Avis n° 103/2018 du 17 octobre 2018

Objet : Projet d'arrêté ministériel portant exécution de certaines dispositions de l'arrêté royal du 16 mars 2009 *relatif à la protection des dépôts et des assurances sur la vie par le Fonds de garantie pour les services financiers* (CO-A-2018-096)

L'Autorité de protection des données (ci-après "l'Autorité") ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 ;

Vu la demande d'avis du Ministre des Finances, reçue le 31 août 2018 ;

Vu le rapport du Président ;

Émet, le 17 octobre 2018, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le 31 août 2018, l'Autorité a reçu une demande d'avis du Ministre des Finances (ci-après le demandeur) concernant un projet d'arrêté ministériel portant exécution de certaines dispositions de l'arrêté royal du 16 mars 2009 relatif à la protection des dépôts et des assurances sur la vie par le Fonds de garantie pour les services financiers[1].

2. Le projet entend exécuter aussi bien l'article 14/1, § 1er, premier alinéa de l'arrêté royal précité du 16 mars 2009 que l'article 7, point 6 de la Directive 2014/49/UE[2]. Ces articles sont libellés comme suit :

> *Art. 14/1. § 1er. En cas de défaillance d'un établissement de crédit ou d'une société de bourse, l'établissement de crédit ou la société de bourse ou le curateur doivent communiquer au Fonds de garantie le fichier informatique établi conformément à l'article 13/2 ou les données exactes, qui sont nécessaires pour payer les interventions au titre de la protection des dépôts, notamment :*
>
> *1° les données requises pour l'identification du titulaire d'un avoir qui entre en compte pour une intervention ;*
>
> *2° le montant de l'intervention qui est déterminé conformément à l'article 11 et qui est limité au montant visé à l'article 6, alinéa 1er, de l'arrêté royal du 14 novembre 2008 ;*
>
> *3° le cas échéant, l'existence des dépôts bloqués et les raisons légales, judiciaires ou conventionnelles du blocage.*
>
> ***Art. 7. Détermination du montant remboursable***
>
> *(...)*
>
> *6. Les États membres veillent à ce que les systèmes de garantie des dépôts puissent à tout moment demander aux établissements de crédit qu'ils les informent du montant total des dépôts de chaque déposant.*

II. CONTEXTE DU PROJET

3. Le présent arrêté s'inscrit dans le cadre de l'exécution de la législation européenne visant à garantir la stabilité du système bancaire et la protection des déposants[3] par une harmonisation européenne des systèmes de garantie des dépôts[4].

[1] M.B., 25 mars 2009.
[2] Directive 2014/49/UE du Parlement européen et du Conseil du 16 avril 2014 *relative aux systèmes de garantie des dépôts*.
[3] Considérant 3 de la Directive 2014/49/UE.
[4] Considérants 3 et 4 de la Directive 2014/49/UE.

III. CONTENU DU PROJET

4. Le projet d'arrêté ministériel porte sur la réglementation de deux flux de données vers le Fonds de garantie. Il s'agit d'une part du flux de données mentionné à l'article 14/1, § 1er, premier alinéa de l'arrêté royal précité du 16 mars 2009 ("élaboration d'un fichier informatique") et d'autre part d'un flux de données pour la réalisation de tests de résistance.

5. Les articles 2 à 4 inclus du projet sont repris dans un Chapitre 2 intitulé "Élaboration du fichier informatique" (voir ci-après).

6. Les articles 7 à 15 inclus du projet constituent le Chapitre 5 intitulé "Les tests de résistance". Le Fonds de garantie organise au moins tous les trois ans des tests de résistance afin de contrôler et d'évaluer les risques opérationnels liés au système de garantie des dépôts (article 7 du projet).

IV. EXAMEN DU PROJET

1. Applicabilité du RGPD

7. L'Autorité n'examine ci-après que les dispositions du projet qui concernent un traitement de données à caractère personnel.

8. La communication de données à caractère personnel au Fonds de garantie via un fichier informatique constitue un traitement de données à caractère personnel. Dès lors, le RGPD s'applique à ce traitement.

9. Le considérant 44 de la Directive précitée 2014/49/UE énonce en outre ce qui suit : "*La directive 95/46/CE du Parlement européen et du Conseil[5] s'applique au traitement des données à caractère personnel effectué en vertu de la présente directive. Les systèmes de garantie des dépôts et les autorités concernées devraient traiter les données relatives aux dépôts individuels avec un soin extrême et maintenir un niveau élevé de protection des données conformément à ladite directive."*

10. L'article 9, § 1 du projet dispose que les données transmises par l'établissement dans le cadre des tests de résistance "*ont été anonymisées au sens de l'article 1er, 5° de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative a la protection de la vie privée à l'égard des traitements de données à caractère personnel*."."

11. Par ailleurs, l'article 9, § 3 dispose que "*les données à caractère personnel sont anonymisées dans le fichier informatique selon les modalités fixées à l'Annexe 2* ".

[5] Remplacée par le RGPD.

12. L'Autorité remarque que l'arrêté royal précité du 13 février 2001 a été abrogé à compter du 5 septembre 2018 par l'article 280 de la loi du 30 juillet 2018[6]. Bien que le RGPD ne contienne pas de définition formelle des données anonymes, il faut supposer qu'il s'agit d' "*informations ne concernant pas une personne physique identifiée ou identifiable, [ou de] données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable* "[7].

13. Par ailleurs, il résulte du RGPD qu'il est préférable de travailler avec différents niveaux de gradation entre le niveau de données à caractère personnel directement identifiables et les données anonymes. Les données pseudonymisées[8] sont donc encore des données à caractère personnel.

14. Il ressort de l'examen des données de l'annexe 2 du projet qu'il y a une **contradiction entre l'article 9, § 1 d'une part et l'article 9, § 3 et l'annexe 2 d'autre part**. L'annexe 2 comporte les données de personnes physiques partiellement codées ou supprimées. Il est question (d'une combinaison) du numéro de client, de la catégorie du client (dont le code 0 pour personne physique), du pays de résidence, ...

15. L'Autorité estime que la réduction du lien pouvant être établi entre les données et une personne physique est insuffisante en raison de l'existence de "small cells" dans l'ensemble de données de l'annexe. Il s'agit donc d'un traitement de **données à caractère personnel pseudonymisées au lieu de données anonymes**. Il ressort d'une explication supplémentaire du demandeur du 20 septembre 2018 que ce dernier est d'accord avec ce point de vue.

16. Il convient donc de supprimer de l'article 9, § 1 le texte à partir de "au sens de ..." et soit de le remplacer par une technique qui garantit effectivement l'anonymisation, soit de préciser que les tests sont effectués sur la base de données pseudonymisées.

17. Si l'on opte pour la première option, l'Autorité suggère d'insérer la formulation suivante après les termes "*dont les données ont été anonymisées*" : "*au moyen d'une méthode ou de critères d'évaluation sur la base desquels l'établissement peut prouver que les données ne concernent pas une personne physique identifiée ou identifiable ou concernent des données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable*".

18. Si l'on opte pour la deuxième option, il faut supprimer la référence au terme "anonyme" dans l'annexe. À l'article 9, § 3, le terme "anonymisées" doit être remplacé par le terme "pseudonymisées".

---

[6] Loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, M.B. du 5 septembre 2018.
[7] Considérant 26 du RGPD.
[8] Le considérant 26 du RGPD dispose ce qui suit : "Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable."

À l'article 9, § 1, il faut supprimer la deuxième partie de la phrase, à partir des termes "dont les données ont été".

2. Détermination des données du traitement

19. Outre les données mentionnées à l'article 14/1, § 1er, premier alinéa de l'arrêté royal précité du 16 mars 2009, le projet prévoit encore le traitement de données complémentaires qui peuvent concerner différentes personnes physiques :

- l'article 3 et l'annexe du projet renvoient aux données complémentaires ("éléments d'information")[9] qui doivent être reprises dans chaque fichier informatique et qui concernent les dépôts couverts. Elles sont distinctes des données reprises séparément (article 2 du projet) ;
- si la personne concernée (le "déposant") dispose de plusieurs numéros de client, le demandeur doit aussi grouper ces données sous un numéro de client ;
- les informations nécessaires à l'application du manuel de procédure mentionné à l'article 13/2, § 1 de l'arrêté royal du 16 mars 2009 (article 5 du projet). Outre des informations techniques, elles concernent également des personnes dans des établissements de crédit (personnes de contact et personnes chargées de la création des fichiers informatiques,...) et des personnes du Fonds de garantie.

3. Confidentialité et principe de limitation des finalités (article 5.1 b) du RGPD)

20. L'article 10 du projet dispose que le Fonds de garantie respecte la confidentialité des données qui lui sont transmises par les établissements et qu'il utilise les informations reçues uniquement pour la réalisation des tests de résistance.

21. L'article 10 du projet étant repris dans le Chapitre 4 sur les tests de résistance, on ne sait pas clairement si cette disposition s'applique aussi aux dispositions du Chapitre 2, même en dehors de ce contexte.

22. Pour apporter une réelle plus-value, l'Autorité recommande que l'article 10 soit repris en tant que disposition générale en dehors des Chapitres 2 et 4, par exemple en insérant dans un chapitre distinct (intitulé "protection des données"), avant le Chapitre 5, les éléments précités en tant que dispositions concrètes de protection des données, respectant ainsi le présent avis.

[9] Label "BBFFSP", code BIC de l'établissement de crédit, identifiant du fichier, nombre de lignes de données clients incluses dans le fichier, date de la défaillance ou date de production du fichier dans le cadre d'un test de résistance, numéro de version du fichier.

4. Implication du délégué à la protection des données ("DPO")

23. D'après l'article 38.1 du RGPD, le DPO du responsable du traitement doit être associé "à toutes les questions relatives à la protection des données à caractère personnel". Le DPO doit donc être impliqué notamment dans les obligations de transparence et de sécurité (voir ci-après) et formuler le cas échéant à cet égard des avis et des recommandations au niveau le plus élevé de la direction du SPF Finances.

24. Il ressort d'une explication complémentaire du demandeur du 20 septembre 2018 que le Fonds de garantie ne dispose pas d'un propre DPO, étant donné qu'il dépend des services du président du SPF Finances. Cette explication révèle également que le DPO n'était pas impliqué dans ce projet (article 38.1 du RGPD). Étant donné qu'il ne s'agit pas d'un projet qui est soumis au Conseil des ministres mais d'un arrêté ministériel concernant un traitement relevant de la responsabilité du SPF Finances, l'Autorité estime que le DPO compétent devait être impliqué en temps utile à l'égard de ce traitement. L'Autorité estime non seulement que cette méthode est obligatoire en vertu du RGPD mais qu'elle peut également permettre d'éviter une mauvaise utilisation de la terminologie (par exemple "anonymisées") dans le projet.

5. Application de la responsabilité (au sens du RGPD) à l'obligation d'anonymiser les données des tests de résistance

25. Dans la mesure où l'on ne choisit pas de travailler avec des données pseudonymisées (voir la proposition 2 à cet égard), l'article 9, § 1 du projet ne tient pas compte de l'obligation du responsable (l'établissement) de pouvoir démontrer que seules des données anonymes sont transmises pour les tests de résistance ("responsabilité" à l'article 5.2 du RGPD).

26. L'affirmation à l'article 9 du projet selon laquelle les données (des tests de résistance) "ont été anonymisées" n'est pas compatible avec le RGPD s'il n'y a pas de garantie que le transfert se fait aussi effectivement de manière anonyme. Ce n'est pas tant le renvoi vers une (la bonne) définition juridique du terme anonyme qui est déterminant ici, mais le fait que les établissements doivent pouvoir démontrer selon quelle méthode ou selon quels critères d'évaluation ils ont anonymisé les données. Le Groupe 29[10] a déjà formulé précédemment un avis critique à cet égard.

[10]Voir l'avis 05/2014 WP 216 du 10 avril 2014 *sur les techniques d'anonymisation*, publié sur http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

6. Transparence du traitement de données à caractère personnel par le Fonds de garantie

27. L'Autorité constate que le Fonds de garantie ne publie aucune déclaration de confidentialité (distincte[11]) sur son site Internet alors qu'il est question de divers traitements de données à caractère personnel. Les données à caractère personnel susmentionnées concernent le traitement réalisé dans le cadre du système de garantie des dépôts et sont reprises dans diverses sources techniques (arrêté royal, arrêté ministériel et manuel de procédure), ce qui peut faire obstacle à la transparence des traitements à l'égard des personnes concernées.

28. Le demandeur a déclaré ce qui suit dans une explication complémentaire du 20 septembre 2018 : "*Dans l'attente d'éventuels développements spécifiques au Fonds de garantie, nous appliquons en effet la politique privacy du SPF Finances* ". Ce choix stratégique n'est toutefois pas assez transparent pour les personnes concernées.

29. Afin de garantir une transparence suffisante du traitement, le site Internet du Fonds de garantie doit dès lors au moins renvoyer à la déclaration sur le site Internet du SPF Finances, à condition que celui-ci contienne aussi les informations pertinentes sur les traitements de données à caractère personnel dans le cadre du système de garantie des dépôts (article 14 du RGPD). L'alternative consiste à ce que le Fonds de garantie élabore une propre déclaration de confidentialité pour les traitements qui le concernent.

7. Remarques techniques concernant la sécurité (article 32 du RGPD)

30. En vertu de l'article 32 du RGPD, les établissements doivent tenir compte, pour la sécurité des données à caractère personnel, de "l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques". Les mesures (par exemple la pseudonymisation) doivent aussi être adaptées au risque pour les personnes concernées.

31. Les tests de résistance ont pour but d'évaluer la qualité des fichiers transmis et de déterminer les principaux manquements et corrections requises, en termes de format et de contenu. On teste ainsi si plus ou moins de "5 % des lignes" ne sont pas conformes ou si toutes les lignes sont conformes (article 11, § 1 du projet). Cela peut générer comme résultat "failed", "error" ou "success".

[11] Outre le site Internet du SPF Finances.

32. Si le RGPD est bien applicable (maintien des annexes actuelles du projet), les tests de validation de l'article 11 sont quoi qu'il en soit insuffisants pour répondre à l'approche basée sur les risques de l'article 32 du RGPD. Un test de l'exactitude technique des transferts de données ne peut en effet pas être considéré comme une évaluation complète des risques en fonction des droits et libertés des personnes concernées.

IV. CONCLUSION

33. L'Autorité constate qu'une grande partie des dispositions du projet sont des éléments techniques propres à la réglementation sur les garanties des dépôts qui ne relèvent pas de sa compétence. Elle ne se prononce pas à ce sujet.

34. À l'article 9 du projet, le renvoi à l'anonymisation de l'arrêté royal du 13 février 2001 est trompeur. Il ressort de l'annexe 2 ainsi que d'une confirmation complémentaire du demandeur que les tests de résistance comportent en effet un traitement de données à caractère personnel pseudonymisées. Il convient de toute façon de supprimer du projet toute référence à l'arrêté royal du 13 février 2001 et aux données anonymes (point 12).

35. L'Autorité estime que les garanties de confidentialité et de limitation des finalités (article 10) devraient de préférence être reprises dans un Chapitre distinct "protection des données", de sorte que les traitements qui concernent assurément un traitement de données à caractère personnel (Chapitre 2) soient soumis à une disposition de protection des données substantielle (point 22).

36. Un renvoi à la déclaration de protection des données sur le site Internet du SPF Finances est requis afin de garantir un traitement transparent (point 28).

37. L'avis de l'Autorité sur un arrêté ministériel ne peut se substituer au rôle d'avis du DPO (article 39.1 a) du RGPD). Le DPO du SPF Finances devait être associé en temps utile au traitement qui relève uniquement de la responsabilité du SPF Finances (article 38.1 du RGPD).

PAR CES MOTIFS,

l'Autorité émet un **avis défavorable sur l'article 9** de l'arrêté soumis.

Elle émet un avis favorable sur les autres dispositions qu'elle a évoquées dans le présent avis, sous réserve du respect des remarques mentionnées aux points 34 à 37 inclus.

Elle ne se prononce pas sur les autres dispositions du projet.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere