Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr 60/2025 van 29 juli 2025

Betreft: Advies m.b.t. Koninklijk besluit tot wijziging van het koninklijk besluit van 31 augustus 2014 betreffende de uitvoering, wat de elektronische handtekening betreft, van artikel I.14,11°, van het Wetboek van economisch recht (CO-A-2025-048)

Trefwoorden: digitaal certificaat die ondersteund en ter beschikking gesteld wordt – multifactor authenticatie die enkel ondersteund wordt – loggegevens – artikel 80/1, §3 WER - artikel 80/2 WER

Originele versie

De Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna: de Autoriteit);

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit,* inzonderheid op artikelen 23 en 26 (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 verzoek om advies van de heer David Clarinval, vice-eersteminister en minister van Werk, Economie en Landbouw (hierna: de aanvrager) ontvangen op 15/05/2025;

Brengt op 29 juli 2025 het volgend advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

1. Op 15 mei 2025 verzocht de aanvrager het advies van de Autoriteit met betrekking tot een Koninklijk besluit tot wijziging van het koninklijk besluit van 31 augustus 2014 betreffende de uitvoering, wat de elektronische handtekening betreft, van artikel I.14,11°, van het Wetboek van economisch recht (hierna: Ontwerp).

2. Het voorliggend Ontwerp heeft in het bijzonder betrekking op de mogelijkheden om, krachtens artikel I.14,11°, van het Wetboek van economisch recht (hierna: WER), een elektronische handtekening te plaatsen m.h.o. het op juridisch geldige en elektronische wijze octrooidocumenten in te dienen bij de Dienst voor de Intellectuele Eigendom.

II. ONDERZOEK TEN GRONDE

3. Terzake voorziet ontworpen artikel 1, naast de bestaande mogelijkheid om een elektronische handtekening uit te voeren met een elektrische chipkaart krachtens artikel I.14,11° WER, in twee aanvullende mechanismes, zodat volgende opties gangbaar worden voor de elektronische handtekening, zijnde:
    - de huidige bestaande mogelijkheid om elektronisch te handtekenen door middel van een chipkaart;
    - Een nieuwe mogelijkheid om te ondertekenen met een digitaal certificaat;
    - Een nieuwe mogelijkheid om te ondertekenen met multifactor authenticatie.

4. De bepaling in kwestie hanteert een uiteenlopende formulering voor de twee nieuwe opties: enerzijds een digitaal certificaat dat ondersteund en ter beschikking gesteld wordt, anderzijds een multifcator authenticatie die enkel ondersteund wordt. De aanvrager gaf hierover de volgende toelichting:

> "*In punt 2° gaat het om een digitaal certificaat, terwijl het in punt 3° gaat om een multifactor authenticatie methode. Een digitaal certificaat moet niet alleen technisch ondersteund worden door de FOD Economie (er bestaan immers verschillende soorten digitale certificaten, die eigen technische specificaties hebben), het wordt ook ter beschikking gesteld via de FOD Economie nadat geverifieerd werd of de betrokken persoon toegang mag hebben tot het octrooi-indieningsplatform (omdat hij octrooigemachtigde is) .*
>
> *In punt 3 gaat het om een multifactor authenticatie methode. Ook hier bestaan verschillende soorten multifactor authenticatiemethoden, die allen eigen technische specificaties hebben. Deze kunnen in de praktijk, gelet op de veelheid aan mogelijke systemen, niet allen technisch ondersteund worden.*"

Uit de toelichting van de aanvrager vermoedt de Autoriteit dat wat betreft de multifactor authenticatie methode, er gebruik gemaakt zal worden van een systeem van een derde (bijv. Microsoft) waardoor deze niet technisch ondersteund kunnen worden, in tegenstelling tot een

eigen ontwikkelde applicatie. De regelgever wordt verzocht om de formulering aan te passen, indien het toch de bedoeling zou zijn om eigen authenticatie-applicaties te gebruiken.

5. Voorts wordt opgemerkt dat er in het aanvraagformulier uitdrukkelijk gestipuleerd wordt dat: "*in het kader van de multifactor authenticatiemethode (Google Authenticator, Microsoft Authenticator en FreeOTP) worden mogelijks verschillende gegevens (login, password, gsmnr) verzameld teneinde de authenticatie, en derhalve een voldoende niveau van zekerheid over de identiteit en van beveliging te kunnen garanderen.*
Tevens moet er op gewezen worden dat overeenkomstig de artikelen XI.80/1 en XI.80/2 WER aan de Dienst voor de Intellectuele Eigendom een ruime wettelijke basis wordt voorzien voor het verwerken van gegevens die verstrekt worden in het kader van de aan hem toevertrouwde opdrachten van algemeen belang betreffende de intellectuele eigendom."

