Aanbeveling nr. 01/2019 van 6 februari 2019

Betreft: het opleggen van de verplichte aanmaak van een gebruikersaccount bij Microsoft voor het raadplegen van toepassingen van overheidsdiensten (CO-AR-2018-004)

De Gegevensbeschermingsautoriteit (hierna de Autoriteit);

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, inzonderheid artikel 23 (hierna "WOG");

Gelet op de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Gelet op het verslag van de heer Frank Robben;

Brengt op 6 februari 2019 uit eigen beweging de volgende aanbeveling uit:

I. VOORWERP EN PROCEDURE

1. De Autoriteit werd gevat door vragen en klachten aangaande het opleggen van de verplichte aanmaak van een account bij Microsoft voor het raadplegen van toepassingen van overheidsdiensten. Deze toepassingen omvatten het raadplegen van wetgeving en het inloggen op een extranet van een Federale Overheidsdienst. Het secretariaat van de Autoriteit onderzocht dit zowel vanuit juridisch als technisch oogpunt.

II. ALGEMENE BESCHOUWING

2. De Autoriteit beslist derhalve om een publieke aanbeveling te formuleren ten aanzien van alle overheidsdiensten die overwegen om met behulp van externe partnerships gelijkaardige toepassingen uit te rollen. Dit in het licht van de algemene beginselen van en de rechten voorzien in de AVG.

III. AANBEVELINGEN

Gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen (artikel 25 AVG)

3. Een toepassing aangeboden door een overheidsdienst kan al dan niet de verwerking van persoonsgegevens inhouden.

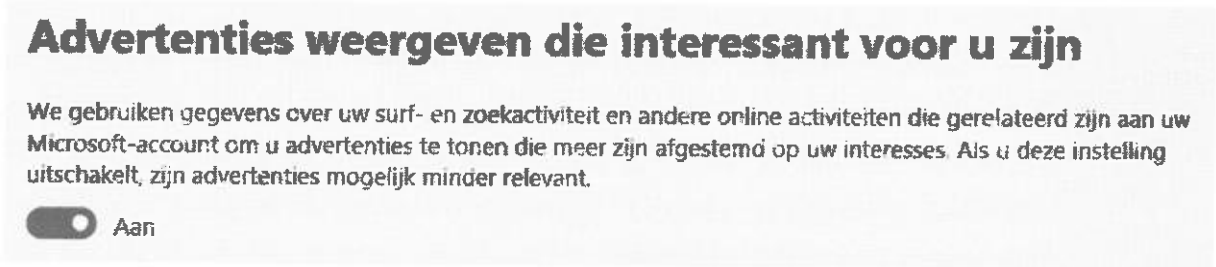
4. De Autoriteit werd concreet gevat door diverse vragen waarbij de toegang tot verschillende toepassingen gekoppeld wordt aan de vraag (plicht) om een Microsoft-account te creëren. De creatie van deze Microsoft-account houdt duidelijk een verwerking van persoonsgegevens in. Bij de creatie van deze account dienen namelijk persoonsgegevens zoals emailadres, land, geboortedatum en telefoonnummer te worden verstrekt.

5. Deze verwerking van persoonsgegevens impliceert dat de overheid als verwerkingsverantwoordelijke rekening dient te houden met de diverse beginselen van de AVG, waaronder gegevensbescherming door ontwerp ("data protection by design") en gegevensbescherming door standaardinstellingen ("data protection by default").

6. Indien de aangeboden toepassing enkel betrekking heeft op de ontsluiting van openbare informatie, die geen persoonsgegevens bevat (zoals een gegevensbank met wetgeving), is het vereisen van het aanmaken van een account om toegang te hebben tot deze informatie en waarbij persoonsgegevens worden verwerkt, in strijd met de beginselen van gegevensbescherming door

ontwerp en door standaardinstellingen vastgelegd in de AVG.

7. De Autoriteit onderzocht in concreto de gestelde vragen en stelde vast dat verschillende toepassingen niet conform deze beginselen worden aangeboden. Immers, deze toepassingen erkennen het privacybeleid van Microsoft. Het privacydashboard van Microsoft is derhalve van toepassing, waar we volgende twee instellingen terugvinden.



8. Deze standaardinstellingen betekenen dan ook dat de verwerker (in dit geval Microsoft) standaard ("by default") gegevens over de surf- en zoekactiviteit en andere online activiteiten die gerelateerd zijn aan het Microsoft-account van de betrokken gebruiker gebruikt.

