Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 136/2021 van 24 augustus 2021

Betreft: Advies m.b.t. een voorstel van resolutie betreffende het bestrijden van cyberfraude via geldezels (CO-A-2021-155)

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna de "Autoriteit"), aanwezig mevrouw Marie-Hélène Descamps, mevrouw Alexandra Jaspar en heren Yves-Alexandre de Montjoye, Bart Preneel en Frank Robben;

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 mevrouw Eliane Tillieux, Voorzitster van de Kamer van Volksvertegenwoordigers, ontvangen op 15/07/2021;

Gelet op het verslag van Alexandra Jaspar;

Brengt op 24 augustus 2021 het volgend advies uit:

I. VOORWERP VAN DE AANVRAAG

1. Mevrouw Eliane Tillieux, Voorzitster van de Kamer van Volksvertegenwoordigers wint het advies van de Autoriteit in m.b.t. een voorstel van resolutie betreffende het bestrijden van cyberfraude via geldezels.

2. In de resolutie wordt gesteld dat cybercriminelen die via het internet mensen geld afhandig maken, veelal "money mules" gebruiken. Om zelf niet betrapt te worden, door bijvoorbeeld het geld rechtstreeks op hun eigen rekening te laten overschrijven, gebruiken de oplichters "geldezels". Deze personen lenen tegen een vergoeding hun bankrekening en/of bankkaart met pincode uit. Het gestolen geld kan zo online uitgegeven worden, naar een andere bankrekening in binnen- of buitenland worden doorgestuurd of aan een bankautomaat worden afgehaald. Vaak is de geldezel de enige die gevat en veroordeeld wordt terwijl de opdrachtgevers buiten schot blijven.

3. Volgens de resolutie is dit het gevolg van het feit dat het de banken aan middelen ontbreekt om het probleem aan de bron te bestrijden. Er is veel meer nood aan uitwisseling van gegevens tussen banken om criminele netwerken te kunnen oprollen naar analogie met het Risk Warning System in Nederland. Dit systeem stelt de banken in staat om onderling onderzoeken te starten bij het witwassen van geld. In de resolutie wordt erop aangedrongen dat de regering een wettelijk kader uitwerkt om het voor de financiële instellingen mogelijk te maken informatie omtrent verdachte rekeningen en transacties uit te wisselen bij een vermoeden van het witwassen van geld, zodat een mogelijk crimineel netwerk makkelijker kan worden opgerold.

II. ONDERZOEK VAN DE AANVRAAG

4. De Autoriteit vestigt er de aandacht op dat het opsporen van criminelen gebeurt door de daartoe gemandateerde overheidsdiensten. Dergelijke onderzoeken gaan immers gepaard met een indringing van de persoonlijke levenssfeer. De vraag stelt zich of het wel de taak is van commerciële ondernemingen zoals banken, die uiteindelijk elkaars concurrenten zijn, om op eigen initiatief onderling onderzoeken op te starten naar hun klanten m.b.t. het witwassen van geld en dus eigenlijk een onderzoek naar strafrechtelijke inbreuken voeren en daarbij gegevens over personen uitwisselen. Dit gaat veel verder dan bijvoorbeeld een meldingsplicht van verdachte transacties aan de bevoegde gerechtelijke autoriteiten die strafonderzoeken voeren met de daarbij horende garanties voor de betrokkenen. Daarenboven leidt het ertoe dat de banken betrokken bij het onderzoek (onderzoeksdoeleinde) in het bezit komen van meer informatie over een klant dan zij in het kader van hun commerciële relatie (commercieel doeleinde) met hem beschikken. Het risico is dan ook aanzienlijk dat de "onderzoeksinformatie" vervolgens commercieel wordt aangewend.

5. Indien overwogen wordt om commerciële ondernemingen een "opsporingsrol" toe te bedelen, dan moet er maximaal naar worden gestreefd om de minimale gegevensverwerking te verzekeren door privacy enhancing technologies. Hierbij kan gedacht worden aan "Private Set Intersection". Daarbij kunnen banken elk een "zwarte lijst" opstellen met mogelijke namen of rekeningen betrokken bij money mules en dan nagaan welke namen ook op de "zwarte lijst" van andere banken voorkomen zonder enige informatie te lekken over gegevens die maar 1 keer voorkomen.

6. Zolang niets precies is uitgewerkt, is het voor de Autoriteit onmogelijk om een standpunt te bepalen. Zij beperkt zich hierna dan ook noodgedwongen tot het in herinnering brengen van de belangrijkste principes die bij de eventuele redactie van regelgeving in acht moeten worden genomen.

A. Noodzakelijkheidstoets

7. Elke verwerking van persoonsgegevens die door regelgeving wordt ingevoerd, houdt in principe een beperking in van het recht op bescherming van persoonsgegevens. Bij de voorbereiding van een ontwerp van normatieve tekst dat verwerkingen van persoonsgegevens omkadert, dient bijgevolg eerst te worden geanalyseerd of de geviseerde maatregel wel noodzakelijk is om het legitiem doel te bereiken dat ermee beoogd wordt. Deze noodzakelijkheidstoets impliceert dat de steller van een ontwerp van normatieve tekst een voorafgaande analyse uitvoert van enerzijds de feiten die de invoering van de maatregel rechtvaardigen en anderzijds de efficiëntiegraad van de maatregel in het licht van het doeleinde dat ermee beoogd wordt. Bij deze analyse dient de steller ook na te gaan of zijn doel eventueel via een maatregel kan bereikt worden die vanuit gegevensbeschermingsoogpunt minder intrusief is.

B. Rechtsgrondslag en voorzienbaarheid van de norm

8. Elke verwerking van persoonsgegevens dient een rechtsgrond te hebben in artikel 6.1 AVG. Gegevensverwerkingen die via een normatieve maatregel worden ingevoerd zijn vrijwel steeds gebaseerd op artikel 6.1. punt c) of e) AVG . Krachtens artikel 22 GW, artikel 8 EVRM en artikel 6.3 AVG, dienen dergelijke verwerkingen omkaderd te worden door duidelijke en nauwkeurige regelgeving, waarvan de toepassing voor de betrokkenen voorzienbaar moet zijn. De regelgeving dient dus op een voldoende precieze manier te bepalen onder welke voorwaarden en in welke omstandigheden de verwerking van persoonsgegevens plaatsvindt. In principe dienen de volgende elementen er daarom in te worden opgenomen:

a) de verwerkingsverantwoordelijke,
b) het (de) doeleinde(n) van de verwerking,

c) het soort gegevens die noodzakelijk zijn voor de verwezenlijking van dit (deze) doeleinde(n),
d) de bewaartermijn van de gegevens,
e) de categorieën betrokkenen van wie de gegevens zullen worden verwerkt,
f) de ontvangers of categorieën ontvangers aan wie de gegevens worden meegedeeld,
g) de omstandigheden waarin ze zullen worden meegedeeld.

C. Verwerking van gevoelige gegevens

9. De Autoriteit wijst er op dat de verwerking van sommige bijzondere categorieën van persoonsgegevens zoals opgesomd in de artikelen 9 & 10 AVG in principe verboden is.

10. Het betreft ten eerste de categorieën opgesomd in artikel 9.1 AVG: de persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Artikel 9.2 AVG beschrijft de situaties waarin uitzonderingen gelden op dit verwerkingsverbod. Indien dergelijke categorieën van gegevens ingevolge een ontwerp van normatieve tekst verwerkt zullen worden, is het aldus noodzakelijk om na te gaan of deze verwerking een basis vindt in één van de uitzonderingsgronden in artikel 9.2 AVG .

