Recommandation n° 01/2019 du 6 février 2019

Objet : l'obligation de créer un compte utilisateur chez Microsoft pour consulter des applications de services publics (CO-AR-2018-004)

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

Vu la loi du 3 décembre 2017 *relative à la loi portant création de l'Autorité de protection des données*, en particulier l'article 23 (ci-après « LCA »);

Vu 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* (ci-après « 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* (ci-après « LTD »);

Vu le rapport de Monsieur Frank Robben ;

Émet d'initiative, le 6 février 2019, la recommandation suivante :

I. OBJET ET PROCÉDURE

1. L'Autorité a reçu des questions et des plaintes relatives à l'obligation de créer un compte chez Microsoft pour consulter des applications de services publics. Ces applications comprennent la consultation de la législation et la connexion à un extranet d'un service public fédéral. Le Secrétariat de l'Autorité a examiné cette problématique, tant d'un point de vue juridique que d'un point de vue technique.

II. CONSIDÉRATION GÉNÉRALE

2. L'Autorité décide dès lors de formuler une recommandation publique à l'égard de tous les services publics qui envisagent de déployer des applications similaires à l'aide de partenariats externes, et ce à la lumière des droits et principes généraux du RGPD.

III. RECOMMANDATIONS

Protection des données dès la conception et protection des données par défaut (article 25 du RGPD)

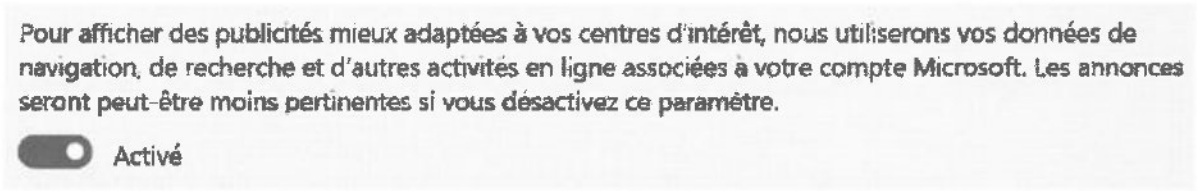
3. Une application proposée par un service public peut ou non impliquer le traitement de données à caractère personnel.

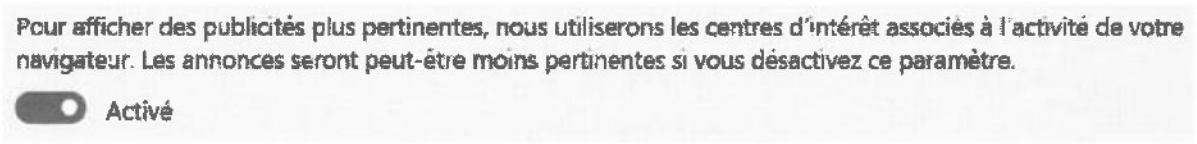
4. Concrètement, l'Autorité a reçu plusieurs questions concernant le fait de lier l'accès à plusieurs applications à l'obligation de créer un compte Microsoft. La création de ce compte Microsoft implique clairement un traitement de données à caractère personnel. Lors de la création de ce compte, des données à caractère personnel telles que l'adresse e-mail, le pays, la date de naissance et le numéro de téléphone doivent en effet être communiquées.

5. Ce traitement de données à caractère personnel implique que l'autorité publique, en tant que responsable du traitement, doit tenir compte des différents principes du RGPD, dont la protection des données dès la conception ("data protection by design") et la protection des données par défaut ("data protection by default").

6. Si l'application proposée concerne uniquement la mise à disposition d'informations publiques qui ne contiennent pas de données à caractère personnel (comme une base de données reprenant la législation), l'exigence de la création d'un compte pour accéder à ces informations, impliquant le traitement de données à caractère personnel, est contraire aux principes de protection des données dès la conception et de protection des données par défaut définis dans le RGPD.

7. L'Autorité a examiné concrètement les questions posées et a constaté que plusieurs applications n'étaient pas proposées conformément à ces principes. En effet, ces applications reconnaissent la politique en matière de protection de la vie privée de Microsoft. Le Privacy Dashboard de Microsoft est donc d'application, dans lequel nous retrouvons les deux paramètres suivants :





8. Ces paramètres standard signifient dès lors que le sous-traitant (dans ce cas Microsoft) utilise par défaut ("by default") des données concernant les habitudes de navigation et de recherche ainsi que d'autres activités en ligne liées au compte Microsoft de l'utilisateur concerné.

Exigence d'un fondement juridique du traitement (article 6 du RGPD)

9. Le fait que plusieurs autorités publiques belges soumettent systématiquement l'accès à des applications à une obligation d'identification soulève encore d'autres questions sur le plan du droit à la protection des données.

10. L'Autorité attire l'attention sur le fait que l'instauration, par des autorités publiques, d'une obligation d'identification à grande échelle pour chaque justiciable exige non seulement une base légale claire (articles 8 de la CEDH et 22 de la Constitution), mais également une "nécessité dans une société démocratique". Cette nécessité n'existe pas pour toutes les applications (par ex. l'accès à la législation ou à de la documentation, l'accès à un service personnalisé, ...).

11. Il ressort de l'article 6 du RGPD que chaque traitement de données à caractère personnel requiert un fondement juridique.

Cas dans lesquels il ne s'agit pas d'un consentement valable de la personne concernée au sens du RGPD

12. Si le responsable du traitement choisit de subordonner l'accès à un service public à l'acceptation des conditions générales d'une plateforme privée d'un sous-traitant (par ex. Microsoft, Facebook, ...), il ne s'agit pas d'un consentement valable au sens de l'article 6 du RGPD.

13. L'Autorité attire également l'attention sur le fait que l'utilisation d'une influence (de formes plus prononcées d'influence) de l'utilisateur peut invalider le consentement. Une des techniques utilisées consiste à **donner l'impression que l'utilisateur a le choix, alors que dans le même temps, il s'agit d'influencer ce choix** afin d'inciter l'utilisateur à choisir l'option peu respectueuse de la vie privée (souvent aussi le paramètre par défaut). Dans la littérature, on parle de donner un "coup de pouce" ("nudge")[1] à l'utilisateur en anticipant ses sensibilités ou sa psychologie par exemple au moyen de la technique de la punition ou de la récompense au moment d'effectuer un choix. La dissimulation de choix respectueux de la vie privée (par ex. la désinscription, ...)[2] aussi a déjà été documentée précédemment.

14. Il n'y a pas de consentement valable en raison d'une forte influence de l'utilisateur si, pour utiliser une application ne fournissant que des informations publiques sans données à caractère personnel, les utilisateurs sont influencés afin d'opter pour une plateforme présentant une obligation d'identification qui est bien plus conviviale ou performante (par ex. en ce qui concerne la fonction de recherche) qu'une autre alternative sans obligation d'identification. En effet, l'utilisateur qui choisit l'alternative respectueuse de la vie privée (par ex. consulter anonymement la législation sans devoir passer par une plateforme commerciale et devoir créer un compte) est "pénalisé" car il ne se voit pas offrir des facilités d'utilisation équivalentes.

Principe de proportionnalité (article 5 du RGPD)

15. Chaque service public s'accompagnant d'un traitement de données à caractère personnel doit tenir compte du principe de proportionnalité et des principes repris aux articles 5 et 25 du RGPD. Les services électroniques d'autorités publiques doivent être disponibles sans traiter plus de données que ce qui est techniquement ou juridiquement nécessaire pour le traitement (par ex. l'utilisation de

[1] Voir les exemples du Norwegian Consumer Council dans *Deceived by design. How tech companies use dark patterns to discourage us from exercising our right to privacy*, 27 juin 2018, publié à l'adresse suivante : https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[2] Pour un exemple de dissimulation d'un choix via webdesign, voir le point 154 de la décision de la CNIL concernant Google, qui peut être consultée via le lien suivant : https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1.

cookies fonctionnels). Chaque service public doit dès lors réaliser une évaluation minutieuse et documentée de la situation dans laquelle s'inscrit son service et évaluer si une identification de la personne concernée est nécessaire.

Pour de nombreux **services publics** (par ex. la consultation de la réglementation ou de la documentation), il n'y a aucune raison concluante de permettre que les utilisateurs soient obligés de communiquer qui ils sont via des techniques (une combinaison de techniques) telles que la création d'un compte et/ou l'utilisation de cookies et la collecte externe de données.

Pour une **version personnalisée d'un service public** non plus (par ex. des pages Internet personnalisées avec votre préférence de langue, votre historique de recherche et vos sources favorites), aucune identification complète (connaissance de l'identité civile) de la personne concernée n'est nécessaire. Se connecter avec un alias ou un compte inidentifiable (enregistré ou non dans un cookie) est souvent suffisant dans ce contexte. Une autre solution peut consister à utiliser le service d'authentification fédéral ("FAS") du SPF BOSA[3] avec un faible niveau d'authentification (voir ci-après).