Vereiste van rechtsgrond voor de verwerking (artikel 6 AVG)

9. Het feit dat verschillende Belgische overheden de toegang tot toepassingen systematisch onderwerpen aan een identificatieplicht roept nog andere vragen op op het vlak van het gegevensbeschermingsrecht.

10. De Autoriteit vestigt de aandacht op het feit dat het invoeren door overheden van een grootschalige identificatieplicht voor elke rechtszoekende niet alleen een duidelijke wettelijke basis vergt (artikelen 8 EVRM en 22 Grondwet), maar ook een "noodzaak in een democratische samenleving". Deze noodzaak is niet aanwezig voor alle toepassingen (bv. toegang tot wetgeving of documentatie, toegang tot een gepersonaliseerde dienst,...).

11. Uit artikel 6 AVG volgt dat elke verwerking van persoonsgegevens een rechtsgrond vereist.

Gevallen waar geen sprake is van een geldige toestemming van de betrokkene in de zin van de AVG

12. Indien de verwerkingsverantwoordelijke ervoor kiest om de toegang tot een overheidsdienst afhankelijk te maken van het aanvaarden van de standaardvoorwaarden van een privaat platform van een verwerker (bv. Microsoft, Facebook,...), is er geen sprake van een geldige toestemming in de zin van artikel 6 AVG.

13. De Autoriteit wijst er ook op dat het gebruik van (meer uitgesproken vormen van) beïnvloeding van de gebruiker de toestemming kan ongeldig maken. Een van de gebruikte technieken is het **wekken van de indruk dat de gebruiker een keuze krijgt, terwijl tegelijk sprake is van beïnvloeding van deze keuze van gebruikers**, teneinde de gebruiker de privacyonvriendelijke optie (vaak ook de standaardinstelling) te laten kiezen. In de literatuur spreekt men over het geven van een "duwtje" ("nudge")[1] aan de gebruiker waarbij men inspeelt op zijn gevoeligheden of psychologie door bijvoorbeeld de techniek van straf of beloning te gebruiken bij het maken van keuzes. Ook het verbergen van privacyvriendelijke keuzes (bv. uitschrijven...)[2] is reeds eerder gedocumenteerd.

14. Er is geen geldige toestemming wegens sterke beïnvloeding van de gebruiker indien gebruikers voor het gebruik van een toepassing waarbij enkel openbare informatie zonder persoonsgegevens worden verstrekt, worden beïnvloed om te kiezen voor een platform met identificatieplicht dat veel gebruiksvriendelijker of performanter (bv. qua opzoekingsfunctie) is dan een andere optie zonder identificatieplicht. De gebruiker die immers kiest voor het privacyvriendelijke alternatief (bv. anoniem de wetgeving raadplegen zonder te moeten passeren langs een commercieel platform en het aanmaken van een account) wordt "bestraft" omdat hij geen gelijkwaardig gebruiksgemak aangeboden krijgt.

Proportionaliteitsbeginsel (artikel 5 AVG)

15. Elke overheidsdienst die gepaard gaat met een verwerking van persoonsgegevens dient rekening te houden met het proportionaliteitsbeginsel en de beginselen in de artikelen 5 en 25 AVG. Elektronische diensten van overheden moeten beschikbaar zijn zonder dat er meer wordt verwerkt dan wat technisch of juridisch noodzakelijk is voor de verwerking (bv. gebruik van functionele cookies).

---

[1] Zie de voorbeelden in Norwegian Consumer Council, *Deceived by design. How tech companies use dark patterns to discourage us from exercising our right to privacy*, 27 June 2018, published on https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[2] Zie voor een voorbeeld van het verbergen van een keuze via webdesign : punt 154 van de beslissing van CNIL betreffende google, raadpleegbaar op https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1.

Elke overheidsdienst moet daarom een zorgvuldige en gedocumenteerde afweging maken in welke situatie haar dienstverlening kadert en of identificatie van de betrokkene noodzakelijk is.

Voor veel **overheidsdiensten** (bv. het raadplegen van regelgeving of documentatie) is er geen enkele afdoende reden om toe te laten dat de gebruikers worden verplicht om mee te delen wie hij/zij is via (een combinatie van) technieken zoals het aanmaken van een account en/of gebruik van cookies en externe datacollectie.

Ook voor een **gepersonaliseerde versie van een overheidsdienst** (bv. gepersonaliseerde webpagina's met je taalvoorkeur, je zoekhistoriek en je favoriete bronnen) is geen volwaardige identificatie (kennis van de burgerlijke identiteit) van de betrokkene nodig. Het inloggen met een alias zonder bijkomende datacollectie via cookies of andere technieken zoals externe dataopslag en dataverrijking bij de verwerker is hierbij vaak voldoende. Een andere oplossing kan erin bestaan om gebruik te maken van de federale authenticatiedienst ("FAS") van de FOD BOSA[3] met een laag authenticatieniveau (zie hieronder).

Voor een beperkt aantal gevallen waar er toch een aantoonbare noodzaak zou bestaan voor een overheid om de betrokkene een **identificatieplicht en authenticatieplicht** op te leggen (bv. raadplegen van je belastingaangifte via tax on web) verdient het aanbeveling dat overheidsdiensten de **federale authenticatiedienst ("FAS")** van de FOD BOSA gebruiken of de daarin geïntegreerde authenticatiemiddelen, eerder dan een systeem van gebruikers- en toegangsbeheer waarbij niet dezelfde waarborgen inzake gegevensbescherming zijn ingebouwd. Bij gebruik van de "FAS" blijft de betreffende informatie onder de controle van de overheidsdienst en worden de beveiligingsrisico's en AVG compliance risico's (bv. vermenging met andere data en gebruik voor andere doeleinden) aanzienlijk gereduceerd. Immers, als overheden de "FAS" gebruiken, vermijdt men dat aanloggegevens of mailadressen op tal van plaatsen moeten worden bewaard, en dat een gebruiker zich, wanneer identificatie en authenticatie in het kader van een bepaalde overheidsdienst nodig zijn, telkens moet inschrijven op tal van verschillende overheidstoepassingen.

16. Indien de verwerkingsverantwoordelijke meer gegevens opvraagt dan nodig voor de basisfunctionaliteit, dan schendt hij ook de beginselen van minimale gegevensverwerking en opslagbeperking (artikel 5 .1 c) en e) AVG).

17. Bij het beoordelen van de voormelde beginselen is het ook van belang om na te gaan of aan de betrokkenen gelijkwaardige alternatieven en een **gebruiksvriendelijke basisdienst** worden aangeboden. Het opleggen door een overheid (via een derde partij) van voorwaarden voor de toegang

[3] Zie artikel 9 van de wet van 18 juli 2017 *inzake elektronische identificatie, B.S.*, 9 augustus 2017.

tot de wetgeving zoals een identificatieplicht via de aanmaak van een account en/of het toestemmen met de cookies en het databeleid van een derde partij, en het aanvaarden van de opgelegde contractuele voorwaarden van een derde partij zijn niet verzoenbaar met de beginselen in de artikelen 5 en 25 AVG. Een verwerkingsverantwoordelijke kan bezwaarlijk verwijzen naar een noodzaak die zou bestaan in de keuze voor een bepaalde technologische oplossing (bv. het gebruik van user accounts in combinatie met het Microsoft Sharepoint platform) die voor de bewuste functionaliteit blijkbaar geen mogelijkheid biedt om de voormelde beginselen in de artikelen 5 en 25 AVG te respecteren.

De informatieplicht (artikelen 13 en 14 AVG)

18. De verwerkingsverantwoordelijke kan zich niet ontslaan van zijn eigen informatieplicht onder artikelen 13 en 14 AVG wanneer hij een beroep doet op een commerciële onderneming voor het aanbieden van de basisfunctionaliteit.

Het tijdig betrekken van de DPO bij de projecten zonder dat deze moet wachten op instructies van het directiecomité (artikel 38.1 AVG)

19. Artikel 38.1 AVG verplicht de verwerkingsverantwoordelijke om haar DPO "naar behoren" en "tijdig" te betrekken "*bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens*". Als er bij het opzetten of wijzigen van een ICT platform voor de toegang tot een overheidsdienst voorwaarden worden opgelegd of risico's kunnen aanwezig zijn voor de betrokkene moet dus de DPO tijdig worden betrokken, zonder dat deze eerst moet passeren langs het directiecomité. In de praktijk blijkt het niet altijd duidelijk dat bij keuzes qua ICT oplossingen de DPO van de overheidsdienst tijdig wordt betrokken. Vaak is ook niet te achterhalen wat het standpunt was van het directiecomité, en wat het advies was van de DPO.

