Publicatieblad
van de Europese Unie

NL
L-serie

2025/301

20.2.2025

GEDELEGEERDE VERORDENING (EU) 2025/301 VAN DE COMMISSIE

van 23 oktober 2024

tot aanvulling van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad met betrekking tot technische reguleringsnormen voor de inhoud en termijnen van de eerste kennisgeving van en het tussentijdse en het eindverslag over ernstige ICT-gerelateerde incidenten en voor de inhoud van de vrijwillige kennisgeving van significante cyberdreigingen

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 ([1]), en met name artikel 20, derde alinea,

Overwegende hetgeen volgt:

(1) Om de harmonisatie en vereenvoudiging van de kennisgevings- en rapportagevereisten voor ernstige ICT-gerelateerde incidenten als bedoeld in artikel 19, lid 4, van Verordening (EU) 2022/2554 te waarborgen, moeten de rapportagetermijnen van ernstige ICT-gerelateerde incidenten een voor alle soorten financiële entiteiten consistente aanpak volgen. Om deze redenen moeten de termijnen ook zo veel mogelijk in overeenstemming zijn met en ten minste gelijkwaardig zijn aan de vereisten van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad ([2]).

(2) Om een onnodige rapportagedruk op financiële entiteiten bij de behandeling van het ICT-gerelateerde incident te voorkomen, moet de inhoud van de eerste kennisgeving worden beperkt tot de meest significante informatie. Om passende toezichtmaatregelen te kunnen nemen, moeten bevoegde autoriteiten zo snel mogelijk nadat de financiële entiteit een ICT-gerelateerd incident als ernstig heeft aangemerkt, informatie over het ernstige ICT-gerelateerde incident ontvangen. Bijgevolg moet de indieningstermijn van een eerste kennisgeving als bedoeld in artikel 19, lid 4, punt a), van Verordening (EU) 2022/2554 zo kort mogelijk nadat een ICT-gerelateerd incident als ernstig is aangemerkt, vallen maar tegelijkertijd ruimte laten voor flexibiliteit, met name voor bedrijfsmodellen voor dienstverlening die niet bijzonder tijdkritisch zijn, indien financiële entiteiten meer tijd nodig hebben om het ICT-gerelateerde incident te behandelen nadat zij er kennis van hebben gekregen.

(3) Na ontvangst van de eerste kennisgeving moeten de bevoegde autoriteiten in het tussentijdse verslag nadere informatie over het ICT-gerelateerde incident en in het eindverslag alle relevante informatie ontvangen. De informatie in die verslagen moet de bevoegde autoriteiten in staat stellen het ICT-gerelateerde incident verder te beoordelen en de toezichtmaatregelen te evalueren die zij eventueel willen nemen.

(4) De in artikel 20, eerste alinea, punt a), ii), van Verordening (EU) 2022/2554 bedoelde rapportagetermijnen moeten daarom een evenwicht vormen tussen de noodzaak voor de bevoegde autoriteiten om de informatie snel te ontvangen, en de noodzaak om financiële entiteiten voldoende tijd te geven om volledige en nauwkeurige informatie te verkrijgen.

(5) Rekening houdend met de criteria van artikel 20, eerste alinea, punt a), van Verordening (EU) 2022/2554 mogen de rapportagetermijnen geen onevenredige last vormen voor micro-ondernemingen en andere financiële entiteiten die niet significant zijn. Bovendien moet, om te voorkomen dat de rapportagetermijnen een onevenredige last vormen voor financiële entiteiten, rekening worden gehouden met het weekeinde en met feestdagen.

([1]) PB L 333 van 27.12.2022, blz. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972, en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(6) Omdat van significante cyberdreigingen kennisgeving mag worden gedaan op vrijwillige basis, mag de inhoud van dergelijke kennisgevingen geen last vormen voor financiële entiteiten en moet deze beperkter blijven dan de informatie die voor ernstige ICT-gerelateerde incidenten wordt gevraagd.

(7) Deze verordening berust op de ontwerpen van technische reguleringsnormen die de Europese toezichthoudende autoriteiten bij de Commissie hebben ingediend.

(8) De Europese toezichthoudende autoriteiten hebben open publieke raadplegingen gehouden over de ontwerpen van technische reguleringsnormen waarop deze verordening is gebaseerd, hebben de mogelijke daaraan verbonden kosten en baten geanalyseerd en hebben het advies ingewonnen van de bij artikel 37 van Verordeningen (EU) nr. 1093/2010 ([3]), (EU) nr. 1094/2010 ([4]) en (EU) nr. 1095/2010 ([5]) van het Europees Parlement en de Raad opgerichte stakeholdergroepen.

(9) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([6]) en heeft op 22 juli 2024 een positief advies uitgebracht. Elke verwerking van persoonsgegevens die binnen het toepassingsgebied van deze verordening valt, moet plaatsvinden in overeenstemming met de toepasselijke beginselen inzake gegevensbescherming en de bepalingen van Verordening (EU) 2018/1725,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Algemene informatie die moet worden verstrekt in de eerste kennisgeving en in het tussentijdse en het eindverslag over ernstige ICT-gerelateerde incidenten

Financiële entiteiten nemen in de eerste kennisgeving, het tussentijdse verslag en het eindverslag als bedoeld in artikel 19, lid 4, van Verordening (EU) 2022/2554, de volgende algemene informatie op:

a) de soort indiening (eerste kennisgeving, tussentijds verslag of eindverslag);

b) de naam van de financiële entiteit, haar LEI-code en de soort financiële entiteit als bedoeld in artikel 2, lid 1, van Verordening (EU) 2022/2554;

c) de naam en identificatiecode van de entiteit die de eerste kennisgeving of het tussentijdse of het eindverslag voor de financiële entiteit indient;

d) indien van toepassing, de namen en LEI-codes van alle financiële entiteiten waarop de geaggregeerde eerste kennisgeving of het geaggregeerde tussentijdse of eindverslag betrekking heeft;

e) de contactgegevens van de personen die verantwoordelijk zijn voor de communicatie met de bevoegde autoriteit over het ernstige ICT-gerelateerde incident;

f) in voorkomend geval, de identificatie van de moederonderneming van de groep waartoe de financiële entiteit behoort;

g) wanneer er sprake is van monetaire gevolgen, de valuta waarop de bedragen zijn gebaseerd.

([3]) Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie (PB L 331 van 15.12.2010, blz. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Verordening (EU) nr. 1094/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/79/EG van de Commissie (PB L 331 van 15.12.2010, blz. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Verordening (EU) nr. 1095/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/77/EG van de Commissie (PB L 331 van 15.12.2010, blz. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Artikel 2

Bijzondere informatie die in de eerste kennisgeving moet worden verstrekt

De eerste kennisgeving als bedoeld in artikel 19, lid 4, punt a), van Verordening (EU) 2022/2554 bevat ten minste alle volgende informatie:

a) de door de financiële entiteit toegekende referentiecode van het incident;

b) de datum van detectie, het tijdstip van detectie en de classificatie van het incident overeenkomstig artikel 8 van Gedelegeerde Verordening (EU) 2024/1772 van de Commissie ([7]);

c) een beschrijving van het ICT-gerelateerde incident;

d) de criteria van de artikelen 1 tot en met 8 van Gedelegeerde Verordening (EU) 2024/1772 op basis waarvan de financiële entiteit het ICT-gerelateerde incident als ernstig heeft geclassificeerd;

e) de lidstaten die door het ICT-gerelateerde incident worden getroffen;

f) informatie over de wijze waarop het ICT-gerelateerde incident is ontdekt;

g) indien beschikbaar, informatie over de oorsprong van het ICT-gerelateerde incident;

h) informatie over de vraag of de financiële entiteit een bedrijfscontinuïteitsplan heeft geactiveerd;

i) indien van toepassing, informatie over de herclassificatie van het ICT-gerelateerde incident van ernstig naar niet-ernstig;

j) indien beschikbaar, alle andere relevante informatie.