Pour un nombre limité de cas où il y aurait quand même une nécessité démontrable pour une autorité publique d'imposer à la personne concernée une **obligation d'identification et une obligation d'authentification** (par ex. consulter votre déclaration fiscale via tax on web), il est recommandé que les services publics utilisent le **service d'authentification fédéral ("FAS")** du SPF BOSA ou les moyens d'authentification qui y sont intégrés, plutôt qu'un système de gestion des utilisateurs et des accès n'offrant pas les mêmes garanties en matière de protection des données. L'utilisation du "FAS" permet de maintenir les informations en question sous le contrôle du service public et de réduire considérablement les risques en matière de sécurité et de conformité avec le RGPD (par ex. fusion avec d'autres données et utilisation pour d'autres finalités). En effet, l'utilisation du "FAS" par les autorités publiques permet d'éviter que des données de connexion ou des adresses e-mail doivent être conservées en de très nombreux endroits et qu'un utilisateur doive systématiquement s'inscrire sur une multitude d'applications publiques différentes lorsque l'identification ou l'authentification est nécessaire dans le cadre d'un service public déterminé.

16. Si le responsable du traitement réclame davantage de données que ne le nécessite la fonctionnalité de base, il viole également les principes de minimisation des données et de limitation de la conservation (article 5.1.c) et e) du RGPD).

[3] Voir l'article 9 de la loi du 18 juillet 2017 *relative à l'identification électronique, M.B.* du 9 août 2017.

17. Lors de l'évaluation des principes susmentionnés, il importe également de vérifier si des alternatives équivalentes et un **service de base convivial** sont proposés aux personnes concernées. L'imposition, par une autorité publique (via un tiers), de conditions pour l'accès à la législation telles qu'une obligation d'identification par la création d'un compte et/ou le consentement aux cookies et à la politique des données d'un tiers et l'acceptation des conditions contractuelles imposées d'un tiers ne sont pas conciliables avec les principes repris aux articles 5 et 25 du RGPD. Un responsable du traitement peut difficilement faire référence à une nécessité qui consisterait à choisir une solution technologique déterminée (par ex. l'utilisation de comptes utilisateurs en combinaison avec la plateforme Microsoft Sharepoint) qui n'offre manifestement aucune possibilité pour la fonctionnalité en question de respecter les principes susmentionnés figurant aux articles 5 et 25 du RGPD.

Obligation d'information (articles 13 et 14 du RGPD)

18. Le responsable du traitement ne peut pas se décharger de sa propre obligation d'information en vertu des articles 13 et 14 du RGPD lorsqu'il a recours à une société commerciale pour proposer la fonctionnalité de base.

Association en temps utile du DPO aux projets sans que celui-ci doive attendre des instructions du comité de direction (article 38.1 du RGPD)

19. L'article 38.1 du RGPD oblige le responsable du traitement à associer son DPO "d'une manière appropriée" et "en temps utile" "*à toutes les questions relatives à la protection des données à caractère personnel*". Si, au moment de mettre sur pied ou de modifier une plateforme ICT pour l'accès à un service public, des conditions sont imposées ou des risques peuvent exister pour la personne concernée, le DPO doit donc être associé, en temps utile, sans devoir au préalable passer par le comité de direction. Dans la pratique, il n'apparaît pas toujours clairement que le DPO du service public est associé, en temps utile, aux choix en matière de solutions ICT. Souvent, il est même impossible de savoir quel était le point de vue du comité de direction et quel était l'avis du DPO.

Application de la réglementation sur les "cookies" (article 129 de la LCE[4]) : manière dont l'exigence de consentement a un impact sur le placement de cookies et sur la possibilité de les retirer

[4] Loi du 13 juin 2005 *relative aux communications électroniques*, *M.B.* du 20 juin 2005.

20. Chaque fois que la fonctionnalité de base est proposée en ligne, lors de la phase de la conception du site Internet, il faut consacrer en temps utile une attention à l'application de la réglementation sur les cookies (actuel article 129 de la LCE). Cela implique davantage que le fait de mentionner que des cookies sont enregistrés (article 13 du RGPD) et exige que l'on travaille surtout avec des cookies fonctionnels qui se limitent aux informations strictement techniques[5]. L'obligation d'accepter les cookies a également un impact sur la base juridique du traitement de données à caractère personnel en vertu du RGPD (voir ci-avant).