Toepassing van de reglementering op de "cookies" (artikel 129 WEC[4]) : hoe de toestemmingsvereiste een impact heeft op het plaatsen van cookies en de intrekbaarheid ervan

20. Bij elk online aanbieden van de basisfunctionaliteit moet in de fase van het webdesign tijdig aandacht worden besteed aan de toepassing van de reglementering op de cookies (actueel artikel 129 WEC). Dit houdt meer in dan het vermelden dat er cookies worden opgeslagen (artikel 13 AVG), en impliceert dat vooral wordt gewerkt met functionele cookies die zich beperken tot de strikt technische

[4] Wet van 13 juni 2005 betreffende de elektronische communicatie, B.S., 20 juni 2005.

informatie[5]. Het verplichten tot het aanvaarden van cookies heeft ook een impact op de rechtsgrond van de verwerking van persoonsgegevens onder de AVG (zie hiervoor).

21. De combinatie van een verplichte registratie van de betrokkene, de verplichte acceptatie van de diverse cookies (waaronder verplichte aanvaarding van third party cookies) en een verplicht gebruik van de ruimste "cookie settings" gaat in tegen de toestemmingsvereiste onder artikel 129 WEC.

Het verrichten van een gegevensbeschermingseffectenbeoordeling

22. De AVG legt de verwerkingsverantwoordelijke op om rekening te houden met de risico's voor de rechten en vrijheden van de betrokkenen, o.m. wat de beveiliging van het webplatform betreft (artikel 32 AVG). De verwerkingsverantwoordelijke dient hierbij oog te hebben voor het risico gekoppeld aan de mogelijkheid voor haar private verwerker om over te gaan tot datacollectie, data mining en dataverrijking. Deze mogelijkheid combineert factoren die het risico voor de rechten en vrijheden van de betrokkene verhogen :

- (Meta)data kan worden gekoppeld aan eenzelfde gebruikersaccount vermits dit via eenzelfde achterliggend platform wordt verwerkt (bv. sharepoint platform en active directory in de public cloud)
- Data kan ook worden gekoppeld aan de diverse diensten die de gebruiker via deze account gebruikt , soms in verschillende contexten (bv. privaat gebruik tijdens de werkuren)
- De data die de overheidsdienst verwerkt kan ook betrekking hebben op het profiel van de betrokkene (bv. verplichte aanmelding voor registratie van mandaten van een publiek persoon, opzoeking van wetgeving over bepaalde ziektes,...).

23. Voor een aantal projecten zal het door de combinatie van deze factoren ook aangewezen zijn een gegevensbeschermingseffectenbeoordeling te verrichten (artikel 35 AVG[6]).

Aanbevelingen

Gelet op het voorgaande, doet de Autoriteit volgende aanbevelingen:

De overheid dient als verwerkingsverantwoordelijke steeds te waarborgen dat de toegang tot een toepassing niet afhankelijk wordt gesteld van het prijsgeven van zijn persoonsgegevens wanneer deze toepassing enkel openbare informatie, en geen persoonsgegevens ontsluit.

---

[5] De informatie die noodzakelijk is voor de communicatie (in al zijn vormen, cookies of andere, persoonlijk of niet), vanaf de verzender tot aan de ontvanger die vervolgens wordt gewist zonder eigenlijk echt verwerkt te zijn voor andere doeleinden, veroorzaakt geen enkel probleem. Zie Commissie voor de bescherming van de persoonlijke levenssfeer, rechtsvoorganger van de Autoriteit , aanbeveling uit eigen beweging n° 01/2015 van 4 februari 2015 *over het gebruik van cookies*, gepubliceerd op https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_01_2015.pdf.

[6] Combinatie van de criteria van "grootschalige verwerking", gebruik van nieuwe technologieën.

Concreet is het verplicht maken door overheden van het gebruik van een Microsoft-account om toegang te krijgen tot een toepassing die enkel openbare informatie, en geen persoonsgegevens ontsluit, in strijd met de AVG.

Bij het aanbieden, door de overheid, van een toepassing waarbij persoonsgegevens worden verwerkt, dient deze verwerking gebaseerd te zijn op een rechtsgrond onder artikel 6 AVG. Het verplichten van de betrokkene om een account bij een verwerker aan te maken en het privacybeleid van deze verwerker te aanvaarden maakt de toestemming ongeldig als rechtsgrond van de verwerking. Dit is eveneens het geval als technieken worden gebruikt om de vrije keuze van de gebruiker wat de bescherming van zijn gegevens betreft te beïnvloeden of keuzes te bemoeilijken.

