Samenvatting van het advies van de Europese Toezichthouder voor gegevensbescherming over het voorstel voor een verordening inzake digitale operationele veerkracht voor de financiële sector en tot wijziging van de Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014

(De volledige tekst van dit advies is beschikbaar in het Engels, het Frans en het Duits op de EDPS-website www.edps.europa.eu)

(2021/C 229/05)

De Europese Commissie heeft op 24 september 2020 een voorstel aangenomen voor een verordening inzake digitale operationele veerkracht voor de financiële sector en tot wijziging van de Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014 (het "voorstel"). Het voorstel voorziet in een alomvattend kader voor digitale operationele veerkracht van financiële entiteiten in de EU, gebaseerd op vijf belangrijke gebieden, namelijk het beheer van ICT-risico's (hoofdstuk II), het beheer, de classificatie en de rapportage van incidenten (hoofdstuk III), het testen van digitale operationele veerkracht (hoofdstuk IV), het beheer van risico's voor derden en de regulering van cruciale aanbieders van ICT-diensten (hoofdstuk V) en het delen van informatie (hoofdstuk VI).

De EDPS is ingenomen met de doelstellingen van het voorstel en acht het voor de stabiliteit van de financiële markt van de Europese Unie van essentieel belang dat financiële instellingen beschikken over een solide, alomvattend en goed gedocumenteerd kader voor ICT-risicobeheer.

De EDPS wijst erop dat het van belang is ervoor te zorgen dat elke verwerking in het kader van de verrichtingen van de financiële entiteiten is gebaseerd op een van de rechtsgrondslagen van artikel 6 van de AVG ([1]). Voorts wijst de EDPS erop dat het voor financiële entiteiten van belang is om in het kader van hun digitale operationele veerkracht een sterk governancemechanisme voor gegevensbescherming in te bouwen, waarin de taken en verantwoordelijkheden van de verwerkingsverantwoordelijke en de verwerker duidelijk worden aangegeven, evenals de verwerkingsactiviteiten die zullen plaatsvinden.

Met betrekking tot de internationale doorgifte aan derde aanbieders van ICT-diensten die in een derde land gevestigd zijn, wijst de EDPS erop dat elke internationale doorgifte van persoonsgegevens moet voldoen aan de vereisten van hoofdstuk V van de AVG, zoals uitgelegd in de jurisprudentie van het HvJ-EU, met inbegrip van het arrest in Schrems II.

Wat betreft de regelingen voor het delen van gegevens over inlichtingen en cyberdreigingen tussen financiële entiteiten, wijst de EDPS erop dat de bescherming van persoonsgegevens geen belemmering vormt voor het delen van inlichtingen in de financiële sector. De vereisten inzake gegevensbescherming moeten veeleer worden gezien als een basisvereiste waaraan moet worden voldaan om de rechten van het individu te waarborgen. In dit verband moedigt de EDPS aan om ook in de financiële sector gedragscodes vast te stellen overeenkomstig artikel 40 van de AVG, met name om de rol van de voornaamste belanghebbenden bij de verwerking van persoonsgegevens duidelijk te omschrijven en een eerlijke en transparante verwerking te waarborgen.

Ten aanzien van de bekendmaking van administratieve geldboetes beveelt de EDPS aan om de risico's voor de bescherming van de persoonsgegevens van het individu op te nemen in de criteria die door de bevoegde autoriteit in overweging moeten worden genomen. De EDPS wijst er voorts op dat het beginsel van de beperking van de opslag vereist dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt.

Wat de kennisgeving van gegevensinbreuken betreft, wijst de EDPS erop dat de formulering van overweging 42 van het voorstel onverenigbaar is met artikel 33 van de AVG. De EDPS beveelt derhalve aan de verwijzing naar gegevensbeschermingsautoriteiten uit overweging 42 van het voorstel te schrappen en artikel 17 van het voorstel enigszins aan te passen in overeenstemming met de aanbevelingen van dit advies.

1. ACHTERGROND

1. De Europese Commissie heeft op 24 september 2020 een voorstel aangenomen voor een verordening inzake digitale operationele veerkracht voor de financiële sector en tot wijziging van de Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014 (het "**voorstel**"). Het voorstel voorziet in een alomvattend kader voor digitale operationele veerkracht van financiële entiteiten in de EU, gebaseerd op vijf belangrijke gebieden, namelijk het beheer van ICT-risico's (hoofdstuk II), het beheer, de classificatie en de rapportage van incidenten (hoofdstuk III), het testen van digitale operationele veerkracht (hoofdstuk IV), het beheer van risico's voor derden en de regulering van cruciale aanbieders van ICT-diensten (hoofdstuk V) en het delen van informatie (hoofdstuk VI).

2. Dit voorstel maakt deel uit van een pakket dat ook een voorstel bevat voor een verordening om markten voor cryptoactiva op te bouwen ([2]) (de "**verordening betreffende markten in cryptoactiva**"), een voorstel voor een proefregeling voor marktinfrastructuren op basis van "distributed ledger"-technologie ([3]) en een voorstel ter verduidelijking of wijziging van een aantal daarmee samenhangende EU-regels voor financiële diensten ([4]). De EDPS is geraadpleegd over het voorstel voor een proefregeling voor marktinfrastructuren op basis van "distributed ledger"-technologie en heeft op 23 april 2021 zijn advies uitgebracht ([5]). Hij is ook geraadpleegd over de verordening betreffende markten in cryptoactiva van 29 april 2021 en zal zijn advies uitbrengen in overeenstemming met artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([6]).