11. Bij de voorbereiding van een ontwerp van normatieve tekst zal vaak de uitzondering onder punt g) van artikel 9.2 AVG relevant zijn: "de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene". Indien de steller van een ontwerp van normatieve tekst een verwerking (ten dele) op dit artikel 9.2.g) AVG wil baseren, dient hij aldus het zwaarwegend algemeen belang aan te tonen dat de verwerking van deze gegevens noodzaakt. Bovendien moet het ontwerp van normatieve tekst specifieke maatregelen treffen om te waken over de bescherming van de grondrechten en de fundamentele belangen van de betrokkenen.

12. De Autoriteit wijst er verder op dat artikel 9 WVG bijkomende voorwaarden oplegt voor de verwerking van deze gegevenscategorieën.

13. Een tweede categorie van gegevens waarvoor een verwerkingsverbod geldt zijn gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (artikel 10 AVG). Dit soort gegevens mag alleen worden verwerkt onder toezicht van de overheid of een andere persoon indien de

verwerking door een wet (nationaal of Europees) is toegestaan. Omvattende registers van strafrechtelijke veroordelingen mogen alleen worden bijgehouden onder toezicht van de overheid. Tot slot bepaalt artikel 10 WVG door welke personen/instellingen dit type van gegevens kan verwerkt worden en onder welke voorwaarden dit dient te gebeuren.

D. Gebruik van het Rijksregisternummer

14. Indien het de bedoeling is om via een ontwerp van normatieve tekst voor welbepaalde doeleinden het gebruik van het Rijksregisternummer in te voeren, dienen onderstaande voorschriften in acht genomen te worden.

15. Artikel 87 van de AVG stelt dat lidstaten die een nationaal identificatienummer vaststellen er moeten over waken dat dit alleen wordt gebruikt indien er passende waarborgen voor de rechten en vrijheden van de betrokkene worden voorzien. Dergelijke garanties impliceren dat:

- het gebruik van een dergelijk nummer beperkt dient te worden tot de gevallen waarin dit strikt noodzakelijk en proportioneel is, aangezien dit gebruik bepaalde risico's met zich meebrengt;
- de doeleinden duidelijk en expliciet worden gepreciseerd zodat men de beoogde soorten verwerkingen kan vermoeden;
- de bewaartermijn en de eventuele mededelingen aan derden eveneens worden omkaderd;
- de technische en organisatorische maatregelen het beveiligd gebruik passend omkaderen.

16. De Autoriteit vestigt er verder de aandacht op dat het gebruik van het Rijksregisternummer slechts toegestaan is voor zover de betrokken instantie(s) over de vereiste machtiging beschik(t)(ken), op grond van de wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen* (artikel 8, § 1) . Overeenkomstig deze bepaling is er geen machtiging vereist om het Rijksregisternummer te gebruiken wanneer dit gebruik uitdrukkelijk voorzien is door of krachtens een wet, een decreet of een ordonnantie. In de andere gevallen wordt de machtiging tot gebruik van het Rijksregisternummer in principe verleend door de minister bevoegd voor Binnenlandse Zaken, onder de voorwaarden bepaald in de artikelen 5 en 8 van de wet van 8 augustus 1983. Wanneer het Informatieveiligheidscomité een beraadslaging moet verlenen voor een mededeling van persoonsgegevens kan hij in voorkomend geval tegelijk een beraadslaging verlenen voor het gebruik van het Rijksregisternummer door de betrokken instanties, indien dat noodzakelijk is in het kader van de beoogde mededeling.

17. Indien persoonsgegevens worden doorgegeven aan derde landen of een internationale organisatie moet erover gewaakt worden dat dit gebeurt hetzij overeenkomstig de instrumenten vermeld in de artikelen 45 - 48 AVG dan wel dat een van de specifieke situaties vermeld in artikel 49 AVG van toepassing is.

Voor het Kenniscentrum,
(get.) Alexandra Jaspar, Directeur