Artikel 3

Bijzondere informatie die in het tussentijdse verslag moet worden verstrekt

Het in artikel 19, lid 4, punt b), van Verordening (EU) 2022/2554 bedoelde tussentijdse verslag bevat ten minste alle volgende informatie:

a) indien van toepassing, de door de bevoegde autoriteit verstrekte referentiecode van het incident;

b) de datum en het tijdstip waarop het ICT-gerelateerde incident zich heeft voorgedaan;

c) indien van toepassing, de datum en het tijdstip waarop de financiële entiteit haar reguliere activiteiten heeft hersteld;

d) informatie over de wijze waarop aan de criteria van de artikelen 1 tot en met 8 van Gedelegeerde Verordening (EU) 2024/1772 is voldaan, op basis waarvan de financiële entiteit het ICT-gerelateerde incident als ernstig heeft geclassificeerd;

e) de soort ICT-gerelateerd incident;

f) indien van toepassing, de dreigingen en technieken die door de dreigingsactor zijn gebruikt;

g) de getroffen functionele gebieden en bedrijfsprocessen;

h) de getroffen infrastructuurcomponenten ter ondersteuning van bedrijfsprocessen;

i) de gevolgen voor de financiële belangen van cliënten;

j) informatie over de rapportage over het ICT-gerelateerde incident aan andere autoriteiten;

k) tijdelijke acties of maatregelen die de financiële entiteit heeft genomen of gepland om te herstellen van het ICT-gerelateerde incident;

l) indien van toepassing, informatie over indicatoren voor aantasting.

([7]) Gedelegeerde Verordening (EU) 2024/1772 van de Commissie van 13 maart 2024 tot aanvulling van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad met betrekking tot technische reguleringsnormen tot nadere bepaling van de criteria voor de classificatie van ICT-gerelateerde incidenten en cyberdreigingen, tot vaststelling van materialiteitsdrempels en tot bepaling van de nadere informatie van verslagen over ernstige incidenten (PB L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

Artikel 4

Bijzondere informatie die in het eindverslag moet worden verstrekt

Het in artikel 19, lid 4, punt c), van Verordening (EU) 2022/2554 bedoelde eindverslag bevat alle volgende informatie:

a) informatie over de onderliggende oorzaken van het ICT-gerelateerde incident;

b) de datums en tijdstippen waarop het ICT-gerelateerde incident is opgelost en de onderliggende oorzaak of oorzaken is of zijn aangepakt;

c) informatie over de oplossing van het ICT-gerelateerde incident;

d) in voorkomend geval, informatie die relevant is voor afwikkelingsautoriteiten;

e) informatie over directe en indirecte kosten en verliezen die voortvloeien uit het ICT-gerelateerde incident en informatie over financiële terugvorderingen;

f) indien van toepassing, informatie over terugkerende ICT-gerelateerde incidenten.

Artikel 5

Termijnen van de eerste kennisgeving en van het tussentijdse en het eindverslag

1. Financiële entiteiten dienen de eerste kennisgeving en het tussentijdse en het eindverslag als bedoeld in artikel 19, lid 4, punten a), b) en met c), van Verordening (EU) 2022/2554 in binnen de volgende termijnen:

a) eerste kennisgeving: zo snel mogelijk, maar in ieder geval binnen vier uur na de classificatie van het ICT-gerelateerde incident als ernstig en uiterlijk 24 uur nadat de financiële entiteit kennis heeft gekregen van het ICT-gerelateerde incident;

b) tussentijds verslag: uiterlijk 72 uur na de indiening van de eerste kennisgeving, ook indien de status of de behandeling van het incident niet is gewijzigd als bedoeld in artikel 19, lid 4, punt b), van Verordening (EU) 2022/2554. Financiële entiteiten dienen onverwijld en in elk geval wanneer de reguliere activiteiten zijn hersteld, een bijgewerkt tussentijds verslag in;

c) eindverslag: uiterlijk één maand na de indiening van het tussentijdse verslag of, in voorkomend geval, na het laatst bijgewerkte tussentijdse verslag.

2. Indien de financiële entiteit een ICT-gerelateerd incident niet binnen 24 uur na het moment waarop zij kennis heeft gekregen van het ICT-gerelateerde incident, als ernstig heeft geclassificeerd, maar dat ICT-gerelateerde incident in een later stadium als ernstig classificeert, dient zij de eerste kennisgeving in binnen vier uur na de classificatie van het ICT-gerelateerde incident als ernstig incident.

3. Financiële entiteiten die niet in staat zijn om de eerste kennisgeving, het tussentijdse verslag of het eindverslag binnen de termijnen van lid 1 in te dienen, stellen de bevoegde autoriteit daarvan onverwijld en uiterlijk binnen de respectieve indieningstermijnen van de kennisgeving of het verslag in kennis en lichten de redenen voor de vertraging toe.

4. Indien in de lidstaat van de rapporterende financiële entiteit de indieningstermijn van een eerste kennisgeving, een tussentijds verslag of een eindverslag op een dag in het weekeinde of op een feestdag valt, kan de financiële entiteit de eerste kennisgeving, het tussentijdse of het eindverslag uiterlijk om 12.00 uur van de volgende werkdag indienen.

5. Lid 4 is niet van toepassing op de indiening van een eerste kennisgeving of een tussentijds verslag door kredietinstellingen, centrale tegenpartijen, exploitanten van handelsplatformen en andere financiële entiteiten die op grond van artikel 3 van Richtlijn (EU) 2022/2555 als essentiële of belangrijke entiteiten zijn aangemerkt.

6. De bevoegde autoriteiten kunnen bepalen dat lid 4 niet van toepassing is op de indiening van een eerste kennisgeving of een tussentijds verslag door andere dan de in lid 5 genoemde financiële entiteiten die op nationaal of Unieniveau van significant belang of een systemisch karakter hebben voor de financiële sector. De bevoegde autoriteiten stellen de desbetreffende financiële entiteiten in kennis van hun beslissing. De beslissing van de bevoegde autoriteit geldt alleen voor incidenten die na de datum van kennisgeving van de beslissing door de bevoegde autoriteit aan de desbetreffende financiële entiteiten worden gerapporteerd.

Artikel 6

Inhoud van de vrijwillige kennisgeving van significante cyberdreigingen

De inhoud van de vrijwillige kennisgeving van significante cyberdreigingen als bedoeld in artikel 19, lid 2, van Verordening (EU) 2022/2554, bestaat uit alle volgende elementen:

a) algemene informatie over de kennisgevende financiële entiteit als bedoeld in artikel 1;

b) de datum en het tijdstip van detectie van de significante cyberdreiging en alle andere relevante tijdstempels in verband met de significante cyberdreiging;

c) een beschrijving van de significante cyberdreiging;

d) informatie over de mogelijke gevolgen van de significante cyberdreiging voor de financiële entiteit, haar cliënten of financiële tegenpartijen;

e) de in de artikelen 1 tot en met 8 van Gedelegeerde Verordening (EU) 2024/1772 vastgelegde classificatiecriteria die aanleiding zouden hebben gegeven tot de rapportage van een ernstig incident indien de cyberdreiging werkelijkheid was geworden;

f) informatie over de status van de significante cyberdreiging en eventuele wijzigingen in de dreigingsactiviteit;

g) indien van toepassing, een beschrijving van de maatregelen die de financiële entiteit heeft genomen om te voorkomen dat de significante cyberdreigingen werkelijkheid worden;

h) informatie over elke kennisgeving van de significante cyberdreiging aan andere financiële entiteiten of autoriteiten;

i) indien van toepassing, informatie over indicatoren voor aantasting;

j) indien beschikbaar, alle andere relevante informatie.

Artikel 7

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 23 oktober 2024.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN