Hieronder volgt een weergave van de vragen die gesteld zijn tijdens het bespreken van Amendement zoals Visma Idella dat wil overeenkomen met haar klanten.

Disclaimer
Dit vraag- en antwoorddocument is uitsluitend bedoeld ter verduidelijking van het addendum op de klantovereenkomst in het kader van de Digital Operational Resilience Act (DORA). De verstrekte informatie dient niet te worden beschouwd als juridisch advies of bindende uitleg van wettelijke vereisten. Hoewel wij ernaar streven om nauwkeurige en actuele informatie te verstrekken, kunnen wij geen garantie bieden voor de volledigheid of juistheid van de inhoud.

V: Waarom staat Artikel 9.2 niet in alle uitgestuurde versies van het Amendement opgenomen?
A: Dit is per abuis bij een aantal klanten achterwege gebleven. In artikel 9.2 staat het volgende:
Visma Idella kan de Overeenkomst en dit Amendement geheel of gedeeltelijk opzeggen door schriftelijke kennisgeving aan Opdrachtgever:

(a) met onmiddellijke ingang, indien een bevoegde autoriteit wijzigingen in de Overeenkomst en/of dit Amendement vereist die redelijkerwijs niet aanvaardbaar zijn voor een van beide Partijen;

V: Waarom is artikel 9.2 geïntroduceerd?
A: Artikel 9 en 9.2 zijn gefundeerd op o.a. het gestelde in artikel 28 DORA. In artikel 28 lid 7 onder b staat:
'Financial entities shall ensure that contractual arrangements on the use of ICT services may be terminated in any of the following circumstances:
a. (...)
b. circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the ICT third-party service provider;
c (...)
d(...)'

Niet gesteld is dat in het geval als voorzien onder b alleen de financiële entiteit mag opzeggen. Dit is ook niet logisch, omdat anders een leverancier die geconfronteerd wordt met *'material changes that affect the arrangement or the situation*' gedwongen wordt zich te committeren aan een overeenkomst, waarvan zij weet dat zij die niet kan uitvoeren vanwege '*material changes*' geïnitieerd door de toezichthouder en/of klant.

In 9.2. hebben we artikel 28 al ingedikt tot een expliciete aanwijzing van de DNB (die een aanwijzing eist die in redelijkheid niet aanvaardbaar is voor één van beide partijen). Overigens is het zeer onaannemelijk dat de DNB eist dat per direct de eis ingaat, waarmee een natuurlijke overgang wordt geïntroduceerd.

V: In artikel 3.4 staat een termijn van 30 dagen genoemd. Is dit afdoende voor het doorvoeren van een wijziging?
A: In artikel 3.4 staat een termijn van *minimaal* 30 genoemd. Dit betekent dat we een ruimere termijn zullen hanteren als de wijziging daarom vraagt.

V: Het amendement van de federatie is gebaseerd op de concept RTS. Is onderzocht of/wat de GAP is met de definitieve RTS en mogelijke impact daarvan op de inhoud van het amendement?

A: Zover wij hebben kunnen beoordelen, hebben de gepubliceerde definitieve RTS documenten geen invloed gehad op de inhoud van het amendement zoals wij dat nu opgesteld hebben op basis van het template van de Pensioenfederatie. Mocht de Pensioenfederatie met een herziene versie komen, zullen wij deze uiteraard beoordelen.

V: Als in de bestaande overeenkomst zaken beter/strikter geregeld zijn voor de klant dan in het amendement, prevaleert dan toch het amendement?
A: In het geval dat afwijkingen worden geconstateerd, verzoeken wij de klant contact op te nemen met de Customer Success manager binnen Visma Idella. De DORA heeft aanvullende verplichtingen in het leven geroepen die niet zonder meer voor het financiële risico van Visma Idella dienen te vallen. Ook niet indien in de huidige Overeenkomst staat omschreven dat bepaalde kosten wel voor rekening van Visma Idella komen. Immers, de huidige overeenkomst is opgesteld zonder dat voldoende concreet de scope en de impact van DORA was meegenomen (en kon worden meegenomen).

V: Wordt DORA expliciet onderdeel van de ISAE?
A: In de huidige scope van ISAE is DORA geen onderdeel van ISAE. Visma Idella bekijkt nog op welke wijze assurance verschaft kan worden over DORA compliancy.

V: Wanneer krijgen wij het informatieregister van jullie?
A: Visma Idella zal uiterlijk 31 december 2024 het register ter beschikking stellen. Dit register volgt het format als aangeleverd door ESA. Visma Idella zal als leverancier in dat register alle informatie opleveren voor zover vereist. Financiële entiteiten hebben ook zelf een deel van het register in te vullen. In november 2024 zal Visma Idella een eerste concept ter beschikking stellen. Zulks in verband met eventuele wijzigingen in het format, welk format nog steeds niet finaal is vastgesteld door ESA.

Toelichting
In artikel 5 lid 2 van de final RTS (52) staat: “To maintain the financial entity’s overall responsibility for the ICT services supporting critical or important functions provided by ICT third-party service providers, including ensuring effective monitoring, the written contractual agreement between the financial entity and the ICT third-party service provider shall enable the financial entity’s effective monitoring of the contracted ICT services in accordance with Article 30(3) point (a) of Regulation (EU) 2022/2554. The contractual arrangements shall in particular include elements enabling the financial entity to fulfil its obligation to monitor the ICT risk that may arise in relation to its use of ICT services provided by subcontractors providing ICT services supporting critical or important functions, in **particular those that effectively underpin the provision of ICT services supporting critical or important functions or material parts thereof**. The monitoring referred to in the second subparagraph may, where appropriate, rely on information provided by the ICT third-party service provider. “

Tijdens het volgende webinar op 7 november a.s. zullen we de draft van het Information Register verder bespreken.

V: En hoe vaak krijgen wij een reguliere update van het informatieregister?
A: Minimaal jaarlijks of zodra er een wijziging is.

V: In de dienstverleningsovereenkomst is een bijlage 'Incident management & Regieorganisatie' bijgevoegd. Wordt deze bijlage nog aangepast aan DORA?
A: dergelijke bijlagen worden onderdeel gemaakt van de security agenda en zullen jaarlijks worden bekeken. In de huidige opzet is incident management en regie losgekoppeld.
(Overige) wijzigingen in de huidige bijlagen worden niet voorzien.

Onderliggende - interne - processen zullen worden aangepast aan de huidige tijdslijnen zoals voorgeschreven onder DORA (en ook NIS2). Voorzien is dat dit gereed zal zijn in november/december 2024.

V: In artikel 14.3 lid g. staat dat kosten die gemaakt worden voor audits door toezichthouders voor rekening zijn van de opdrachtgever.
A: Correct, dit is conform ook de aangeleverde templates van de pensioenfederatie. Implementatie van DORA leidt potentieel tot additionele audits en daarmee aanvullende kosten die ten tijde van de totstandkoming van de overeenkomst niet althans onvoldoende voorzienbaar waren. Dergelijke kosten dienen in redelijk te worden toegekend aan de Financiële entiteiten op wie DORA direct van toepassing is. In hoedanigheid als Financiële entiteit. Indien een audit al dan niet betrekking heeft op meer klanten (lees de audit is productspecifiek en niet klantspecifiek) dan zal Visma Idella aansturen op deling van die kosten over de betrokken/geraakte klanten.

V: In het begeleidend schrijven stond: Naast het amendement kan het nodig zijn wijzigingen aan te brengen in contractbijlagen om te voldoen aan DORA, zoals bijvoorbeeld de Security bijlage of het Exit Plan. Als dat het geval is, neemt uw customer success manager hierover op een later moment contact op. Vraag: hoe weet ik of dit van toepassing is op onze organisatie en zo ja, wanneer neemt de customer success manager hierover contact op?
A: Wijzigingen in bijlagen - indien noodzakelijk zullen via de governance / Regie-organisatie kenbaar worden gemaakt. Het exitplan als onderdeel van de overeenkomst dient conform de DORA jaarlijks te worden herzien en geconcretiseerd. Visma Idella stuurt ook hierin op naleving van de overeengekomen governance.
In het amendement staat (...) Partijen zorgen ervoor dat het Exitplan:

- alomvattend en gedocumenteerd is, rekening houdend met de complexiteit van de Functies en de Transitie,
- realistisch en haalbaar is, gebaseerd op plausibele scenario's en redelijke aannames, en
- een gepland implementatieschema bevat dat verenigbaar is met de exit- en beëindigingsvoorwaarden die in dit Amendement en de Overeenkomst zijn vastgelegd.

Het huidige exitplan is reeds alomvattend, realistisch en haalbaar en omvat een verkort exit-schema. Op basis van het gestelde in artikel 15.2 van het amendement wordt gesteld "*de laatste versie van het Exitplan waar nodig te testen en herzien om te waarborgen en te bevestigen dat de Exitplannen toereikend zijn om een succesvolle Transitie te waarborgen*". Het herzien en testen moet ingepland worden (via de overeengekomen governance).

Visma Idella interpreteert de eis van DORA aldus dat de eerste herziening (en test) plaats dient te vinden in de periode 17.01.2025 - 17.01.2026, maar dat er vóór 17.01.2025 wel al een exitplan moet liggen die 'alomvattend, gedocumenteerd' is (artikel 28 lid 8 DORA). Dit laatste is dus reeds het geval.

Sidenote: het testen en reviewen van het exitplan is eerst mogelijk na volledige implementatie en live-gang van de dienst.

V: Wat wordt het vervolg in het kader van timing?
A: De contratering dient uiterlijk 17 januari 2025 gereed te zijn. Visma Idella stuurt aan op ondertekening voor 1 december 2024.

V: Zou je de keuze in artikel 7 kunnen toelichten? Hier staat dat de assistentie wordt verleend tegen redelijke kosten. Wat zijn redelijke kosten? Is dit nader te specificeren?

A: Redelijkheid (en billijkheid) is een open norm. De eisen zijn dan ook niet in abstracto te geven en mede afhankelijk van de omstandigheden van dat specifieke geval. In de eerste plaats moet het gaan om kosten die noodzakelijk zijn, waarna eveneens moet worden gekeken (indien die noodzaak er is) of de hoogte redelijk is. Medewerking na werktijd kan in redelijkheid leiden tot een hogere vergoeding dan medewerking gedurende kantooruren. Eea dient in dat geval uiteraard wel afgezet te worden tegen o.a. de positie van de persoon wier medewerking noodzakelijk is, het gebruikelijk uurtarief en/of bijvoorbeeld sprake is van spoed. Gezien het vorenstaande zullen wij de clausule als opgenomen in 7 niet verder abstraheren.

V: Geeft Visma Idella een In Control Statement af dat ze DORA compliant is?
A: Ja, uiterlijk op 17 januari 2025.

V: Wanneer wordt de Q&A en definitieve versie van het Amendement verstuurd? Timing is van belang om voor jullie deadline het Amendement voor akkoord op de juiste wijze door onze governance te laten gaan.
A: Uiterlijk in de week van 23 september 2024, waarbij een Track & Trace versie wordt verstrekt.

V: Verwacht Visma zelf in de toekomst direct onder toezicht te vallen?
A: Op dit moment zijn er nog geen concrete aanwijzingen om dit aan te nemen. Voor klanten waar Visma Idella de pensioenuitvoering doet, is er sprake van PUO Gericht Toezicht door DNB.

V: Kan er een actielijst opgesteld waaruit duidelijk wordt wat er allemaal nog gedaan moet worden om DORA compliant te zijn. Hieruit zou aangegeven kunnen worden wat Visma Idella doet, wat in gezamenlijkheid opgepakt moet worden en wat volledig bij het pensioenfonds ligt.
A: Intern hebben wij een fit gap-analyse gedaan en op basis daarvan zijn interne processen op de roadmap geplaatst voor wijziging, althans acties uitgezet. Het is aan de Financiële Entiteit zelf om op basis van de DORA voor eigen interne processen (als FE) eventuele acties te administreren. Het is goed in dit kader te benadrukken dat Visma Idella een ICT-leverancier is die kritieke en belangrijk processen ondersteunt en in dat kader proactief uitvoering geeft aan de verplichtingen uit de DORA, maar dat zij niet in staat is om namens de FE uitvoering te geven aan de DORA waar het de interne van de FE zelf betreft.

V: Kan deze actielijst onderdeel worden van de NFR-rapportage?
A: Een nadere toelichting op rapportages, waaronder de NFR zal worden toegelicht in het volgende webinar.

V: Wordt er bij het opstellen van de bedrijfsnoodplannen ook een verwijzing gemaakt naar/een link gelegd met ESG?
A: Wij herzien momenteel onze bedrijfsnoodplannen in het kader van DORA. Hierbij wordt geen expliciete link gelegd met ESG. Uiteraard worden wel onderdelen meegenomen in de onderliggende risicoanalyse. Denk hierbij bijvoorbeeld aan milieurampen of op het gebied van governance, het risico op datalekken en bijkomende mogelijke boetes.