Avis n° 132/2018 du 28 novembre 2018

Objet : projet de loi modifiant la loi du 17 juin 2016 relative aux marchés publics, la loi du 17 juin 2016 relative aux contrats de concession et la loi du 13 août 2011 relative aux marchés publics et à certains marchés de travaux, de fournitures et de services dans les domaines de la défense et de la sécurité (CO-A-2018-122)

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 Secrétaire d'État chargé de la Simplification administrative, reçue le 1er octobre 2018 ;

Vu le rapport du Président ;

Émet, le 28 novembre 2018, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le 1er octobre 2018, l'Autorité a reçu une demande d'avis du Secrétaire d'État chargé de la Simplification administrative concernant un projet de loi modifiant la loi du 17 juin 2016 relative aux marchés publics, la loi du 17 juin 2016 relative aux contrats de concession et la loi du 13 août 2011 relative aux marchés publics et à certains marchés de travaux, de fournitures et de services dans les domaines de la défense et de la sécurité (ci-après "le projet").

2. Le projet vise une adaptation de trois lois à la suite de la transposition de la Directive 2014/55/UE du Parlement européen et du Conseil du 16 avril 2014 *relative à la facturation électronique dans le cadre des marchés publics*[1]. Ces trois lois sont les suivantes :

- la loi du 17 juin 2016 *relative aux marchés publics* ;
- la loi du 17 juin 2016 *relative aux contrats de concession* ;
- la loi du 13 août 2011 *relative aux marchés publics et à certains marchés de travaux, de fournitures et de services dans les domaines de la défense et de la sécurité*.

II. CONTEXTE DU PROJET

3. Le présent projet s'inscrit dans le cadre de l'exécution de la législation européenne qui a pour but de développer un modèle européen pour la facturation électronique dans le cadre des marchés publics.

4. Le Contrôleur européen de la protection des données a déjà émis un avis[2] le 11 novembre 2013 sur cette question avec des recommandations pertinentes visant à garantir un niveau suffisant de protection des données dans le cadre de l'application de la législation européenne susmentionnée.

5. Le législateur doit tenir compte de ces recommandations et des principes complémentaires du Règlement (UE) 2016/679[3] (ci-après le "RGPD") lors du traitement des données à caractère personnel par des pouvoirs adjudicateurs ou des entités adjudicatrices. Il convient, en particulier, d'établir clairement que la législation existante en matière de protection des données s'applique également dans le domaine de la facturation électronique, et que, lors de la publication de données à caractère personnel, il convient de respecter le juste équilibre entre les exigences en matière de transparence et de responsabilité et le respect de la vie privée[4].

---

[1] JO, *L 133, 6.5.2014*.
[2] https://edps.europa.eu/sites/edp/files/publication/13-11-11_electronic_invoicing_fr.pdf.
[3] 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*.
[4] Considérant 36 de la Directive 2014/55/UE.

III. CONTENU DU PROJET

6. Le projet contient diverses dispositions relatives à l'envoi électronique de factures aux pouvoirs adjudicateurs et aux entreprises publiques (articles 6, 9, 14, 17, 20 et 24 du projet).

IV. EXAMEN DU PROJET

1. Applicabilité du RGPD

7. La Directive 2014/55/UE susmentionnée affirme ce qui suit dans son considérant 20 : "*Les factures électroniques étant susceptibles de contenir des données à caractère personnel, la Commission devrait également exiger que la norme européenne sur la facturation électronique tienne compte de la protection des données à caractère personnel, conformément à la directive 95/46/CE du Parlement européen et du Conseil, ainsi que des principes de protection des données dès la conception, de proportionnalité et de minimisation des données*."

8. Actuellement, la Directive 95/46/CE a été remplacée par le RGPD, les principes susmentionnés de protection des données étant repris aux articles 5 et 25 du RGPD et complétés par de nouvelles obligations et de nouveaux principes.

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

2. Données traitées - principe de minimisation des données

10. Les articles 4, 11 et 19 du projet insèrent une nouvelle définition d' "éléments essentiels d'une facture électronique"[5] dans les trois lois susmentionnées. Les articles 7, 15 et 21 du projet contiennent une disposition similaire qui précise que la facture électronique contient au moins les éléments essentiels suivants qui sont repris de la Directive 2014/55/UE susmentionnée :

"1° identifiants de processus et de facture ;
2° période de facturation ;
3° renseignements concernant le vendeur ;
4° renseignements concernant l'acheteur ;
5° renseignements concernant le bénéficiaire du paiement ;
6° renseignements concernant le représentant fiscal du vendeur ;
7° référence du contrat ;
8° détails concernant la fourniture (par ex. l'adresse) ;
9° instructions relatives au paiement ;
10° renseignements concernant les déductions ou frais supplémentaires ;

[5] "*un ensemble d'informations essentielles qui doit figurer dans une facture électronique pour permettre l'interopérabilité transfrontière, y compris les informations nécessaires pour assurer le respect de la législation*."

11° informations concernant les postes figurant sur la facture ;
12° montants totaux de la facture ;
13° répartition par taux de TVA. "

11. L'Autorité estime que les termes "au moins" dans les articles 7, 15 et 21 du projet formulés de manière similaire ne peuvent pas faire l'objet d'une interprétation extensive, étant donné que ce sont principalement les éléments essentiels 3 à 6 inclus qui peuvent concerner un traitement de données à caractère personnel qui doit absolument satisfaire au **principe de minimisation des données** mentionné à l'article 5.1.c) du RGPD[6]. Les autres informations (fiscales, comptables, ...) peuvent toutefois aussi concerner une personne physique (par ex. l'acheteur, le vendeur, ...) de sorte que le traitement des données de ces champs doit également être considéré comme un traitement de données à caractère personnel.

12. L'utilisation de champs libres dans des applications électroniques pour des factures électroniques avec de nouveaux éléments essentiels lors du traitement de factures électroniques et l'ajout de plusieurs données à caractère personnel doivent dès lors être évités car ils ne sont pas compatibles avec l'article 5.1.c) du RGPD.

3. Principe de finalité et publication, à des fins de transparence et de comptabilité, de données à caractère personnel qui ont été collectées dans le cadre de la facturation électronique

13. L'article 8 de la Directive 2014/55/UE contient les dispositions concrètes suivantes :

"1. La présente directive est sans préjudice de la législation de l'Union et la législation nationale applicables en matière de protection des données.
2. Sauf disposition contraire du droit de l'Union ou du droit national, et sans préjudice des exceptions et limitations prévues à l'article 13 de la directive 95/46/CE, les données à caractère personnel obtenues aux fins du traitement de factures électroniques ne peuvent être utilisées qu'à ces fins ou à d'autres fins compatibles avec celles-ci.
3. Sans préjudice des exceptions et limitations prévues à l'article 13 de la directive 95/46/CE, les États membres veillent à ce que, à des fins de transparence et de comptabilité, les conditions de la publication de données à caractère personnel collectées lors du traitement de factures électroniques soient conformes aux finalités de la publication ainsi qu'au principe de protection de la vie privée."

[6] "*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.*".

14. Le projet transpose les points 2 et 3 de l'article 8 susmentionné de la Directive 2014/55/UE dans ses articles 5 (nouvel article 13, § 4 de la loi du 17 juin 2016 *relative aux marchés publics*) et 13 (nouvel article 31, § 4 de la loi du 17 juin 2016 *relative aux contrats de concession*).

> *"§ 4. Les données à caractère personnel obtenues aux fins du traitement de factures ne peuvent être utilisées qu'à ces fins ou à d'autres fins compatibles avec celles-ci. Les conditions de la publication de données à caractère personnel collectées lors du traitement de factures électroniques sont conformes aux finalités de la publication ainsi qu'au principe de protection de la vie privée."*

15. Le fait que la législation déclare que le principe de finalité doit être garanti ne signifie évidemment pas que cela sera également le cas dans la pratique. La disposition selon laquelle la publication est "conforme au principe de protection de la vie privée" est reprise littéralement de la Directive européenne mais n'ajoute pas fondamentalement de réelle garantie. En ce qui concerne surtout la publication de données à caractère personnel liées à la facturation électronique, il n'y a pas d'orientation par le législateur européen et belge, ce qui donnera lieu à une application divergente et à un risque variable pour les personnes physiques concernées.