6. Hoewel het Ontwerp zelf enkel vermelding maakt van de nieuwe opties voor elektronische handtekening, stelt de Autoriteit vast op basis van het aanvraagformulier, zoals hierboven weergeven, dat in dit kader een verwerking en bewaring van persoonsgegevens zou plaatsvinden. Dienaangaande werd de aanvrager verzocht verdere duiding te geven over de specifieke regelgevende norm die hiervoor de basis vormde.

> *"Er worden geen andere gegevens verzameld. Voorts kan vermeld worden dat artikel XI.80/2 Wetboek van Economisch Recht het volgende bepaalt […]."*

Na analyse van de door de aanvrager aangehaalde bepaling stelt de Autoriteit vast dat artikel XI.80/2 WER weliswaar de doeleinden aangeeft waarvoor persoonsgegevens verwerkt mogen worden, maar geen melding maakt van de categorieën gegevens die voor die verwerking in aanmerking komen. Dat laatste kan gevonden worden in artikel 80/1 WER. Terzake wordt vastgesteld dat er geen vermelding gemaakt wordt van loggegevens, hetgeen redelijkerwijs overeenstemt met login en passwoord. Zodoende wordt de aanvrager verzocht de nodige maatregelen te nemen om hieraan te remediëren, in acht genomen dat de categorieën gegevens een essentieel onderdeel vormt voor de adequate invulling van het legaliteits-, transparantiebeginsel en het principe van minimale gegevensverwerking. Wat het gsm-nummer betreft wordt verwezen naar randnr. 8.

7. De Autoriteit bevroeg de aanvrager of er alternatieve systemen in aanmerking komen voor de authenticatiemethode. Desgevallend werd specificering gevraagd.

> *"We willen graag verduidelijken dat de multifactorauthenticatiemethoden geen toegang hebben tot login of wachtwoord, en dit ook niet opslaan. Een nuance die moet aangebracht worden, is dat bij het activeren van FreeOTP er weliswaar een GSM nummer wordt ingegeven, maar dat de authenticatiemethode dat GSM nummer niet kan linken aan een bepaalde persoon, of andere persoonsgegevens."*

In aanmerking genomen dat de aanvrager geen andere systemen dan Google Authenticator, Microsoft Authenticator en FreeOTP vermeld, gaat de Autoriteit ervan uit dat er geen andere

authenticatiesystemen in aanmerking komen. Het verdient de aanbeveling om dit in het verslag aan de Koning op te nemen.

8. Het gebruik van het gsm-nummer werd eerder aangehaald in randnrs. 5 en 6. In dit verband lijkt het pertinent om de aanvrager eraan te herinneren dat omwille van het risico van onderschepping en misbruik, het gebruik van gsm-nummers en sms-berichten als authenticatiemethode, niet langer als state-of-the-art beschouwd wordt. In het licht hiervan wordt de aanvrager aanbevolen om het actief gebruik van gsm-nummer en sms-authenticatie als tweede authenticatiemethode, te vermijden en dit uitsluitend als laatste optie aan te wenden, indien werkelijk geen andere methode kan worden ingezet.

9. Voorts wordt opgemerkt dat het gebruik van een gsm-nummer, niet vanzelfsprekend onder contactgegevens lijkt te ressorteren, aangezien de aanvrager uitdrukkelijk aangeeft dat het telefoonnummer enkel ter activatie van FreeOTP dient en niet aangewend wordt om een persoon te identificeren of te linken aan persoonsgegevens. Zodoende lijkt het essentieel om bij voorkeur in de basiswet (WER) en minstens in het Ontwerp duidelijk te omschrijven waarvoor het gsm-nummer dient. Er moet hierbij aangegeven worden dat het niet gebruikt wordt binnen de multifactor authenticatiestap zelf en dat er geen identificatie gebeurt op basis van het gsm-nummer binnen de authenticatiemethode.

10. Er werd aan de aanvrager expliciet gevraagd of, naast de opgesomde gegevens, nog andere gegevens worden bijgehouden.

> *"Door de genoemde authenticatiemethodes (Google Authenticator, Microsoft Authenticator en FreeOTP) worden geen (andere) gegevens bijgehouden"*

Wat de voorgestelde authenticatiemethodes betreft, geven deze – behoudens de in dit advies geformuleerde opmerkingen – geen aanleiding tot verdere bemerkingen. Daarnaast is het voor de Autoriteit niet duidelijk of de Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie ook loggegevens wenst bij te houden en welke deze dan zijn (IP-adres, lokalisatie, etc.). In die mate dat voormelde entiteit dit oogmerk heeft, verdient het de aanbeveling om hier verdere duiding over te voorzien.

11. Aangaande de verwijzing naar het 'paswoord', werd aan de aanvrager gevraagd om te verduidelijken of het de bedoeling is dat elk paswoord wordt bewaard, wat het oogmerk daarvan is, en wie er toegang toe heeft. De aanvrager verduidelijkte dat:

> *"Het paswoord wordt op zich niet as such bewaard: het paswoord wordt op versleutelde wijze opgeslagen door het octrooi-indieningsplatform (en dus niet door de authenticator app). Indien de klant het paswoord vergeet, zal een nieuw paswoord moeten worden aangemaakt: de beheerder van het octrooi-indieningsplatform heeft geen toegang tot het paswoord van de klant op zich."*

In acht genomen dat het noodzakelijk is voor de werking van het systeem dat dit gegeven opgeslagen wordt, docht op versleutelde wijze en in die mate dat er geen toegang tot het passwoord is vormt dit geen grond voor bijkomende opmerkingen.

12. Voorts werd verdere duiding verzocht van de aanvrager, betreffende de bewaartermijn van de loggegevens. Dienaangaande stipuleerde de aanvrager:

> *"De loggegevens worden door het octrooi-indieningsplatform typisch opgeslagen gedurende een termijn van 6 maanden."*

Dienaangaande verdient het de aanbeveling – rekening houdend met het transparantie en legaliteitsbeginsel – om dit vast te leggen in de norm zelf of te verwijzen naar de norm die dit vastlegt.

13. Tenslotte wordt op gewezen dat de Autoriteit zich in advies 55/2021 reeds uitgesproken heeft over de wet houdende de invoeging in boek XI van het wetboek van economisch recht van diverse bepalingen betreffende intellectuele eigendom. In het bijzonder werd daarin ingegaan op artikelen 80/1 WER en 80/2 WER. Analyse van het huidig bestaand regelgevend kader wijst uit dat deze op heden nog niet voldoet aan de vereisten van de AVG. De Autoriteit beperkt zich, naast de eerder aangehaalde aanbevelingen, ertoe om op te merken – in het kader van onderliggend voorwerp en het beginsel van de minimale gegevensverwerking – dat artikel 80/1, §3: "*alle persoonsgegevens die de betrokken persoon wenst te delen met de Dienst"* niet voldoet aan de noodzakelijkheidsvereiste en geenszins gegevens zijn die voor onbeperkte duur bewaard kunnen worden, zoals er in artikel 80/1, §5 gesuggereerd wordt. Voor het overige wordt de aanvrager aangemoedigd om de aanbevelingen uit advies nr. 55/2021 in het bijzonder randnrs. 30 t.e.m. 32; 35 t.e.m. 36; 41 en 42 in acht te nemen, m.h.o. het remediëren van de tekortkomingen uit hoofde van de AVG.

OM DEZE REDENEN,
de Autoriteit,

formuleert de volgende opmerkingen met betrekking tot het Ontwerp (dispositief):

is van oordeel dat geen bijzondere opmerkingen, m.u.v. randnrs. 4 en 6, aangaande de mogelijkheden die ingevoegd worden voor de elektrische handtekening voorhanden is. Niettemin is enige verduidelijking randnrs. 7, 10 en remediëring randnrs. 4, 6, 9, 12 aan de orde. Bovendien geldt omwille van de correlatie tussen het ontwerp en bepaalde kernbepalingen het WER, dat er ook rekening

gehouden moet worden met eerder geleverd advies 55/2021 en wordt verzocht de daarin geschetste aandachtspunten te remediëren om in lijn te zijn met de AVG.

Voor de Autorisatie- en Adviesdienst,
(get.) Jaspar Alexandra, Directeur