenus responsables de leurs actes, les incidents peuvent être reconstitués et on peut donner preuve que certaines conditions juridiques ou réglementaires relatives à la durée ou aux modalités de conservation et de consultation des données sont respectées.

8. En tant que fournisseur et administrateur de l'eBox, le SPF BOSA souhaite maintenant effectuer un test en collaboration avec le SPF Finances pour établir un *audit trail* de l'utilisation de l'eBox (c.-à-d. la transmission d'un message par une institution fédérale à un citoyen). En principe, les tests sont effectués dans un environnement d'essai, mais dans ce cas, l'environnement d'intégration de la FPF Finance est insuffisant pour effectuer un test efficace.

9. Le test ne porte que sur la construction d'un *audit trail* dans le contexte de l'utilisation de l'eBox: Quelle institution (en l'occurrence, le SPF Finances) a envoyé un message à quelle personne physique à quel moment. Le message en question n'est que le message adressé à la personne concernée que sa déclaration de revenus ou une proposition de déclaration simplifiée est disponible sur le site Web du SPF Finances. Les données nécessaires à la réalisation du test de message réel sont les suivantes:
— Timestamp (indication temporelle de la transmission du message)
— Object_ID_Hashed (RRN of the attendee) – un one-way hash du numéro register national, SHA-256
— Document provider ID (identification du SPF Finances)
— API call response code (information indiquant si un citoyen a donné son consentement à l'utilisation de la boîte eBox ou non)

II. OBJET DE LA DEMANDE

A. COMPETENCE DU COMITE

10. En vertu de l'article 35/1, §1, premier alinéa, de la loi du 15 août 2012 *à la création et à l'organisation d'un intégrateur de services fédéral* la communication de données à caractère personnel par des services publics et des institutions publiques de l'autorité fédérale à des tiers autres que les institutions de sécurité sociale visées à l'article 2, alinéa 1er, 2°, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* doit faire l'objet une délibération préalable de la chambre autorité fédérale du comité de sécurité de l'information, dans la mesure où les responsables du traitement de l'instance qui communique et des instances destinatrices ne parviennent pas, en exécution de l'article 20 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel*, à un accord concernant la communication ou au moins un de ces responsables du traitement demande une délibération.

11. Conformément à l'art. 35/1, §2 de la loi du 15 août 2012 précitée, la chambre autorité fédérale du comité de sécurité de l'information rend, le cas échéant, une délibération pour l'utilisation

du numéro d'identification du Registre national des personnes physiques par les instances concernées si cela s'avère nécessaire dans le cadre de la communication envisagée.

12. Le Comité de sécurité de l'information est donc compétent à décider de la communication des données à caractère personnel et de l'utilisation du numéro du registre national.

B. QUANT AU FOND

B.1. RESPONSABILITE

13. Conformément à l'article 5.2 du règlement général sur la protection des données (ci-après dénommé «RGPD»), le SPF Finances (instance qui transfert les données) et le SPF BOSA (instance destinataire) en tant que responsables du traitement sont responsables du respect des principes du RGPD et devraient être en mesure de le démontrer.

14. Le Comité de sécurité de l'information rappelle que le responsable du traitement doit tenir un registre des activités de traitement effectuées sous sa responsabilité dans les conditions prévues à l'article 30 du RGPD.

B.2. LICEITE

15. Conformément à l'article 5.1 a) RGPD, les données à caractère personnel doivent être traitées d'une manière licite à l'égard de la personne concernée. Cela signifie que le traitement envisagé doit être fondé sur l'un des motifs juridiques énoncés à l'article 6 RGPD.

16. Le Comité note que le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement (article 6.1 e) RGPD. En vertu de la loi du 27 février *relative à l'échange électronique de messages par le biais de l'eBox*, le SPF BOSA est chargé d'offrir une eBox aux personnes physiques. Ce faisant, elle doit prendre les mesures techniques et organisationnelles nécessaires pour assurer la sécurité et la confidentialité des données, ce qui signifie qu'un *audit trail* doit être établie, en coopération avec les expéditeurs des messages, en l'occurrence le FPS Finances.

17. Compte tenu de ce qui précède, le Comité de sécurité de l'information considère que le traitement prévu des données à caractère personnel est licite.

B.3. LIMITATION DES FINALITES

18. Article 5.1 b) RGPD ne permet le traitement de données à caractère personnel que pour des fins déterminées, explicites et légitimes (principe de finalité). En outre, les données ne peuvent pas faire l'objet d'un traitement ultérieur d'une manière incompatible avec ces objectifs.

19. Pour s'acquitter de sa mission légale et pour fournir un service de qualité, il est nécessaire que le SPF BOSA puisse tester, éventuellement corriger et maintenir les applications. Ce n'est qu'ainsi que le fonctionnement efficace, la sécurité et la disponibilité continue d'une application pourront être assurés. Toutefois, sans effectuer de véritables transactions, les essais dans ce cas ne sont pas efficaces et les applications ne peuvent être corrigées et maintenues.