16. Dans la pratique, il est important, lors de la publication ou d'une autre réutilisation, de prévoir des garanties suffisantes visant à protéger les personnes physiques concernées, comme :

- la pseudonymisation[7] et/ou l'anonymisation des données à caractère personnel ;
- une interdiction de décoder des données à caractère personnel codées ;
- une information suffisante aux personnes concernées quant à leurs droits d'accès, de rectification ou d'opposition si des tiers traitent leurs données à caractère personnel à des fins de marketing direct [NdT : prospection au sens du RGPD] (articles 15, 16 et 21 du RGPD) ;
- une base légale claire et des garanties pour l'établissement de profils de personnes physiques, d'analyses de données ("data mining") qui indiqueraient des corrélations sans garantir l'exactitude, avec de possibles effets (juridiques) que certains groupes de la population ressentent comme inattendus, inappropriés ou non désirés.

17. Le respect des principes du RGPD dépendra dans une large mesure des fonctionnalités du logiciel choisi et de la manière dont il est utilisé.

18. Il ressort de la note adressée au Conseil des ministres que le SPF Stratégie et Appui (ci-après le "SPF BOSA") a développé une interface "*qui permet de transformer en un PDF lisible les factures reçues électroniquement par les institutions qui [ne] disposeraient pas d'un logiciel de comptabilité*

[7] Article 4, 5) et considérant 28 du RGPD.

qui traite des factures électroniques". Dans la mesure où cette interface est appliquée, des garanties techniques doivent également être apportées afin que lors de l'application de la fonctionnalité de lisibilité (automatique), le principe susmentionné de limitation des finalités reste garanti.

4. Approche basée sur les risques en vertu du RGPD et de l'analyse d'impact relative à la protection des données : évaluation des caractéristiques du logiciel utilisé pour le traitement des éléments essentiels des factures électroniques

19. Selon le RGPD[8], les principes de **protection dès la conception** ("privacy by design") et de **protection des données par défaut** ("privacy by default") doivent également être pris en considération dans le cadre d'adjudications publiques.

20. La législation devrait davantage mettre l'accent sur l'exigence du RGPD (ce qu'on appelle "l'approche basée sur les risques"[9]) d'évaluer les risques et les caractéristiques (ir)respectueuses en matière de protection des données du logiciel et des conditions de licence pour les personnes concernées en vertu du RGPD, qui sont propres aux progiciels (types) les plus utilisés pour la facturation, la comptabilité et la fiscalité.

21. Dans une réaction complémentaire du 23 octobre 2018, le demandeur a affirmé ce qui suit : "*tous les logiciels intégrant le traitement de factures entrantes et /ou sortantes sont potentiellement concernés. Nous ne disposons pas d'une liste de ces logiciels. La conformité de ces logiciels avec le RGPD n'a pas fait l'objet d'une vérification*."

22. Sans une analyse d'impact relative à la protection des données (article 35 du RGPD), au cours de laquelle le logiciel et les licences utilisés font l'objet d'un examen approfondi, la référence susmentionnée à une partie des principes du RGPD risque de n'être qu'une façade, et ce étant donné que de nombreuses applications ne respectent pas les principes de base du RGPD, que les déclarations de protection des données de donneurs de licence sont peu transparentes et/ou que les fournisseurs de licence affirment trop rapidement qu'ils travaillent "conformément au RGPD". Un certain nombre de donneurs de licence communiquent des données à caractère personnel à des tiers pour leurs finalités commerciales (lucratives) et/ou pour profiler des personnes physiques sur la base du contenu des communications, profilage parfois présenté comme une "mesure de sécurité". L'utilisation de nombreux progiciels types, licences types et/ou logiciels gratuits pour traiter des données de facture électroniques peut impliquer des risques particuliers ou sans précédent pour l'utilisateur et les fonctionnalités types ne tiendront pas toujours suffisamment compte des obligations des responsables

[8] Considérant 78, *in fine*.
[9] Voir notamment l'article 32.1 du RGPD.

du traitement en vertu du RGPD. Ainsi, des données sont souvent placées dans le cloud dans des pays n'ayant pas un niveau adéquat de protection des données.

23. Une des caractéristiques ne bénéficiant pas encore d'une attention suffisante est le couplage d'API ("Application Programming Interfaces") avec les applications pour la facturation électronique, la comptabilité, ... via lesquelles des données à caractère personnel sont traitées. L'application d'API peut en effet comporter une augmentation des risques (y compris le risque de non-respect de principes pertinents du RGPD comme dans le cadre de l'augmentation du partage des données), ou une diminution des risques pour les droits et libertés des personnes concernées (par ex. le chiffrement, la pseudonymisation, l'agrégation, ...).

