
Deze meeting wordt opgenomen

# Amendement

Visma Idella B.V.
Corinna Angel, sr. Legal Counsel
Lilian Rolefes, Risk Officer
Gerwin Dirkzwager, Security Manager

**LEI-nummer: 724500693TLYPRVVPS58**

VISMA

# Agenda

| Onderwerp | Slide (#) |
|---|---|
| Achtergrond | 3 |
| Aanpak | 4 |
| Inhoud: te bespreken onderwerpen | 5 |
| Artikel 2, 3, 6, 7, 11, 12 en 13 | 6-16 |
| Vragen (overige) | 17 |
| Vervolg | 18 |

# Achtergrond

***D**igital **O**perational **R**esilience **A**ct* (Article 28 & 30)
⇒ implementatie uiterlijk per 17.01.2025

Template Amendement Pensioenfederatie (Kritiek / belangrijk)

- Marktstandaard*
  - brancheverenigingen DUFAS, VV&A, de Pensioenfederatie en het Verbond van Verzekeraars
- Input & Advies: Loyens & Loeff,  DNB, AFM

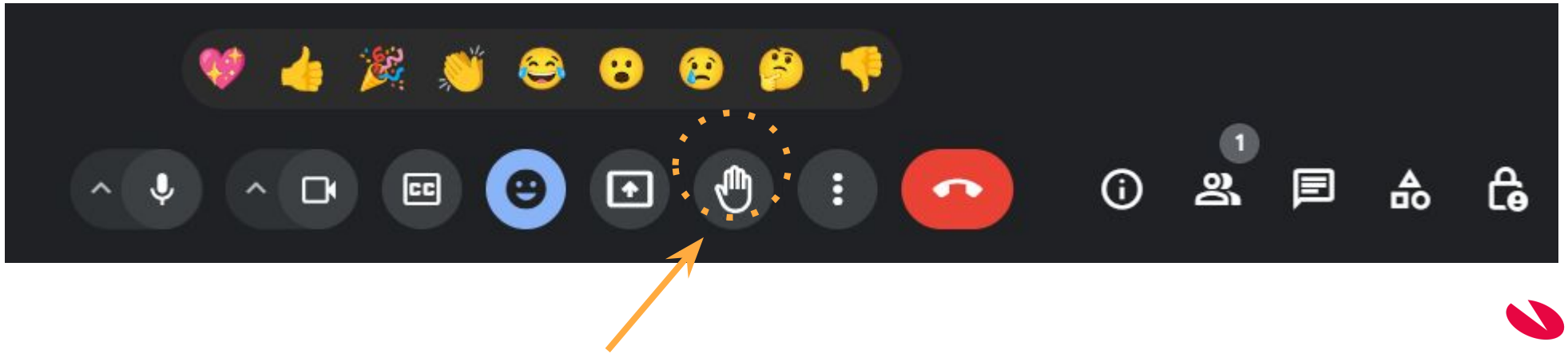
*www.verzekeraars.nl, www.pensioenfederatie.nl

VISMA

# Aanpak

Uw actieve deelname wordt gewaardeerd!

In deze call zijn de volgende disciplines aanwezig namens Visma Idella:
Legal, Privacy, Security, Customer Succes en Sales



# Inhoud

1. Definities en Interpretatie
2. Amendement
3. Functiebeschrijvingen en Uitbesteding
4. Locaties van Functies en Gegevensverwerking
5. Dienstenniveaus
6. Gegevensbescherming, Toegang, Herstel en Teruggave
7. Assistentie bij Incidenten
8. Samenwerking met Autoriteiten
9. Beëindigingsrechten
10. Deelname aan Training
11. Opzegtermijnen en Rapportageverplichtingen
12. Bedrijfscontinuïteit en ICT-Beveiliging
13. Testen
14. Monitoring
15. Exit
16. Vertrouwelijkheid
17. Diversen
18. Toepasselijk Recht en Jurisdictie

VISMA

# Algemeen

1. Open velden zijn in- en aangevuld (m.u.v. naam klant)
2. Bepaalde bepalingen zijn nader toegelicht en/of gespecificeerd
3. Artikel 16 ‘Wijziging’ is vervallen (was facultatief)
4. Terminologie (waar mogelijk) gelijk getrokken met Visma standaard(en)

VISMA

# Artikel 2

## Art. 2 - Amendement

1. Doel: voldoen aan gestelde in DORA

2. Rangorde: Artikelen 3 t/m 15 (exit) prevaleren boven gestelde in de Overeenkomst

3. Opgebouwde rechten: Niet van invloed op de opgebouwde rechten en verplichtingen van Partijen onder de Overeenkomst

VISMA

# Artikel 3

## Art. 3 - Functiebeschrijvingen en uitbestedingen

- Wijzigingsproces (3.3.c) & toezicht (3.3.f) (*'opties' toegepast)*
- Geldige Legal Entity Identifier (LEI) Kritieke Onderaannemers ( *gewijzigd*)
- 3.6: materiële tekortkoming (*Toegevoegd*))

# Artikel 3

## LEI (niet voor alle onderuitbesteders)

- *Taking a risk-based and proportionate approach, FEs are requested to ensure that all their **direct** ICT third-party service providers and all the subcontractors that **effectively underpinning ICT services supporting critical or important functions** that are legal person procure and maintain valid an LEI. This requirement should be explicitly included in all the contractual arrangements for the use of ICT services provided.*

VISMA

# Artikel 3

## Materiële Tekortkoming

3.6.iii (...) "*de [uitbestede] Functies materieel niet voldoen aan de door Opdrachtgever overeengekomen dienstenniveaus (Materiële Tekortkoming).* ***Een Materiële Tekortkoming wordt hierbij omschreven als een aanzienlijk falen, nalaten of tekortschieten in het nakomen van één of meer wezenlijke verplichtingen onder de Overeenkomst, zodanig dat het de fundamenten van de in de Overeenkomst vastgelegde afspraken dermate ondermijnt dat aan Opdrachtgever de gerechtvaardigde mogelijkheid dient te worden geboden om de overeenkomst, middels een schriftelijke mededeling aan Visma Idella, gedeeltelijk of geheel op te zeggen***."

# Artikel 6

## Art. 6 - Gegevensbescherming, Toegang, Herstel en Teruggave

- Documentatie en Onderhoud (*'opties' toegepast*):
  - Gegevensbeheer- en bedrijfsnoodplannen: in overeenstemming met Goede Industriepraktijken.
  - Doel: beschikbaarheid, authenticiteit*, integriteit en vertrouwelijkheid van klantgegevens te waarborgen.
  - Evaluatie: jaarlijks.
- Gegevensbescherming bij Bedrijfsbeëindiging (*gewijzigd*):
  - Behoud eigendomsrechten Klant is overgenomen.
  - 6.3 is aangepast aan werkwijze Visma Idella.

VISMA

# Toelichting

| | Identiteitsverificatie | Integriteit van gegevens | Bronauthenticiteit |
|---|---|---|---|
| **Disbursements** | Multi-factor authenticatie (MFA)<br>Rolgebaseerde toegang (RBAC)<br>Single Sign-On (SSO) | Versleuteling van gegevens at rest en in transit<br>Audit logs op wijzigingen via audit records in de database<br>SHA256 Hash / Checksums op gegevens. | File API voor aanleveren bestanden, alleen te gebruiken door geautoriseerde clients. |
| **VPaaS** | idem Disbursement +<br>DigiD voor deelnemers eHerkenning voor werkgevers | Idem Disbursement +<br>(Technical) events worden gelogd<br>Vastlegging van procesverwerking in process logs | Verificatiestappen: afgedwongen<br>PKI koppelingen met externe systemen |
| **DPaaS** | Idem VPaaS+<br>Gedelegeerde toegang tot Gedeelde mailboxen<br>Gedelegeerde toegang tot shared drives (op basis van least privilege) | Idem VPaaS +<br>Versiebeheer op documenten<br>Vastlegging contactmomenten in CRM | Idem VPaaS +<br>Verificatiestappen / controlevragen in processen<br>Vaste contactpersonen bij fondsen / werkgevers. |

VISMA

# Artikel 7

## Art. 7 - Assistentie bij Incidenten

- *‘optie’ toegepast*
- *Kosten*: Voorwaarden gespecificeerd waaronder kosten in rekening worden gebracht of juist niet.

# Artikel 11

## Art. 11 - Rapportageverplichting

Art. 30.3.b DORA: *kennisgevingstermijnen en rapportageverplichtingen van de derde aanbieder van ICT-diensten ten aanzien van de financiële entiteit, met inbegrip van de kennisgeving van ontwikkelingen die materiële gevolgen kunnen hebben voor het vermogen van de derde aanbieder om op doeltreffende wijze de ICT-diensten die kritieke of belangrijke functies ondersteunen te leveren in overeenstemming met de afgesproken dienstverleningsniveaus;".*

- Periodieke Rapporten: ingevuld
  - het op verzoek aanleveren van aanvullende informatie dat niet vereist is vanuit DORA is niet overgenomen.
- Incidentmelding: overgenomen
  - *Call for action: controle van contactgegevens.*

VISMA

# Artikel 12

## Art. 12 - Bedrijfscontinuïteit en ICT-beveiliging

- **Onderwerpen:**
  - Bedrijfsnoodplannen
  - ICT-Beveiliging & (kritieke) kwetsbaarheden
  - Evaluatie
  - Klantcommunicatie
  - Certificeringen: ISO/IEC 27001 en ISAE 3000/3402
- **‘opties’ toegepast en  periodiciteit gespecificeerd**
- **Kosten:** Voorwaarden gespecificeerd waaronder kosten in rekening worden gebracht of juist niet.

# Artikel 13

## Art. 13 - Testen

- UPDATE:
- 13.2 *“Visma Idella zal deelnemen en volledig meewerken aan dreigingsgestuurde penetratietesten (TLPT) van Opdrachtgever zoals bedoeld in artikel 26 en 27 van DORA (indien en voor zover van toepassing op Opdrachtgever).”*
    - Final report on draft RTS on TLPT: Pensioensector is niet **meer** benoemd als  entiteit die Threat-Led Penetration Testing (TLPT) moet uitvoeren.

# Vragen

# Vervolg

1. Toch nog een vraag/opmerking?
    a. Stel deze tijdig en bij voorkeur schriftelijk aan uw CS-manager voor 30-09-2024
2. Onderteken (vóór 31-10-2024)
    a. ‘nat’ ⇒ ondertekening klant ⇒ scan ⇒ mail aan uw CS- manager ⇒ ondertekening Visma Idella ⇒ mail klant ⇒ archiveer
    b. ‘digitaal’⇒ geef mailadres tekeningsbevoegde(n) door aan uw CS-manager ⇒ u ontvangt een melding van VismaSign voor ondertekening ⇒ onderteken ⇒ archiveer

VISMA