20. Compte tenu de ce qui précède, le Comité de sécurité de l'information considère que les finalités de la communication envisagée de données à caractère personnel sont déterminées, explicites et légitimes.

21. L'article 5, paragraphe 1, point b), du RGPD dispose également que les données à caractère personnel ne peuvent être traitées d'une manière incompatible avec leurs objectifs initiaux. Afin d'établir si les finalités d'un traitement ultérieur sont compatibles avec celles pour lesquelles les données à caractère personnel ont été collectées initialement, le responsable du traitement, après avoir respecté toutes les exigences liées à la licéité du traitement initial, devrait tenir compte, entre autres: de tout lien entre ces finalités et les finalités du traitement ultérieur prévu; du contexte dans lequel les données à caractère personnel ont été collectées, en particulier les attentes raisonnables des personnes concernées, en fonction de leur relation avec le responsable du traitement, quant à l'utilisation ultérieure desdites données; la nature des données à caractère personnel; les conséquences pour les personnes concernées du traitement ultérieur prévu; et l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu.[3]

22. Compte tenu de la loi du 27 février 2019 *relative à l'échange électronique de messages par le biais de l'eBox*, qui impose l'utilisation du numéro du registre national, et du fait que le SPF BOSA comme responsable de traitement doit prévoir des mesures techniques et organisationnelles adéquates, y compris l'établissement d'un *audit trail*, et que l'utilisation de transactions réelles est nécessaire à des tests efficaces, le Comité de la sécurité de l'information constate qu'il existe un lien suffisant entre les objectifs de la collecte initiale et les objectifs du traitement ultérieur prévu. Le comité de la sécurité de l'information considère donc que l'objet du traitement ultérieur est compatible avec l'objectif pour lequel les données à caractère personnel ont été initialement collectées.

B.4. PROPORTIONALITE

B.4.1. Minimisation de données

23. L'article 5.1 b) du RGPD dispose que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées («minimisation des données»).

24. Le Comité de sécurité de l'information note que le traitement prévu des données à caractère personnel se limite aux données techniques du message, à l'identification de l'expéditeur (SPF Finances) et à l'identification du destinataire (une personne physique), c.-à-d. un hash du numéro registre national. Par analogie avec la décision de l'ancien comité sectoriel du registre national, le comité de la sécurité de l'information estime acceptable que le SPF BOSA puisse effectuer les tests avec des données réelles dans l'environnement de production afin d'établir un *audit trail*. Toutefois, le comité de la sécurité de l'information estime que ce traitement devrait être soumis aux conditions suivantes:

- le délégué à la protection des données du SPF BOSA détermine la population sur laquelle les tests doivent être effectués avant les travaux internes d'essai, de correction et d'entretien;

- cette population compte jusqu'à 10 000 personnes;

- le délégué à la protection des données surveille de près le respect de ces paramètres par les personnes effectuant les travaux.

[3] Considération 50 du RGDP.

25. Compte tenu de ce qui précède, le Comité de sécurité de l'information considère que les données à caractère personnel sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

B.4.2. Limitation de conservation

26. En ce qui concerne le délai de conservation, le Comité rappelle que les données à caractère personnel ne doivent plus être conservées sous une forme permettant d'identifier les personnes concernées au-delà des finalités pour lesquelles les données à caractère personnel sont traitées.

27. Le Comité de sécurité de l'information prend acte du fait que si le test n'est pas réussi, les données seront immédiatement détruites. Si le test est concluant, les données doivent être stockées temporairement afin de prouver que le demandeur et l'expéditeur de documents ont mené à bien un *audit trail*. Compte tenu de ce qui précède, le Comité estime qu'une période de conservation des résultats des tests pouvant aller jusqu'à 6 mois est acceptable.

B.5. SECURITE

28. Les données à caractère personnel doivent être traitées en prenant des mesures techniques ou organisationnelles appropriées de manière à assurer une sécurité adéquate, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle («intégrité et confidentialité»).

29. Le Comité de sécurité de l'information note que SPF BOSA a un délégué à la protection des données et qu'il est tenu de respecter les normes de sécurité applicables à toutes les institutions fédérales incluses dans la politique fédérale sur la sécurité de l'information (Federal Information Security Policy).

30. Le Comité de sécurité de l'information note que le test en question sera effectué par une personne identifiée du Directorat-général Transformation Digitale du SPF BOSA, qui a également signé une déclaration de confidentialité. En consultation avec le délégué à la protection des données du SPF BOSA, le nombre de cas requis est déterminé, avec un maximum de 10 000. Après la reconstruction du audit trail en collaboration avec le SPF Finances, les données de test seront détruites après une période de conservation maximale de 6 mois.

31. Le Comité de la sécurité de l'information note que, dans le cadre de l'essai prévu, le numéro du registre national serait encrypté, en particulier au moyen d'un hachage à sens unique SHA 256. Le Comité souligne, tout d'abord, qu'un hache d'un numéro de registre national n'est plus un numéro de registre national, de sorte qu'il n'est peut-être pas possible d'effectuer tous les tests envisagés. De plus, l'utilisation d'un SHA-256 signifie qu'il n'y a que 36,5 millions de possibilités et qu'un tableau de correspondance peut être établi en quelques secondes. Le Comité estime que si le SPF Bosa veut obtenir plus que la sécurité symbolique, il est plus important d'appliquer SHA-256 1 milliards de fois, voire mieux, pour utiliser une fonction de hachage comme Argon2 avec des paramètres qui garantissent que le hachage du d'un numéro registre nationale prend 30-60 secondes et nécessite 1 Gbyte de RAM. De cette manière, le calcul ou l'élaboration d'une table exige un effort considérable. De plus, si le SPF BOSA veut que le résultat de hachage soit représenté comme un numéro de registre national, un format de conservation du chiffrement peut être utilisé, bien que cela puisse nécessiter la

gestion d'une clé secrète[4]. Le Comité de sécurité de l'information conclut donc que le SPF BOSA, en coopération avec son délégué à la protection des données, devrait exercer une fonction de hachage garantissant une sécurité efficace et adéquate.

32. Le Comité rappelle que, dans certains cas, l'article 35 du RGPD impose au responsable du traitement de procéder à une évaluation de l'impact des activités de traitement envisagées sur la protection des données à caractère personnel avant le traitement. À cet égard, le Comité se référerait aux "lignes directrices pour les évaluations d'impact sur la protection des données et déterminerait si le traitement présente un "risque probablement élevé" au sens du règlement (CE) no 2016/679 du groupe de travail article 29 et de la recommandation de la Commission no 01/2018 du 28 février 2018 relative à la protection de la vie privée en ce qui concerne l'évaluation d'impact sur la protection des données et la consultation préalable'.

33. Si cette évaluation montre qu'il y a lieu de prendre des mesures supplémentaires, les parties concernées présentent, de leur propre initiative, une demande de modification du présent débat. Le cas échéant, la communication de données à caractère personnel n'a lieu que lorsque l'autorisation requise du comité a été obtenue. Si l'analyse d'impact sur la protection des données montre qu'il existe un risque résiduel élevé, le demandeur doit soumettre le traitement des données prévu à l'Autorité de la protection des données, conformément à l'article 36.1 du RGPD.

[4] https://csrc.nist.gov/publications/detail/sp/800-38g/final

Par ces motifs,

la chambre autorité fédérale du Comité de sécurité de l'information

conclut que la communication des données à caractère personnel par le SPF Finances au SPF BOSA dans le cadre des tests pour la mise en œuvre d'un *audit trail* de l'utilisation de l'eBOX pour les personnes physiques, est autorisée moyennant le respect des mesures de protection des données définies, en particulier les mesures en matière de limitation de la finalité, de minimisation des données, de limitation de la durée de conservation des données et de sécurité de l'information, pour autant que :

- le délégué à la protection des données du SPF BOSA détermine la population sur laquelle les tests doivent être effectués avant les travaux internes d'essai, de correction et d'entretien;

- cette population compte jusqu'à 10 000 personnes;

- le délégué à la protection des données surveille de près le respect de ces paramètres par les personnes effectuant les travaux ;

- pour le hachage du numéro du registre national en collaboration avec le délégué à la protection des données, une fonction de hachage est appliquée qui garantit une sécurité efficace et adéquate (voir paragraphe 31).

En vertu de l'art. 35/1, §2 de la loi du 15 août 2012 2012 *à la création et à l'organisation d'un intégrateur de services fédéral*, la chambre autorité fédérale du comité de sécurité de l'information autorise l'utilisation du numéro d'identification du Registre national, sous forme hash, dans l'environnement de production afin d'établir un *audit trail*

Le comité de sécurité de l'information indique que les responsables du traitement sont tenus de procéder, conformément à l'article 35 RGDP, à une évaluation d'impact sur la protection des données. Si cette évaluation montre qu'il y a lieu de prendre des mesures supplémentaires pour protéger les droits et libertés des personnes concernées, les parties sont tenues de soumettre les dispositions relatives au traitement des données modifiées au Comité de sécurité de l'information.

M. SALMON

Présidente

Le siège de la chambre autorité fédérale du Comité de sécurité de l'information est établi dans les bureaux du SPF Stratégie et Appui à l'adresse suivante: Boulevard Simon Bolivar 30, 1000 Bruxelles.