21. La combinaison d'un enregistrement obligatoire de la personne concernée, de l'acceptation obligatoire des divers cookies (dont l'acceptation obligatoire de third party cookies) et d'une utilisation obligatoire des "cookie settings" (paramètres de cookies) les plus larges est contraire à l'exigence de consentement figurant à l'article 129 de la LCE.

Effectuer une analyse d'impact relative à la protection des données

22. Le RGPD impose au responsable du traitement de tenir compte des risques pour les droits et libertés des personnes concernées, notamment en ce qui concerne la sécurité de la plateforme Internet (article 32 du RGPD). Dans ce cadre, le responsable du traitement doit tenir compte du risque lié à la possibilité, pour son sous-traitant privé, de procéder à une collecte de données, à du data mining (exploration de données) et à de l'enrichissement de données. Cette possibilité combine des facteurs qui augmentent le risque pour les droits et libertés de la personne concernée :

- des (méta)données peuvent être couplées à un même compte utilisateur puisque celles-ci sont traitées via une même plateforme sous-jacente (par ex. une plateforme Sharepoint et un répertoire actif dans le cloud public)
- des données peuvent également être couplées aux différents services que l'utilisateur utilise via ce compte, parfois dans différents contextes (par ex. l'utilisation privée pendant les heures de travail)
- les données traitées par le service public peuvent également avoir trait au profil de la personne concernée (par ex. une inscription obligatoire pour l'enregistrement de mandats d'une personne publique, une recherche de législation sur certaines maladies, ...).

[5] Les informations nécessaires à la communication (sous toutes formes, cookies ou autres, à caractère personnel ou non), depuis l'émetteur jusqu'au destinataire qui sont ensuite effacées sans avoir été à proprement parler traitées pour d'autres fins ne posent aucun problème. Voir la Commission de la protection de la vie privée, prédécesseur en droit de l'Autorité, recommandation d'initiative n° 01/2015 du 4 février 2015 *concernant l'utilisation des cookies*, publiée à l'adresse suivante : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2015_0.pdf.

23. Pour un certain nombre de projets, il sera également recommandé d'effectuer une analyse d'impact relative à la protection des données, en raison de la combinaison de ces facteurs (article 35 du RGPD[6]).

Recommandations

Vu ce qui précède, l'Autorité formule les recommandations suivantes :

En tant que responsable du traitement, l'autorité publique doit toujours garantir que l'accès à une application n'est pas subordonné à la divulgation de ses données à caractère personnel lorsque cette application met à disposition uniquement des informations publiques et pas des données à caractère personnel.

Concrètement, l'imposition, par des autorités publiques, de l'utilisation d'un compte Microsoft pour accéder à une application qui ne met à disposition que des informations publiques et pas des données à caractère personnel est contraire au RGPD.

Lorsqu'une autorité publique propose une application qui traite des données à caractère personnel, ce traitement doit se baser sur un fondement juridique repris à l'article 6 du RGPD. Obliger la personne concernée à créer un compte auprès d'un sous-traitant et à accepter la politique en matière de protection de la vie privée de ce sous-traitant invalide le consentement en tant que fondement juridique du traitement. C'est également le cas si l'on utilise des techniques pour influencer le libre choix de l'utilisateur en ce qui concerne la protection de ses données ou pour compliquer les choix.

Les services publics doivent toujours garantir le libre accès aux sources officielles de législation, et ce sans y associer la moindre condition qui constitue une ingérence dans la vie privée et/ou implique des risques pour les droits et libertés des personnes concernées, que ce soit ou non en reprenant tacitement les conditions ou le modèle d'utilisation d'un tiers. De tels services doivent offrir une totale convivialité et la fonctionnalité (de base) dans son intégralité et être faciles à trouver par rapport aux services qui sont eux proposés avec des conditions, par exemple pour personnaliser l'accès aux informations. Dans ce cadre, il est exclu d'utiliser des techniques d'influence qui rendent impossible, plus difficile ou moins intéressant le choix de l'alternative plus respectueuse de la vie privée, privant ainsi la personne concernée d'un choix équivalent.

[6] Combinaison des critères de "traitement à grande échelle", utilisation de nouvelles technologies.

Les DPO de services publics doivent (de préférence en groupe) être associés au traitement de données à caractère personnel de citoyens ou de membres du personnel des services publics via les systèmes de sous-traitants privés qui interviennent dans les applications les plus courantes (par ex. des systèmes d'exploitation, des logiciels bureautiques, des plateformes et des extranets sur lesquels il est possible de consulter des documents ou de la législation, des fournisseurs de médias sociaux, ...).