Overheidsdiensten dienen steeds de vrije toegang tot de officiële bronnen van wetgeving te waarborgen. Dit zonder enige voorwaarden hieraan te koppelen die inmengingen in de persoonlijke levenssfeer uitmaken en/of onnodige risico's inhouden voor de rechten en vrijheden van de betrokkenen, al dan niet door de voorwaarden of het gebruiksmodel van een derde partij stilzwijgend over te nemen. Dergelijke diensten moeten de volle gebruiksvriendelijkheid en (basis)functionaliteit bieden en makkelijk te vinden zijn ten opzichte van de diensten die wel met voorwaarden worden aangeboden, bijvoorbeeld om de toegang tot de informatie te personaliseren. Hierbij mag geen sprake zijn van het gebruik van beïnvloedende technieken die de keuze voor het meer privacyvriendelijke alternatief onmogelijk, moeilijker of minder interessant maken waardoor de betrokkene geen gelijkwaardige keuze krijgt aangeboden.

De DPO's van overheidsdiensten dienen (bij voorkeur in groep) te worden betrokken bij het verwerken van persoonsgegevens van burgers of overheidspersoneel via de systemen van private verwerkers die betrokken zijn bij de meest gangbare toepassingen (bv. besturingssystemen, kantoorsoftware, platformen en extranetten waarop documenten of wetgeving kunnen worden geconsulteerd, social media aanbieders,...)

De overheid dient als verwerkingsverantwoordelijke zorgvuldig te overwegen welke keuzes worden gemaakt of welke mogelijkheden worden overgelaten aan private ondernemingen waarop (soms onbewust) beroep wordt gedaan als verwerker (bv. gebruik van social media knoppen op websites, gebruik van besturingssytemen en zoekrobotten, dataopslag door Microsoft via haar sharepoint platformen of public cloud). Dit geldt ook bij het aanbieden van een overheidsdienst (bv. platform om wetgeving te raadplegen,...).

Keuzes die een (hoog) risico vormen voor de rechten en vrijheden van de betrokkenen kunnen niet worden overgelaten aan verwerkers, zoals de keuze om te werken met de verplichte aanvaarding van de algemene voorwaarden van de derde partij door de betrokkene, het bepalen van de gevallen van identificatie van de betrokkene, het al dan niet toepassen van dataverrijking en data mining via eigen platformen, en het al dan niet aanbieden van gebruiksvriendelijkheid aan de betrokkene naargelang de gemaakte keuze. Ook het verrichten van een onderzoek naar de impact van bepaalde keuzes op de rechten en vrijheden van de betrokkenen kan niet volledig worden overgelaten aan de derde partij.

Ook voor een gepersonaliseerde versie van een overheidsdienst (bv. gepersonaliseerde webpagina's met je taalvoorkeur, je zoekhistoriek en je favoriete bronnen) is geen volwaardige identificatie (kennis van de burgerlijke identiteit) van de betrokkene nodig. Het inloggen met een alias zonder bijkomende datacollectie via cookies of andere technieken zoals externe dataopslag en dataverrijking bij de verwerker is hierbij vaak voldoende. Een andere oplossing kan erin bestaan om gebruik te maken van de federale authenticatiedienst ("FAS") van de FOD BOSA[7] met een laag authenticatieniveau.

Voor een beperkt aantal gevallen waar er toch een aantoonbare noodzaak zou bestaan voor een overheid om de betrokkene een identificatieplicht en authenticatieplicht op te leggen (bv. raadplegen van je belastingaangifte via tax on web) verdient het aanbeveling dat overheidsdiensten de federale authenticatiedienst ("FAS") van de FOD BOSA[8] gebruiken of de daarin geïntegreerde authenticatiemiddelen, eerder dan een systeem van gebruikers- en toegangsbeheer waarbij niet dezelfde waarborgen inzake gegevensbescherming zijn ingebouwd.

Deze aanbeveling geldt onverminderd de middelen die de Autoriteit kan inzetten in geval van het verder aanhouden van de niet naleving van de AVG door een bepaalde overheid en/of verwerker.

GEGEVENSBESCHERMINGSAUTORITEIT
AUTORITÉ DE PROTECTION DES DONNÉES

An Machtens
Wnd. Administrateur

Willem Debeuckelaere
Voorzitter,
Directeur Kenniscentrum

[7] Zie artikel 9 van de wet van 18 juli 2017 *inzake elektronische identificatie, B.S.*, 9 augustus 2017.

[8] Zie artikel 9 van de wet van 18 juli 2017 *inzake elektronische identificatie, B.S.*, 9 augustus 2017.