Visma Idella B.V.

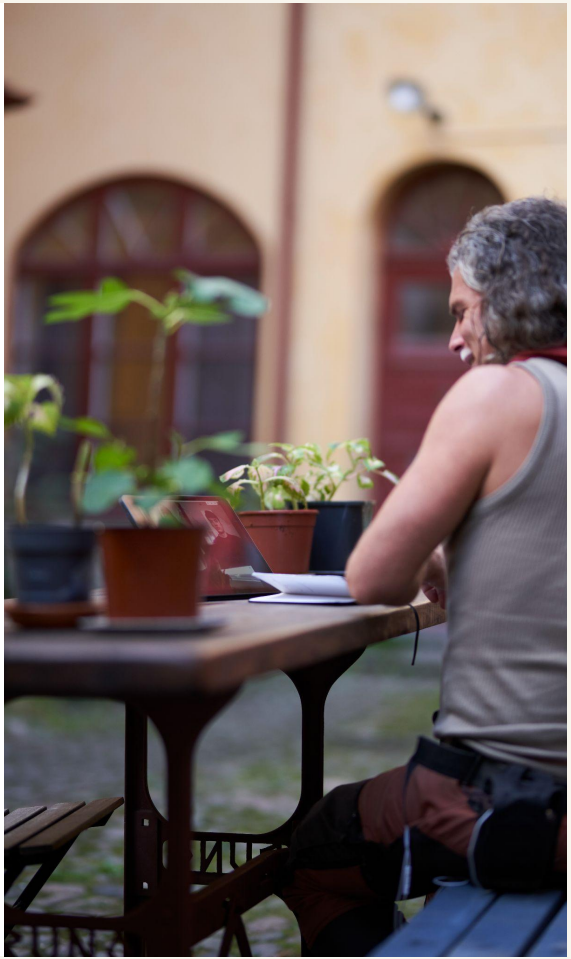
In Control met DORA

Dit webinar wordt opgenomen!

7 november 2024

Silviu Fulga *Information Security Manager* (Visma Software Int. AS)
Lilian Rolefes *Risk Manager*
Corinna Angel *sr. Legal Counsel & Data Protection Manager*
Gerwin Dirkzwager, *Security Manager*

VISMA | idella



Corinna ANGEL
corinna.angel@visma.com

Silviu FULGA
silviu.fulga@visma.com

Gerwin DIRKZWAGER
gerwin.dirkzwager@visma.com

Lilian ROLEFES
lilian.rolefes@visma.com

Inhoud

1. Introductie
2. Contracting - Amendement 2.0
3. Register of Information
4. Threat Lead Penetration Testing (TLPT)
5. Aan het woord: Visma Software International AS (in het Engels)
6. Vooruitblik
7. Vragen

1. Introductie

3 blokken

- Blok 1: DORA-Amendement en Informatie-
- register
- Blok 2: TLPT/Visma Software International
- Blok 3: Vooruitblik / afsluiting (vragen)

Na elk blok behandelen we binnengekomen vragen.

1. Introductie

Corinna Angel

- Sr. Legal Counsel
- Data Protection Manager
- Lid Regulatory Guild
- Lid Information Security Board

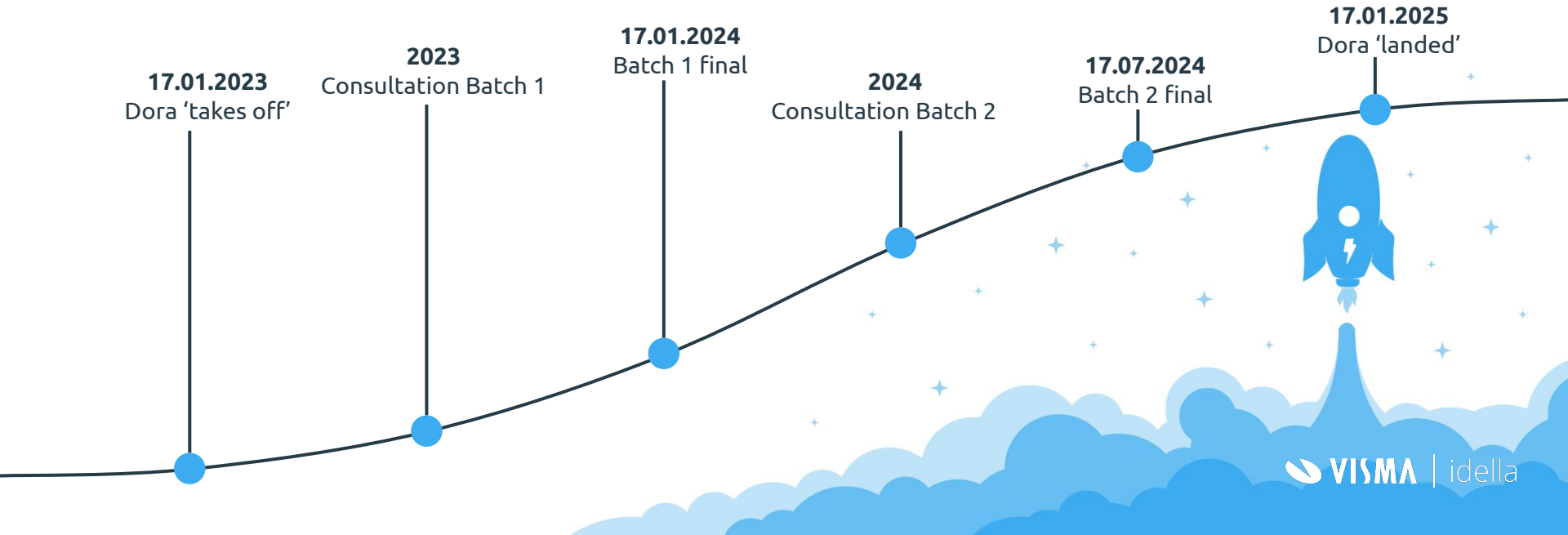
Gerwin Dirkzwager

- Security Manager
- Voorzitter Information Security Board

Silviu Fulga

- Information Security Manager SwInt

1. Introductie



2. Contracting - Amendement 2.0

2. Contractering - Amendement 2.0

Pensioenfederatie amendement 2.0

1. Wijzigingen
    a. Dienstenniveaus
        i. Servicelocaties (*update / aanscherping*)
        ii. Monitoring onderaannemers (*update / aanscherping*)
    b. Locaties van Functies en Gegevensverwerking (Clausule 4):
        i. Service- en gegevensopslaglocaties moeten schriftelijk worden vastgelegd. Wijzigingen in deze locaties vereisen schriftelijke kennisgeving en soms toestemming van de klant.

2. Wettelijke grondslag wijzigingen: *must have vs nice to have*

3. Amendement Visma Idella 2.0
    a. Toegezonden (*niet ontvangen, mail uw CS-Manager)*
        i. Opname wijzigingen Pensioenfederatie (mits wettelijke grondslag aanwezig)
        ii. Nuancering opzegtermijnen (artikel 9).

Artikel 30.2 Dora

The contractual arrangements on the use of ICT services shall include at least the following elements: (h) ***termination rights*** *and related* ***minimum notice periods*** *for the termination of the contractual arrangements,* ***in accordance with the expectations of competent authorities and resolution authorities****;*

VISMA | idella

2. Contractering - Amendement 2.0

Pensioenfederatie amendement 2.0

1. **Waarom** nuancering opzegtermijnen (artikel 9).
   a. Art. 34 PW jo artt. 12 t/m 14 Besluit uitvoering Pensioenwet en Wet verplichte beroepspensioenfonds:
      i. Geen plicht tot opname directe opzegging (‘***de wijze waarop*** *de overeenkomst wordt beëindigd (…)*”)
   b. Artikel 30.2 Dora: *“The contractual arrangements on the use of ICT services shall include at least the following elements: (h) termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities;”*
      i. Geen plicht tot opname directe opzegging (= maximum geen minimum)
      ii. Verwachtingen DNB zijn nog niet bekend, zie o.a. onderstaande melding.

> Deze DNB-beleidsuiting wordt momenteel opnieuw door DNB beoordeeld in het licht van de Digital Operational Resilience Act (DORA) die met ingang van 17 januari 2025 van kracht wordt voor de financiële sector. Mogelijk wordt deze beleidsuiting aangepast of ingetrokken. De beleidsuiting blijft tot het moment van een eventuele herziening of intrekking van toepassing. Nadere informatie over DORA is te vinden op (inclusief periodieke verschijnende nieuwsberichten): www.dnb.nl/DORA

2. Contractering - Amendement 2.0

Uiterlijk op 30 november 2024 dienen alle eventuele opmerkingen t.a.v. het amendement te zijn ontvangen.

3. Register of information

3. Register of Information (1)

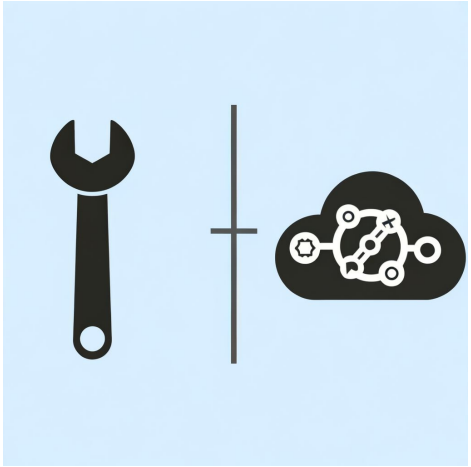
Vooraf

De Europese Commissie moet het Informatieregister nog definitief vaststellen!
(zie https://www.pensioenfederatie.nl/website/themas/pensioenuitvoering/dora)

		Concept advies toezichthouders	Definitief advies toezichthouders	Vaststelling Europese Commissie	Publicatie in Europees Staatsblad
Eerste set	RTS ICT-risicomanagementkader	√	√	√	√
	RTS Incidentclassificatie	√	√	√	√
	RTS Uitbestedingsbeleid	√	√	√	√
	ITS Informatieregister	√	√	Q4 2024?	Q4 2024?
Tweede set	Richtsnoer Kostenschatting	√	√	Niet nodig	Niet nodig
	RTS Incidentrapportage	√	√	√	December 2024
	ITS Incidentrapportage	√	√	√	December 2024
	RTS Testen (TLPT)	√	√	Q4 2024?	Q4 2024?
	RTS Onderuitbesteding	√	√	Q1 2025?	Q1 2025?

VISMA | idella

3. Register of Information (2)



Vooraf

Rol van Onderaannemers:

- Diversiteit in Onderaannemers:
  1. *Support en Tool Leveranciers*
  2. *Full Data Processors:*
- Onderscheid in Onderaannemers:
  3. Tooling Leveranciers (niet kritieke Onderaannemers):
     a. **Functie**: Zij leveren technologieën en software die wij bv intern gebruiken voor efficiënte dienstverlening. Er is sprake van beperkte data-interacties,
     b. **DORA-impact:** Zij vallen onder de brede definitie van ICT-dienstverleners, maar worden door ons niet als 'kritiek' geclassificeerd, wat betekent dat zij onder een lichter toezicht- en monitoringsregime vallen.
  4. Full data Processors (Kritieke Onderaannemers):
     a. **Functie**: Kritieke onderaannemers verwerken volledige klantbestanden en/of zijn essentieel bij het leveren van de kritieke Functies.
     b. **DORA-impact:** Deze partijen zijn o.a. Onderworpen aan uitgebreide monitoring en toezicht verplichtingen.

3. Register of Information (3)

Register of Information

Een eerste concept zal worden gedeeld in de week van 11 november 2024

Aandachtspunten

- Hover over kolommen om extra informatie te zien
- Het betreft over-all register:
  - niet klantspecifiek

VISMA | idella


Vragen?
VISMA | idella

4. TLPT - update

4. Threat Led Penetration Testing (TLPT) - update (1)

- Pensioenfondsen zijn op basis van de final RTS tekst (17 juli 2024) niet expliciet vereist TLPT uit te voeren, maar gezien hun belang kunnen nationale regelgevingen of bredere EU-regelgevingen dit alsnog vereisen of aanmoedigen.
  Op dit moment neemt Visma Idella het standpunt in dat er geen vereiste is om TPLT uit te voeren, maar zal meewerken indien er klanten zijn die hieraan moeten voldoen.

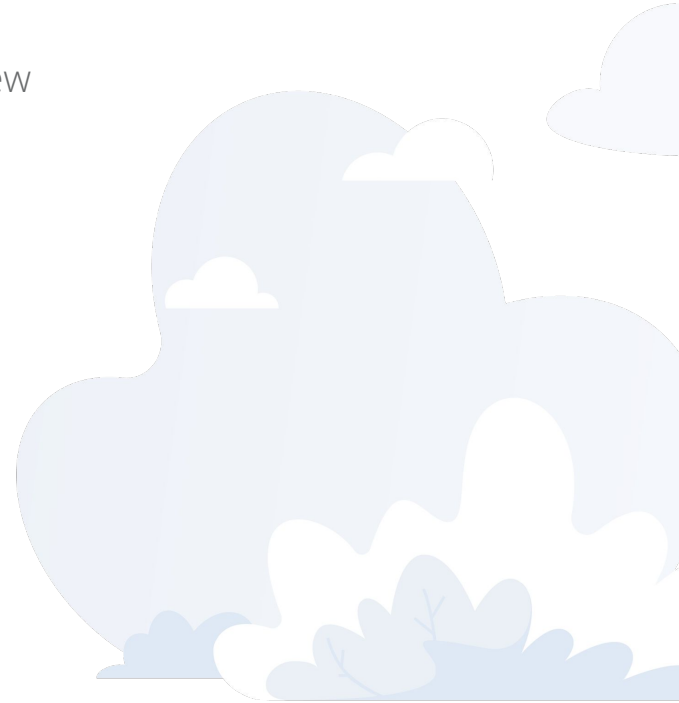
4. Threat Led Penetration Testing (TLPT) - update (2)

- ➔ De regelgeving staat ook het gebruik van interne testers toe, mits zij voldoen aan strenge eisen betreffende bekwaamheid, onpartijdigheid, en effectiviteit, en dat hun inzet geen negatieve invloed heeft op de ICT-verdedigings- of weerbaarheidscapaciteit van de financiële entiteit.
  Visma onderzoekt wat er nodig is voor het security team om hieraan te voldoen en of dit ingezet zal worden.

5. Visma IT&C B.V./ Visma Software International AS

Agenda

- Visma IT&C BV and Visma Software International AS overview
- Services Overview
- Group wide cybersecurity services
- Compliance driven approach



VISMA | idella

Visma IT&C BV and Visma Software International AS overview

Both legal units offer Group wide services to Visma companies, including Visma Idella.

From a hosting perspective, we offer both traditional data center hosting services as well as Visma managed private cloud solutions (eg. Azure Private Cloud).

Last but not least, we also help our customers manage their solutions in Public Cloud environments.

Services Overview

- **Internal IT services** - user facing services for Idella employees:
  - Service desk
  - Local support
  - Identity and access management
  - Google Workspace services
  - Client VPN
  - Office Network as a Service
  - Endpoint Management
- **Data Center and Infrastructure (DCI) services** - hosting services
  - Cloud Services Brokerage
  - Public and Private Cloud: Microsoft Azure, AWS, GCP
  - Server Management
  - Monitoring
  - Centralized Logging System
  - SSL/TLS Certificates
  - Citrix infrastructure services
  - Storage as a service
  - Business Continuity as a Service

Both types of services are covered by Visma Group's cybersecurity services.

Group wide cybersecurity services

- Bug Bounty programs
- Cyber Threat Intelligence
- Dynamic Application Security Testing (DAST)
- Static Application Security Testing (SAST)
- Endpoint Protection
- External Attack Surface Mapping
- Penetration Test
- Security Log Management
- Software Composition Analysis
- Highly trained and experienced GSOC team

Compliance driven approach

Commitment to Compliance and Security:

- **Customer-centric compliance:** We prioritize compliance with our customers' regulatory requirements, adapting our services to meet specific directives and regulatory requirements
- **Alignment with Regulatory Frameworks:** Our services are designed to support compliance with European and global regulatory frameworks, including NIS2, GDPR, and sector-specific frameworks such as DORA.

Adhering to the Good Practice Information Security provisions (DNB)

- We fully align with the Good Practice Information Security provisions issued by De Nederlandsche Bank (DNB), ensuring our security measures meet the highest standards.

Our certifications and assurance reports: ISO 9001, ISO 14001, **ISO 27001, ISAE 3402** and **ISAE 3000**


Vragen?
Questions?
VISMA | idella

6. Vooruitblik

Planning (onder voorbehoud)

Voorjaar:
- Kennissessie 2 (juni*) ✅
- Mapping DNB GP Informatiebeveiliging 2023 ✅
- DNB Security Self Assessment ✖
- ISO27001 (re-audit) ✅

Zomer:
- ~~Kennissessie 3 (september*)~~
- Vaststelling beleid en processen **eerste** batch (1.0) ✖
- Oplevering contractuele wijzigingen bestaande klanten ✅
- Herijking afspraken kritieke leveranciers (0.7) ✅
- ISO27001-2022 mapping/overige assurance ✅
- ICT informatieregister (0.8) ✖

*digitaal

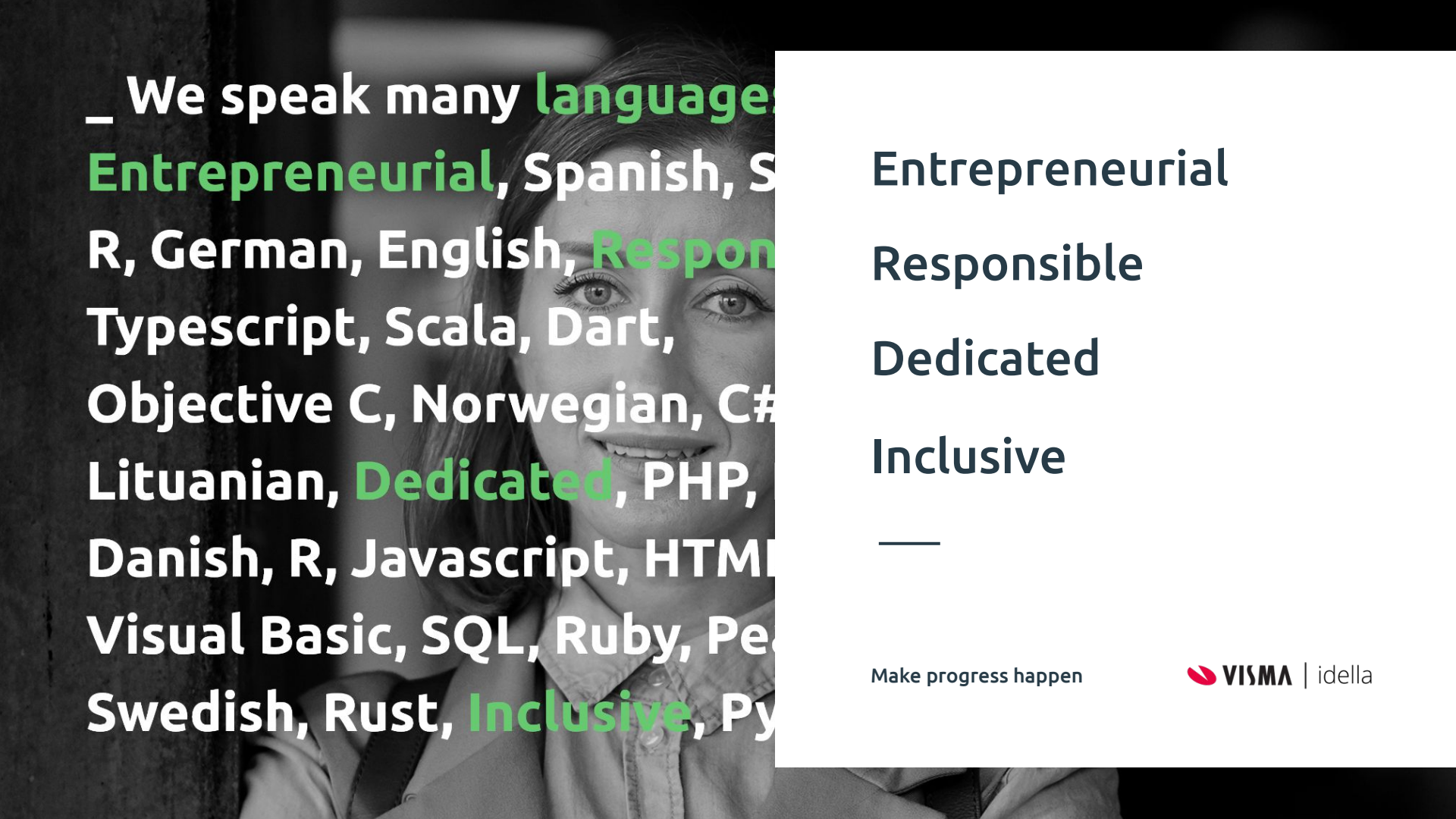
Najaar:
- Kennissessie 4 (november*) ✅
- 0.9 vaststelling beleid en processen **tweede** batch
- Afronding contractuele wijzigingen
- Herijking afspraken kritieke leveranciers (1.0)

Winter:
- Vaststelling beleid en processen **tweede** batch (1.0)
- Oplevering Informatieregister (1.0)
- Feestelijke afronding DORA + kennissessie
  - Locatie: Amersfoort
  - Datum: volgt plus tijdstip

7. Afsluiting

VISMA | idella


Vragen?
VISMA | idella



Entrepreneurial

Responsible

Dedicated

Inclusive

Make progress happen

VISMA | idella