En tant que responsable du traitement, l'autorité publique doit réfléchir soigneusement aux choix qui sont faits ou aux possibilités qui sont laissées à des entreprises privées auxquelles il est fait appel (parfois inconsciemment) en tant que sous-traitant (par ex. l'utilisation des boutons de médias sociaux sur des sites Internet, l'utilisation de systèmes d'exploitation et de moteurs de recherche, le stockage de données par Microsoft via ses plateformes Sharepoint ou le cloud public). Cela vaut aussi pour le fournisseur d'un service public (par ex. une plateforme pour consulter la législation, ...).

Des choix qui constituent un risque (élevé) pour les droits et libertés des personnes concernées ne peuvent pas être délégués à des sous-traitants, comme le choix de travailler avec l'acceptation obligatoire des conditions générales du tiers par la personne concernée, la détermination des cas d'identification de la personne concernée, l'application ou non de l'enrichissement de données et du data mining (exploration de données) via des plateformes propres et l'offre ou non d'une convivialité à la personne concernée en fonction du choix effectué. La réalisation d'un examen de l'impact de certains choix sur les droits et libertés des personnes concernées ne peut pas non plus être totalement confiée au tiers.

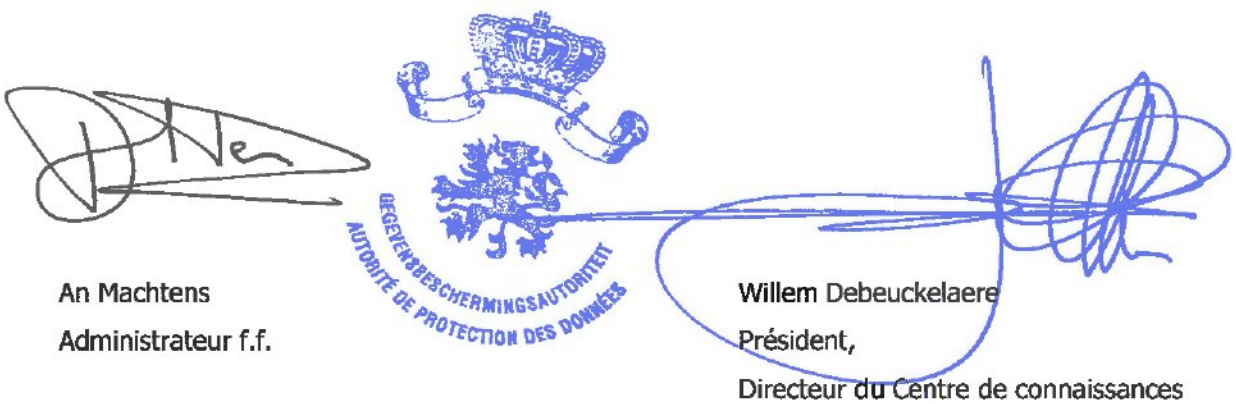
Pour une version personnalisée d'un service public non plus (par ex. des pages Internet personnalisées avec votre préférence de langue, votre historique de recherche et vos sources favorites), aucune identification complète (connaissance de l'identité civile) de la personne concernée n'est nécessaire. Se connecter avec un alias (enregistré ou non dans un cookie) est souvent suffisant dans ce contexte. Une autre solution peut consister à utiliser le service d'authentification fédéral ("FAS") du SPF BOSA[7] avec un faible niveau d'authentification.

Pour un nombre limité de cas où il y aurait quand même une nécessité démontrable pour une autorité publique d'imposer à la personne concernée une obligation d'identification et une obligation d'authentification (par ex. consulter votre déclaration fiscale via tax on web), il est recommandé que les services publics utilisent le service d'authentification fédéral ("FAS") du SPF BOSA ou les moyens d'authentification qui y sont intégrés, plutôt qu'un système de gestion des utilisateurs et des accès n'offrant pas les mêmes garanties en matière de protection des données.

---

[7] Voir l'article 9 de la loi du 18 juillet 2017 *relative à l'identification électronique, M.B.* du 9 août 2017.

Cette recommandation s'applique sans préjudice des moyens que l'Autorité peut mettre en place si une autorité publique déterminée et/ou un sous-traitant persiste(nt) à ne pas respecter le RGPD.



An Machtens
Administrateur f.f.

Willem Debeuckelaere
Président,
Directeur du Centre de connaissances