DEEL 1: DATA PRO STATEMENT

Dit Data Pro Statement vormt samen met de dienstverleningsovereenkomst van Visma Raet voor verwerkingen de basis voor de verwerkersovereenkomst voor het product of de dienst van het bedrijf dat dit Data Pro Statement heeft opgesteld.

ALGEMENE INFORMATIE

1. **Dit Data Pro Statement is opgesteld door de volgende data processor (verwerker):**
   Visma Raet BV
   Plotterweg 38
   3821 BB Amersfoort

   Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met: *privacy.raet@visma.com*

2. **Dit Data Pro Statement geldt vanaf *1 maart 2022; en betreft versie 3***
   Dit Data Pro Statement en de daarin omschreven beveiligingsmaatregelen past Visma | Raet regelmatig aan om ten aanzien van dataprotectie steeds voorbereid en actueel te blijven. Visma | Raet houdt u op de hoogte van nieuwe versies via onze website https://www.vismaraet.nl/trust de standaard verwerkersovereenkomst kan gevonden worden via https://www.vismaraet.nl/avg

3. **Dit Data Pro Statement is van toepassing op de volgende producten en diensten van data processor:**
   e-HRM diensten op basis van SaaS platformen (zoals Youforce en Visma.net HR en Payroll) en HR Services.

4. **Omschrijving product/dienst**
   Visma | Raet is een HR-softwareleverancier die met cloudoplossing organisaties ondersteunt bij het digitaliseren van hun HR-processen, het zogeheten e-HRM. Daarnaast biedt Visma | Raet oplossingen voor talent management, workforce management en HR analytics. worden andere vormen van HR dienstverlening aangeboden zoals interim services en HR en Payroll outsourcing.

   Het hoofdkantoor van Visma | Raet staat in Amersfoort en bedient de markten Overheid, Zorg en Welzijn, Onderwijs en Zakelijke Markt. Naast de directe dienstverlening worden diensten aangeboden als leverancier (subverwerker) van organisaties die gebruik maken van onderdelen van het Visma | Raet SaaS productaanbod.

5. **Beoogd gebruik**
   Producten en diensten zijn ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:

Visma | Raet verwerkt gegevens gerelateerd aan HR- en salarisdienstverlening zoals gespecificeerd in de bijlage 1 van de Visma | Raet standaard verwerkersovereenkomst en de met de klant overeengekomen dienstverleningsovereenkomst.

Bij de privacy maatregelen in producten en diensten is rekening gehouden met de verwerking van bijzondere persoonsgegevens (zoals gegevens betreffende verzuim) of door de overheid uitgegeven persoonsnummers (zoals BSN).

6. **Data processor heeft bij het ontwerpen van het product/de dienst *privacy by design/privacy by default* op de volgende wijze toegepast:**
Visma | Raet ontwikkelt software op basis van Non Functional Requirements voor veilige software ontwikkeling. Hier maken o.a. bestaande standaarden en best practises deel van uit. Zoals: OWASP top 10, SANS en NCSC. Software wordt vooraf getoetst op basis van functionele, technische en privacy aspecten. Er wordt getest op kwetsbaarheden voordat de software beschikbaar gesteld wordt aan de eindgebruikers. Bij het leveren of implementeren van software wordt standaard voorzien in privacy vriendelijke instellingen.
Er zijn een dertigtal niet-functionele eisen, richtlijnen en/of aanbevelingen geïmplementeerd die specifiek voor softwareontwikkeling zijn vastgesteld op basis van de aanbevelingen van de Autoriteit Persoonsgegevens.

   Deze eisen zijn gecategoriseerd als:
   - Doel, minimalisering en proportionaliteit
   - Gegevens verwijderen
   - Gegevens exporteren en retourneren
   - Gegevens herstellen
   - Klantenbegeleiding
   - Geautomatiseerde besluitvorming
   - Pseudonimisering en anonimisering
   - Toestemming van betrokkene

   Deze vereisten en aanbevelingen variëren van het simpele "heeft het sollicitatieproces alleen de minimale persoonlijke gegevens die nodig zijn om te functioneren" en of rollen in het systeem kunnen worden geconfigureerd om alleen toegang te hebben tot relevante gegevens, tot complexere en specifieke vereisten voor het verwijderen van gegevens wanneer een klantrelatie wordt beëindigd, en methodologische richtlijnen voor verschillende anonimiseringstechnieken.

7. **Data Processor gebruikt NIET de Standaardclausules voor verwerkingen, maar gebruikt in plaats daarvan de *Visma | Raet Verwerkersovereenkomst,* die als bijlage bij de Overeenkomst aangeboden wordt.**
De standaard verwerkersovereenkomst is tevens beschikbaar via **https://www.vismaraet.nl/over-ons/system-privacy-security/avg/avg-agreement/**.

8. **Data Processor verwerkt de persoonsgegevens binnen de EU/EER. De Data processor heeft op de volgende manier geborgd dat een passend beschermingsniveau van toepassing is:**
Visma | Raet hanteert als uitgangspunt dat gegevens alleen binnen de EER worden verwerkt. In het uitzonderlijke geval dat dit niet mogelijk is zal Visma | Raet zal zich houden aan de vereisten van de wetgeving inzake bescherming van Persoonsgegevens van de Europese Economische Ruimte (hierna: de EER) betreffende Verwerken van Persoonsgegevens uit de EER. Verwerker zal erop toezien dat overdrachten van Persoonsgegevens naar een land buiten de EER of een internationale organisatie, een land betreft zoals beschreven in artikel 45 van de AVG of onderworpen zijn aan passende veiligheidsmechanismen, zoals beschreven in artikel 46 van de AVG, en dat dergelijke overdrachten en veiligheidsmechanismen worden gedocumenteerd overeenkomstig artikel 30, lid 2 van de AVG. In het geval dat er Persoonsgegevens buiten de EER worden Verwerkt op basis van de modelcontracten (zoals bedoeld in artikel 46 lid 2 of 3 AVG), machtigt de klant Visma | Raet om deze namens haar overeen te komen.

9. **Data processor maakt gebruik van de volgende sub-processors:**
Visma | Raet publiceert informatie over data locatie en de sub-processors via de website https://www.vismaraet.nl/over-ons/system-privacy-security/privacy/.
Details zijn opgenomen onder de knop: ‘Overzicht leveranciers in relatie tot Youforce’ of https://www.visma.com/trust-centre/transparency/ onder de in te geven Visma productnaam.

10. **Data processor ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**
Visma | Raet zal de klant (als zijnde verwerkingsverantwoordelijke) informeren over :
    - verzoeken van een betrokkene op grond van toepasselijke Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming; en
    - verzoeken van een overheidsinstantie, zoals de politie, op grond van toepasselijke Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming.

Visma | Raet zal niet reageren op verzoeken van betrokkenen (veelal medewerkers van de klant) zelf tenzij Visma | Raet daartoe gerechtigd is door de klant op basis van schriftelijke instructies of verplicht is krachtens toepasselijke wetgeving die van toepassing is op Visma | Raet als verwerker. In dit laatste geval zal Visma | Raet, voor zover toepasselijke wetgeving dit toestaat, de klant informeren over deze wettelijke verplichting voordat op het verzoek gereageerd wordt. Hetzelfde geldt voor verzoeken van overheidsinstanties.

Bovenstaande heeft alleen betrekking op de situatie wanneer een betrokkene zich meldt bij Visma | Raet. In zo’n geval zal Visma | Raet de betrokkene altijd verwijzen naar de verwerkingsverantwoordelijke en ook de verwerkingsverantwoordelijke hierover informeren.

Wanneer een betrokkene een verzoek indient bij de verwerkingsverantwoordelijke kan deze laatste veel, zo niet alle, gevraagde informatie via de aangeboden SaaS applicaties en/of de

trustpagina's van Visma | Raet achterhalen. Indien verwerkingsve de klant niet geheel kan voldoen aan het verzoek kan aan Visma | Raet gevraagd worden de ontbrekende informatie op te leveren. Het verzoek daartoe van de klant kan gericht worden aan de met de klant overeengekomen supportorganisatie.

11. **Data processor zal op de volgende wijze medewerking verlenen aan Data Privacy Impact Assessments:**
Informatie over de wijze van verwerken, subverwerker, verwerkingslocaties, beveiligingsmaatregelen en dergelijke wordt verstrekt via de trust websites www.vismaraet.nl/trust en www.visma.com/trust-centre.

Als opdrachtgever informatie of assistentie behoeft omtrent beveiligingsmaatregelen, documentatie, of overige (vormen van) informatie behoeft omtrent de wijze waarop Visma | Raet persoonsgegevens verwerkt, dan kan Visma | Raet de kosten van haar aanvullende diensten bij de opdrachtgever in rekening brengen overeenkomstig de tussen partijen aangegane overeenkomst(en) voor zover zulke verzoeken betrekking hebben op informatie die Visma | Raet niet standaard aan de opdrachtgever hoeft te verstrekken om te voldoen aan de op verwerker van toepassing zijnde privacy wetgeving.

12. **Na afloop of tussentijdse beëindiging van de Verwerkersovereenkomst zal Verwerker alle Persoonsgegevens binnen een redelijke termijn terug overdragen aan Verwerkingsverantwoordelijke en/of op verzoek van Verwerkingsverantwoordelijke vernietigen of verwijderen, inclusief alle (kopieën van) elektronisch vastgelegde Persoonsgegevens en schriftelijk bevestigen aan Verwerkingsverantwoordelijke dat alle Persoonsgegevens terug aan haar zijn overgedragen dan wel zijn vernietigd of verwijderd. Indien op Verwerker de wettelijke plicht rust om te blijven Verwerken, dan zal zij aan het verzoek van Verwerkingsverantwoordelijke voldoen voor zover zulks is toegestaan op grond van toepasselijke wet- en regelgeving. Op verzoek en op kosten van Verwerkingsverantwoordelijke zal Verwerker deze schriftelijke bevestiging voorzien van een gecertificeerde verklaring van een register IT-auditor.**

Op het moment dat de dienstverleningsovereenkomst eindigt, zal Visma | Raet de ten behoeve van de opdrachtgever verwerkte persoonsgegevens verwijderen of retourneren. Tenzij anders overeengekomen, zijn de daarmee gepaard gaande kosten gebaseerd op: i) uurtarieven voor bestede uren en ii) de complexiteit van de gevraagde actie.

Visma | Raet mag de persoonsgegevens na het eindigen van de overeenkomst bewaren, voor zover dit wettelijk is vereist, met inachtneming van dezelfde technische en organisatorische maatregelen zoals bepaald in de overeenkomst.

13. **[Optie niet toegepast]**

BEVEILIGINGSBELEID

14. **Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:**
Visma | Raet heeft het Informatiebeveiligings Management Systeem (ISMS) en het kwaliteitsmanagementsysteem gecertificeerd conform de internationale ISO 27001 en ISO 9001 normen voor "Ontwikkeling, levering, implementatie van producten en SaaS dienstverlening voor e-HRM, Payroll, Personele en Salarisadministratie en HR Services".
Meer informatie over het informatiebeveiligingsbeleid is beschikbaar via: https://www.vismaraet.nl/over-ons/system-privacy-security/security/ en de op verzoek te ontvangen Verklaring van Toepasselijkheid

15. **Data processor heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):**

- NEN-ISO 27001
- OWASP;
- BIO (Baseline Informatiebeveiliging Overheid)
- Microsoft Security Development Lifecycle
- NCSC Webrichtlijnen

16. **Data processor heeft de volgende certificeringen en rapportages:**

- Data Pro certificaat
- ISO 9001
- ISO 27001
- ISAE 3402 type 2

Sub-verwerkers hebben de certificaten zoals weergegeven op de trust sites van Visma en Visma | Raet

DATALEKPROTOCOL

17. **In geval er toch iets mis gaat, hanteert data processor het volgende datalekprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:**
In geval van een privacy incident of datalek stelt Visma | Raet de klant hiervan onverwijld in kennis na het constateren ervan. Om dit te realiseren, zorgt Visma | Raet ervoor dat alle personeelsleden in staat zijn, en blijven, om een datalek te constateren en verwachten wij van onze opdrachtnemers dat zij ons in staat stellen om hieraan te voldoen.
Meldingen van privacy incidenten door klanten kunnen primair gericht worden aan de servicedesk. Individuele medewerkers kunnen melding maken van incidenten bij hun werkgever. Derden kunnen gebruik maken van het email adres: security.raet@visma.com.
Voor nadere details zie:
https://www.vismaraet.nl/over-ons/system-privacy-security/privacy/meldplicht-datalekken/