3. De Europese Commissie heeft op 15 maart 2021 de Europese Toezichthouder voor gegevensbescherming (de "EDPS") verzocht een advies uit te brengen over het voorstel, overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725. Dit advies blijft beperkt tot de bepalingen van het voorstel die relevant vanuit het oogpunt van gegevensbescherming relevant zijn.

4. CONCLUSIES

Gelet op het vorenstaande wijst de EDPS:

— op het belang om ervoor te zorgen dat **elke verwerking** in het kader van de verrichtingen van de financiële entiteiten **gebaseerd is op een van de rechtsgrondslagen van artikel 6 van de AVG**, en wijst hij op artikel 6, lid 1, onder c), e) en f), van de AVG als mogelijke rechtsgrondslag die door de financiële entiteiten in overweging moet worden genomen;

— op het belang voor financiële entiteiten om in het kader van hun digitale operationele veerkracht een **sterk governancemechanisme voor gegevensbescherming** in te bouwen, waarin de taken en verantwoordelijkheden van de verwerkingsverantwoordelijke en de verwerker duidelijk worden aangegeven, evenals de verwerkingsactiviteiten die zullen plaatsvinden;

— op het feit dat **elke internationale doorgifte van persoonsgegevens door financiële entiteiten** aan een in een derde land gevestigde derde aanbieder van ICT-diensten **moet voldoen aan de vereisten van hoofdstuk V van de AVG**, en, indien uitgevoerd, onderworpen moet zijn aan passende waarborgen die in overeenstemming zijn met het gegevensbeschermingskader en de jurisprudentie van het HJEU, in het bijzonder de zaak Schrems II. Dergelijke financiële entiteiten kunnen een beroep doen op de standaardcontractclausules, omdat die het meest geschikte overdrachtsinstrument lijken te zijn.

— De EDPS benadrukt dat de **bescherming van persoonsgegevens geen belemmering vormt voor het delen van inlichtingen in de financiële sector**. De vereisten inzake gegevensbescherming moeten veeleer worden gezien als een basisvereiste waaraan moet worden voldaan om de rechten van het individu te waarborgen in het kader van de digitale operationele veerkracht van financiële entiteiten.

— De EDPS **moedigt aan om ook in de financiële sector gedragscodes vast te stellen** overeenkomstig artikel 40 van de AVG, met name om de rol van de voornaamste belanghebbenden bij de verwerking van persoonsgegevens duidelijk te omschrijven en een eerlijke en transparante verwerking te waarborgen.

— Ten aanzien van de **bekendmaking van administratieve geldboetes** beveelt de EDPS aan om de **risico's voor de bescherming van de persoonsgegevens van het individu** op te nemen in de criteria die door de bevoegde autoriteit in overweging moeten worden genomen.

— Overeenkomstig het beginsel van de beperking van de opslag beveelt de EDPS de financiële entiteiten aan maatregelen te nemen om ervoor te zorgen dat de **informatie over administratieve geldboetes van hun website wordt verwijderd nadat de vijf jaar zijn verstreken, of eerder** indien, zij niet langer nodig is.

— De EDPS wijst erop dat de **formulering van overweging 42 van het voorstel onverenigbaar is met artikel 33 van de AVG**. De EDPS beveelt derhalve aan de verwijzing naar de gegevensbeschermingsautoriteiten uit overweging 42 van het voorstel te schrappen en artikel 17 van het voorstel te wijzigen met een verwijzing naar de verplichting tot kennisgeving van inbreuken op de gegevensbescherming aan de relevante gegevensbeschermingsautoriteiten.

— De EDPS beveelt aan artikel 23, lid 2, van het voorstel zodanig te wijzigen dat het testen, de productontwikkeling of het onderzoek van de ICT-systemen niet kan worden uitgevoerd op systemen die prestaties in het reële leven verrichten die persoonsgegevens van klanten bevatten.

Brussel, 10 mei 2021.

Wojciech Rafał WIEWIÓROWSKI

([1]) 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 (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

([2]) *Voorstel voor een verordening van het Europees Parlement en de Raad betreffende markten in cryptoactiva en tot wijziging van Richtlijn (EU) 2019/1937, COM(2020) 593 final. Beschikbaar op https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A52020PC0593&qid=1621601324333*

([3]) *Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende een proefregeling voor marktinfrastructuren op basis van "distributed ledger"-technologie COM(2020) 594 final, beschikbaar ophttps://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A52020PC0594&qid=1621601091442*

([4]) *Voorstel voor een richtlijn van het Europees Parlement en de Raad tot wijziging van de Richtlijnen 2006/43/EG, 2009/65/EG, 2009/138/EU, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 en 2016/2341/EU, COM(2020) 596 final. Beschikbaar op https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52020PC0596*

([5]) *Advies 6/2021 over het voorstel voor een proefregeling voor marktinfrastructuren op basis van "distributed ledger"-technologie, beschikbaar op 2021-0219_d0912_opinion_6_2021_en_0.pdf (europa.eu)*

([6]) Verordening (EU) 2018/1727 van het Europees Parlement en de Raad van 14 november 2018 betreffende het Agentschap van de Europese Unie voor justitiële samenwerking in strafzaken (Eurojust), en tot vervanging en intrekking van Besluit 2002/187/JBZ van de Raad (PB L 295 van 21.11.2018, blz. 138).