24. L'Autorité estime dès lors recommandé qu'au niveau fédéral, un inventaire et une analyse d'impact relative à la protection des données (liste de risques, failles dans le logiciel, ...) soient réalisés périodiquement. Cela peut être effectué au niveau du SPF BOSA avant que les services publics développent leurs principales applications (par ex. FEDCOM[10], ...) pour le traitement à des fins de factures électroniques.

5. Implication du délégué à la protection des données ("DPO") et transparence de son rôle

25. À la lumière de la responsabilité mentionnée à l'article 5.2 du RGPD, l'Autorité estime que le traitement de données à caractère personnel via des factures électroniques doit toujours se baser sur des choix réfléchis des dirigeants au sein des services publics (responsables du traitement).

26. L'Autorité estime qu'il faut accorder plus d'attention au rôle du DPO qui doit être associé au développement d'applications dans ce contexte. D'après l'article 38.1 du RGPD, le DPO du responsable du traitement doit en effet être associé "à toutes les questions relatives à la protection des données à caractère personnel".

27. Cela implique également que le DPO (au besoin soutenu par une équipe technique du SPF BOSA) doit être associé lorsque des choix et des réflexions sont soumis pour décision aux dirigeants au sein des autorités concernées eu égard au traitement de données à caractère personnel provenant de factures électroniques (choix de la plateforme ICT, du logiciel, ...).

28. En l'occurrence, le SPF BOSA a conçu une application disposant d'une fonctionnalité qui augmente potentiellement le risque pour les droits et libertés des personnes concernées (tels que

[10] Le logiciel comptable de l'autorité fédérale qui reçoit et traite les factures. Voir les FAQ (https://spp.yourict.be/ucontent/6369c7c90f504f829dbb221697f3b51c_fr-FR/WORD/index.pdf) et le helpdesk (adresse de contact FEDCOM.Helpdesk@bosa.fgov.be).

visés dans le RGPD) alors qu'après avoir pris des renseignements, il s'avère que le DPO n'a pas été associé à cette conception. Le site Internet du SPF BOSA ne mentionne pas non plus la possibilité de prendre contact avec le DPO, ni les modalités de ce contact, ce qui est contraire aux dispositions des articles 13.1.b), 14.1.b) et 38.4[11] du RGPD.

29. Dans une réaction complémentaire du 23 octobre 2018, le demandeur a toutefois affirmé que le DPO du SPF BOSA sera impliqué dans la réalisation des analyses de risques nécessaires et qu'il en établira un rapport.

30. Le projet peut prévoir des dispositions concrètes dans les lois susmentionnées qui soutiennent le rôle du DPO dans ce sens lors de l'établissement de choix concernant le traitement des éléments essentiels des factures électroniques.

IV. CONCLUSION

31. L'Autorité estime que la simple référence à des éléments de protection des données du RGPD n'a qu'une valeur (symbolique) limitée (point 15).

32. Si le législateur souhaite appliquer le RGPD, il faut miser davantage, dans les lois adaptées, sur la concrétisation d'obligations des responsables du traitement en vertu du RGPD lorsque des éléments essentiels de factures électroniques sont traités. Les actions fondamentales devant intervenir sont :

- établir un inventaire des logiciels couramment utilisés pour le traitement des éléments essentiels avec une liste des risques et des caractéristiques (ir)respectueuses en matière de protection des données de ces logiciels (point 19) ;
- réaliser une évaluation périodique des risques et des caractéristiques des principales applications qui sont utilisées par les services publics (par ex. FEDCOM, ..) au moyen d'une analyse d'impact relative à la protection des données (point 23) ;
- associer le DPO aux choix pertinents en matière de plateformes, logiciels, ... permettant le traitement de ces éléments essentiels et prévoir une meilleure communication quant aux modalités de prise de contact avec le DPO (point 26).

[11] "*Les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le présent règlement.*"

PAR CES MOTIFS,

l'Autorité émet un avis favorable sur les éléments du projet qui ont été abordés, à condition que les éléments mentionnés au point 31 soient respectés.

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

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere