Sven Uiterwijk
sven.uiterwijk@nautadutilh.com

Joris Willems
joris.willems@nautadutilh.com

Amsterdam, 17 oktober 2024

Memorandum

Aan **Stichting Waarborgfonds Eigen Woningen**

Betreffende Implementatie van DORA

1 INLEIDING

1.1 Stichting Waarborgfonds Eigen Woningen (de "**Stichting**" of "**NHG**") heeft ons gevraagd te beoordelen hoe zij invulling geeft aan de verplichtingen die voortvloeien uit de verordening betreffende digitale operationele weerbaarheid voor de financiële sector ("**DORA**")[1].

1.2 Het verzoek van NHG houdt verband met de rol van NHG als derde aanbieder van ICT-diensten (zoals in DORA gedefinieerd, hierna kortweg: "**ICT-dienstverlener**"). Meer specifiek richt onze beoordeling zich op artikelen 28(7) en 30(2) DORA, waarin staan opgesomd welke elementen moeten worden opgenomen in contractuele overeenkomsten inzake het gebruik van ICT-diensten die worden verleend door ICT-dienstverleners.

1.3 Wij nemen voor onze beoordeling aan dat NHG kwalificeert als een ICT-dienstverlener onder DORA met betrekking tot de ICT-voorziening die zij aan geldverstrekkers beschikbaar stelt. Tegelijkertijd nemen wij aan dat NHG niet zal kwalificeren als een kritieke derde aanbieder van ICT-diensten onder DORA en zodoende niet onder toezicht komt te staan van een Europese toezichthouder. NHG verwacht bovendien dat haar ICT-dienst niet essentieel is voor geldverstrekkers om hypothecaire kredieten te kunnen verstrekken. Zij heeft zodoende de verplichtingen die gelden voor ICT-diensten die kritieke of belangrijke functies ondersteunen buiten beschouwing gelaten. Deze aannames en uitgangspunten vormen de basis voor de verdere beschrijving en beoordeling in dit memorandum.

1.4 We merken op dat toekomstige ontwikkelingen en interpretaties van

[1] 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) 2016/101.

DORA (bijvoorbeeld als gevolg van toezichthouderrichtsnoeren) de hiervoor genoemde aannames en uitgangspunten, en onze beoordeling, kunnen doen veranderen. Het is uiteindelijk de verantwoordelijkheid van de relevante geldverstrekkers om een eigen beoordeling te maken.

1.5 Wij sluiten in dit memorandum aan bij de terminologie in DORA, tenzij anders vermeld.

1.6 Dit memorandum is gericht aan de Stichting. De Stichting mag dit memorandum op haar website plaatsen, zodat geldverstrekkers er kennis van kunnen nemen. Zij kunnen echter geen rechten aan dit memorandum ontlenen.

2 (ICT-)DIENSTVERLENING VAN NHG

2.1 In deze paragraaf geven wij een korte beschrijving van de dienstverlening vanuit NHG aan geldverstrekkers en de daarop van toepassing zijnde voorwaarden.

2.2 NHG heeft met geldverstrekkers een overeenkomst van borgtocht gesloten, waarop haar voorwaarden en normen van toepassing zijn verklaard. NHG staat door middel van deze overeenkomst van borgtocht borg voor bepaalde hypothecaire kredieten verstrekt door de geldverstrekkers aan consumenten. In het kader van haar dienstverlening omtrent de borgtocht stelt NHG een ICT-voorziening beschikbaar aan de geldverstrekkers. De ICT-voorziening bevat meerdere functies, waaronder de 'NHG-toets' die wordt gebruikt om te beoordelen of een woning en de daarvoor te sluiten lening binnen de NHG-voorwaarden valt. Daarnaast kunnen de geldverstrekkers via de ICT-voorziening nieuwe leningen bij NHG aanmelden, declaraties indienen, uitzonderingsverzoeken doen en een beheertoets uitvoeren. De 'Algemene voorwaarden data en ICT – versie 1 januari 2025' (voorheen ‘Algemene voorwaarden uitwisseling gegevens’) en het 'Weerbaarheid en security statement – versie 1 januari 2025' (voorheen 'Privacy & Security Statement') zijn hierop in het bijzonder van toepassing.

3 DORA OP HOOFDLIJNEN

3.1 DORA heeft als doel een geharmoniseerd kader te creëren voor de digitale operationele weerbaarheid van financiële entiteiten binnen de Europese Unie. Het voorziet in een breed scala aan regels rondom ICT-risicobeheer, beveiliging, bedrijfscontinuïteit, testen van de digitale weerbaarheid en het contracteren van ICT-dienstverleners.

3.2 Vanaf 17 januari 2025 moeten financiële entiteiten volledig voldoen aan de regels en verplichtingen uit DORA. In dat kader moeten bepaalde elementen (bepalingen) worden opgenomen in de overeenkomsten tussen financiële entiteiten en hun ICT-dienstverleners. Deze hebben bijvoorbeeld te maken met het beheer van (persoons)gegevens,

incidentrespons en beëindigingsgronden van de overeenkomst. Indien de diensten van de ICT-dienstverlener zogenoemde kritieke of belangrijke functies van de financiële entiteit ondersteunen, gelden er strengere (contractuele) verplichtingen, waaronder met betrekking tot monitoring, onderaannemers en rapportageverplichtingen.

3.3 Hoewel DORA deze verplichtingen voorschrijft met verwijzing naar ICT-dienstverleners en de overeenkomsten met die dienstverleners, zijn uiteindelijk de financiële entiteiten verantwoordelijk voor het naleven van de regels. Omdat NHG meerdere financiële entiteiten als ketenpartners kent en er belang aan hecht om DORA op een consistente en werkbare wijze in haar dienstverlening te implementeren, heeft zij reeds stappen gezet om de contractuele voorwaarden uit DORA te integreren in haar dienstverlening. Dat doet zij op de wijze zoals hieronder beschreven.

4 IMPLEMENTATIE VAN DORA

4.1 Om invulling te geven aan de contractuele voorwaarden uit DORA heeft NHG haar 'Algemene voorwaarden data en ICT' (voorheen ‘Algemene voorwaarden uitwisseling gegevens’) en het 'Weerbaarheid en security statement' (voorheen 'Privacy & Security Statement') aangepast en aanvullende bepalingen opgenomen. Daarnaast heeft zij een 'DORA Statement – versie 17 januari 2025' opgesteld. Hierin beschrijft NHG hoe zij, door de eerdergenoemde voorwaarden te wijzigen, invulling geeft aan de voor financiële entiteiten verplichte contractuele voorwaarden.

4.2 NHG heeft als uitgangspunt genomen dat haar ICT-dienst niet essentieel is voor geldverstrekkers om hypothecair krediet te kunnen verstrekken en zodoende de verplichtingen die gelden voor ICT-diensten die kritieke of belangrijke functies ondersteunen buiten beschouwing gelaten. Daardoor zijn enkel de contractuele vereisten uit artikelen 28(7) en 30(2) DORA van toepassing op haar overeenkomsten met de geldverstrekkers. In de volgende paragrafen worden de contractuele voorwaarden uit deze artikelen besproken. Opgemerkt zij dat er op het moment van schrijven geen verdere richtsnoeren vanuit wetgevers of toezichthouders zijn gepubliceerd die een verdere invulling geven aan de genoemde vereisten.

Art. 30(2), sub a: een duidelijke en volledige beschrijving van alle door de derde aanbieder van ICT-diensten te leveren functies en ICT-diensten (…)

4.3 Ten eerste moeten de contractuele overeenkomsten tussen financiële entiteiten en ICT-dienstverleners volgens artikel 30 lid 2 sub a DORA een duidelijke en volledige beschrijving bevatten van alle door de ICT-dienstverlener te leveren functies en ICT-diensten. Artikel 4 van de 'Algemene voorwaarden data en ICT' bevat een beschrijving van de door NHG geleverde ICT-dienst en bijbehorende functies, waar het 'DORA Statement' eveneens naar verwijst. Deze beschrijving voldoet naar onze mening aan de vereisten uit artikel 30 lid 2 sub a DORA.

Art. 30(2), sub b: de locaties, met name de regio's of landen, waar de contractueel overeengekomen of uitbestede functies en ICT-diensten moeten worden geleverd en waar gegevens moeten worden verwerkt, (…), en de verplichting voor de derde aanbieder van ICT-diensten om de financiële entiteit vooraf in kennis te stellen indien hij voornemens is van locatie te veranderen

Art. 30(2), sub c: bepalingen inzake beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid met betrekking tot de bescherming van gegevens, met inbegrip van persoonsgegevens

Art. 30(2), sub d: bepalingen inzake het waarborgen van de toegang, het herstel en de teruggave in een gemakkelijk toegankelijk formaat van de (…) persoonsgegevens en niet-persoonsgebonden gegevens (…)

4.4 Daarnaast schrijft DORA een aantal contractuele voorwaarden voor omtrent (persoons)gegevens. Zo verplicht artikel 30 lid 2 sub b DORA dat partijen de locaties moeten beschrijven van waaruit ICT-diensten geleverd worden en waar gegevens verwerkt worden. Tevens moet de ICT-dienstverlener de financiële entiteit vooraf in kennis stellen als hij voornemens is om deze locaties te veranderen. Volgens artikel 30 lid 3 sub c DORA moeten eveneens afspraken worden gemaakt over de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van (persoons)gegevens. Tot slot dienen er uit hoofde van artikel 30 lid 2 sub d DORA bepalingen te worden opgenomen middels die waarborgen dat bij faillissement of beëindiging van bedrijfsactiviteiten of beëindiging van de overeenkomst de verwerkte gegevens worden geleverd in een toegankelijk formaat.

4.5 NHG heeft in artikel 5 van de 'Algemene voorwaarden data en ICT' vermeld dat haar ICT-dienst vanuit Nederland wordt geleverd en dat gegevens binnen de Europese Economische Ruimte worden verwerkt. Bij wijzigingen van deze locaties zullen geldverstrekkers op voorhand worden geïnformeerd. In artikel 6 van de 'Algemene voorwaarden data en ICT' vermeldt NHG dat zij, ter bescherming van de door haar ontvangen gegevens, de 'DNB Good Practice Informatiebeveiliging 2023' volgt. Dit heeft onder meer betrekking op de onderwerpen beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid. Specifiek voor persoonsgegevens hanteert NHG het 'Privacy Management Accountability Framework' van Nymity en heeft NHG een uitvoerige beschrijving toegewijd aan privacy in de 'Weerbaarheid Security Statement'. Wat de beschikbaarheid van gegevens betreft staat in artikel 7 van de 'Algemene voorwaarden data en ICT' dat de gegevens die NHG ontvangt onverminderd in het bezit blijven van de geldverstrekkers. Daardoor hebben laatstgenoemde altijd toegang tot hun gegevens die via de ICT-dienst worden verwerkt. Feitelijk gezien is het teruggeven van de gegevens in een toegankelijk formaat aldus niet nodig, hoewel NHG zich eraan verbindt om in elk geval de gegevens te bewaren zo lang dat nodig is. In onze optiek heeft NHG hierdoor de contractuele normen uit DORA met

betrekking tot (persoons)gegevens op afdoende wijze geïmplementeerd.

Art. 30(2), sub e: beschrijvingen van het dienstenniveau, met inbegrip van actualiseringen en herzieningen daarvan

4.6 Ook moeten de contractuele overeenkomsten volgens artikel 30 lid 2 sub e DORA beschrijvingen van het dienstenniveau bevatten, met inbegrip van actualiseringen en herzieningen daarvan. Het dienstenniveau staat beschreven in artikel 8 van de 'Algemene voorwaarden data en ICT'. De belangrijkste uitgangspunten daarvan zijn dat de ICT-dienst 24x7 beschikbaar is met een uptime van 99,5%. Eventuele actualiseringen en herzieningen daarvan zullen hierin moeten worden verwerkt.

Art. 30(2), sub f: de verplichting van de derde aanbieder van ICT-diensten om (…) bijstand te verlenen wanneer zich een incident voordoet (…)

4.7 Artikel 30 lid 2 sub f DORA bevat de eis dat een ICT-dienstverlener bijstand moet verlenen wanneer zich een incident voordoet dat verband houdt met de door hem geleverde ICT-dienst. Ook dit wordt door NHG uitgewerkt in artikel 8 van de 'Algemene voorwaarden data en ICT': geldverstrekkers mogen kosteloos gebruikmaken van ondersteuning door NHG bij een incident dat verband houdt met de ICT-dienst.

Art. 30(2), sub g: de verplichting van de derde aanbieder van ICT-diensten om volledige medewerking te verlenen aan de bevoegde autoriteiten en de afwikkelingsautoriteiten

4.8 Een andere verplichting dat artikel 30 lid 2 sub g DORA voorschrijft is dat ICT-dienstverleners volledige medewerking moeten verlenen aan de bevoegde nationale autoriteiten en afwikkelingsautoriteiten van financiële entiteiten. NHG heeft deze verplichting voor haarzelf rechtstreeks opgenomen in artikel 9 van de 'Algemene voorwaarden data en ICT'.

Art. 30(2), sub h: beëindigingsrechten en de bijbehorende minimumopzegtermijnen

Art. 28(7): financiële entiteiten zorgen ervoor dat contractuele overeenkomsten inzake het gebruik van ICT-diensten in elk van de volgende omstandigheden kunnen worden beëindigd (…)

4.9 Daarnaast moeten er volgens artikel 30 lid 2 sub h DORA beëindigingsrechten en de bijbehorende minimumopzegtermijnen worden opgenomen in de overeenkomst. Deze beëindigingsrechten zijn in elk geval verplicht voor de situaties die genoemd worden in artikel 28 lid 7 DORA. Samengevat hebben deze betrekking op de volgende omstandigheden: i) bij ernstige overtredingen van toepasselijke wetten, voorschriften of contractuele voorwaarden; ii) indien zich voor de overeenkomst relevante risico’s materialiseren tijdens de uitvoering van de overeenkomst; iii) bij klaarblijkelijke zwakheden van de ICT-dienstverlener in het beheer van ICT-risico’s; en iv) indien de bevoegde

autoriteit niet langer doeltreffend toezicht kan uitoefenen op de financiële entiteit.

4.10 In artikel 10 van de 'Algemene voorwaarden data en ICT' heeft NHG aangegeven dat geldverstrekkers op grond van de overeenkomst van borgtocht het recht hebben om deze overeenkomst op te zeggen met een opzegtermijn van twaalf maanden. Bovendien kunnen geldverstrekkers het gebruik van de ICT-dienst per direct beëindigen indien zij besluiten tot opzegging, ongeacht de reden. Daarmee worden de vereisten en situaties uit paragraaf 4.9 gedekt, zonder dat een uitsplitsing van beëindigingsgronden noodzakelijk is.

Art. 30(2), sub i: de voorwaarden voor deelname van derde aanbieders van ICT-diensten aan bewustmakingsprogramma's (...)

4.11 De laatste contractuele voorwaarde, artikel 30 lid 2 sub i DORA, houdt in dat ICT-dienstverleners moeten deelnemen aan bewustmakingsprogramma's van financiële entiteiten. NHG heeft in artikel 11 van de 'Algemene voorwaarden data en ICT' opgenomen dat zij enkele medewerkers zal laten deelnemen aan tenminste één bewustmakingsprogramma of opleiding die wordt aangeboden door of via een brancheorganisatie bij wie geldverstrekkers aangesloten zijn. Dit zullen dan medewerkers zijn voor wie de betreffende onderwerpen relevant zijn in verband met hun taken en verantwoordelijkheden. Dit is onzes inziens een afdoende invulling van de verplichting onder artikel 30 lid 2 sub i DORA.

5 BEOORDELING

5.1 Wij hebben de voorwaarden die van toepassing zijn op de ICT-dienstverlening van NHG aan geldverstrekkers getoetst aan de relevante vereisten zoals gesteld in artikelen 28(7) en 30(2) DORA. Op basis van bovenstaande analyse zijn wij van mening dat NHG deze vereisten op afdoende wijze heeft weergegeven in die voorwaarden.