Visma | Raet
In Control

Version 2023-12

“Als Visma | Raet in control is, ben jij in control.”

VISMA | raet

Inleiding

Als je bedrijfsprocessen volledig of gedeeltelijk uitbesteedt, wil je zeker weten dat dit beheerst en betrouwbaar gebeurt. Het algemene kwaliteitsniveau, de mate van informatiebeveiliging en privacy moeten voldoen aan jouw verwachtingen, de afgesproken dienstverlening en aan actuele wet- en regelgeving.

Met andere woorden, je wilt weten hoe Visma | Raet ‘in control’ is over de door jou uitbestede bedrijfsprocessen. Uitbesteding van werkzaamheden ontslaat je immers niet van je (eind) verantwoordelijkheid voor processen waar je geen directe invloed op hebt.

Visma | Raet staat al jaren bekend als een zeer betrouwbare partner voor de levering van ‘Software as a Service’ en aanverwante dienstverlening.

En als Visma | Raet ‘in control’ is dan ben jij ‘in control’.
In dit document lees je hoe wij dit invullen.

Visma | Raet ‘in control’

De dienstverlening van Visma | Raet heeft een sterke focus op risicobeheersing, informatiebeveiliging en compliance. Op basis van een robuust beheersraamwerk is het mogelijk op effectieve wijze risico’s te identificeren, beoordelen en te managen.

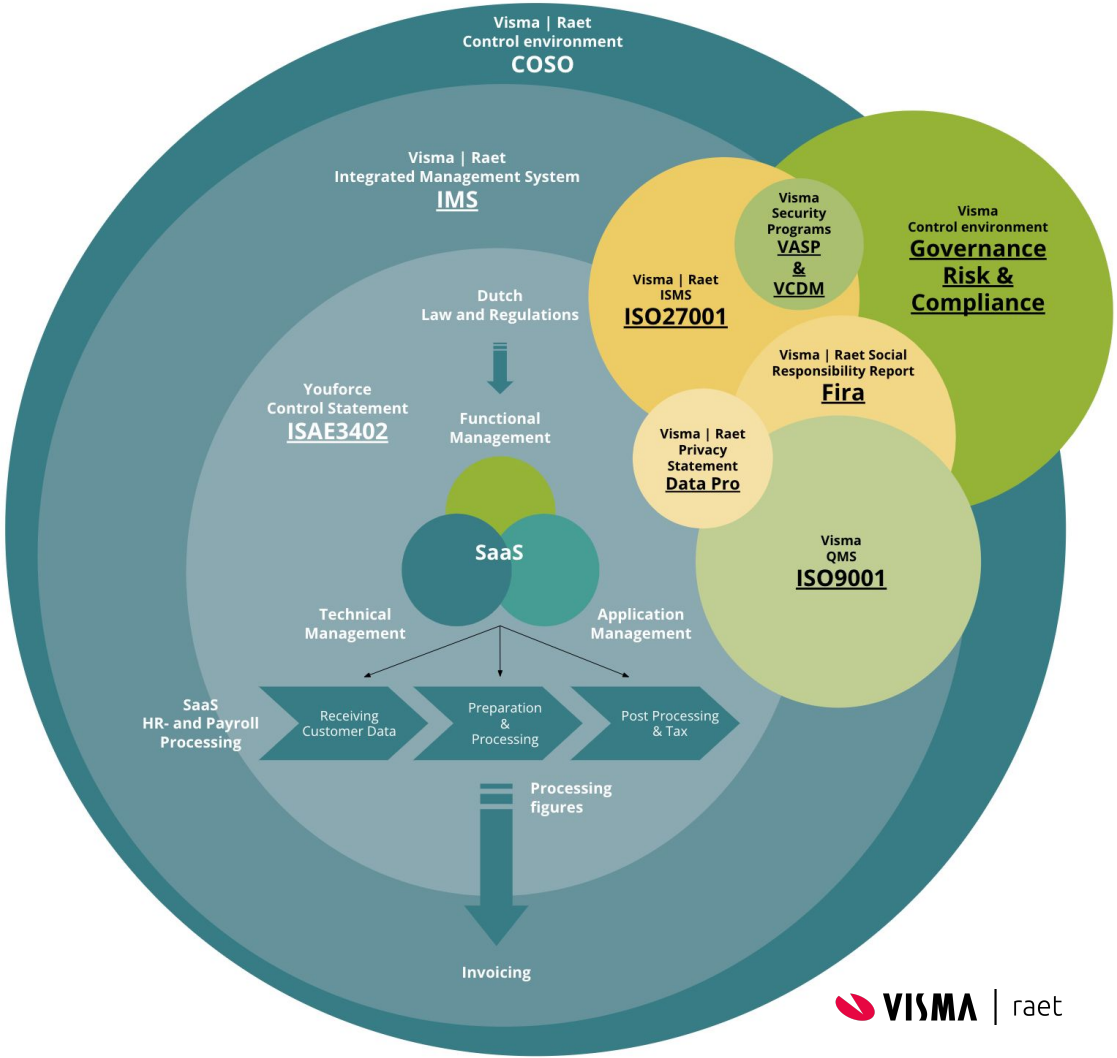
Visma | Raet heeft de aandachtsgebieden van de corporate governance van Visma, de ISO9001, ISO27001, Privacy standaarden en het Visma | Raet ISAE3402 raamwerk samengebracht in één managementsysteem.

Het Integrated Management System (IMS)
De afdeling Compliance Management beheerst en controleert dit geïntegreerde managementsysteem. Op de genoemde afdeling werken specialisten op het gebied van procesmanagement, informatiebeveiliging, privacy en kwaliteitsmanagement samen met de operationele- en stafafdelingen om de beheersbaarheid van de verwerking van je gegevens juist, tijdig, volledig en veilig te laten plaatsvinden.

Het IMS wordt beheerst volgens de plan-do-check-act cyclus om ervoor te zorgen dat de oorzaak van afwijkingen in de geleverde producten en diensten wordt weggenomen zodat herhaling wordt voorkomen, zowel in corrigerende als preventieve zin.

Interne en externe audits op basis van erkende standaarden worden gebruikt om de risico's te beheersen als om de werking van de ingestelde beheersmaatregelen te garanderen.

Geïntegreerd Management Systeem



VISMA | raet

Kwaliteit

VISMA | raet

Kwaliteit

De directie en de medewerkers van Visma | Raet onderkennen het belang van kwaliteit en streven continu naar een excellente en klantgerichte organisatie. Onder andere door de implementatie van kwaliteitsstandaarden en bedrijfsprocessen.

Het Visma | Raet kwaliteitssysteem is een geïntegreerd systeem bestaande uit meerdere management systemen. We noemen dit het Visma | Raet Integrated Management System.

Het systeem omvat onder andere: kwaliteitsdoelen, procesbeschrijvingen, rollen, taken, verantwoordelijkheden, beheersmaatregelen, procedures, werkinstructies, beleidsdocumenten, interne en externe audits op het gebied van de de beheersing van de reguliere operatie, informatiebeveiliging, privacy en overige interne en externe regelgeving.

Visma | Raet biedt hiermee aan haar relaties continu een hoog kwaliteitsniveau. Het kwaliteitssysteem borgt een goede afstemming tussen afdelingen onderling en is de basis voor permanente aandacht van verbeteren van werkwijze, producten en diensten.

Het algemene kwaliteitssysteem van Visma | Raet is sinds 1997 ISO9001 gecertificeerd en sinds 2022 geïntegreerd met het kwaliteitssysteem van Visma. De scope van dit kwaliteitssysteem omvat alle aangesloten producten, diensten en locaties van Visma zoals op het certificaat vermeld waaronder vanaf 2023 dus ook Visma | Raet.

De ISO90001 norm

In hoofdlijnen schrijft deze norm voor dat wij vastleggen hoe we de processen beheersen en de benodigde middelen beschikbaar stellen om onze producten en diensten volgens klanteisen te leveren. De norm vraagt ook om bewaking van processen, producten en diensten en een analyse van de resultaten zodat verbeteringen doorgevoerd kunnen worden.

De ISO9001 norm eist dat een organisatie:

- werkzaamheden gepland uitvoert;
- de productie beheerst uitvoert;
- de totstandkoming van producten en diensten bewaakt
- productfouten beheerst en problemen oplost;
- in de norm beschreven activiteiten als klachten en leveranciersbeoordeling registreert en afhandelt;
- invulling geeft aan in de norm vastgelegde processen en activiteiten;
- zorgt voor een kwaliteitsmanagementsysteem met relevante documenten;
- risico's identificeert en beperkt;
- voortdurend verbeteringen doorvoert.

Kwaliteitsbewaking

Het auditproces is een management-instrument voor onafhankelijke beoordeling en bewijsvoering dat aan bestaande eisen binnen de normering is voldaan. De audits evalueren de doeltreffendheid en doelmatigheid van de organisatie.

Een van de ISO-eisen is dat we zorgdragen voor de opzet van een doeltreffend en doelmatig auditproces om sterke en zwakke punten van het kwaliteitssysteem binnen onze organisatie te beoordelen.

Een goedlopend intern auditproces vormt de basis voor de externe audits. De afspraken over de kwaliteitsbewaking zijn vastgelegd in een auditbeleid.

Samen met geaccrediteerde partners worden periodiek interne- en externe audits uitgevoerd en bewaken we daarmee mede het niveau van het kwaliteitssysteem. Hiermee zorgen wij dat onze software en dienstverlening voldoen aan de serviceovereenkomsten en dragen wij zorg voor een correcte en veilige werking van de door ons geboden diensten.

Kwaliteitsverbetering

Het kwaliteitssysteem van Visma is digitaal vastgelegd en voor iedere medewerker toegankelijk. Dit ‘kwaliteitshandboek’ bevat onder andere de processchema’s, rollen, policies, richtlijnen en systemen met bijbehorende beschrijvingen.

Visma | Raet verbetert continu haar processen om klanten optimaal te bedienen en gemaakte afspraken na te komen. Bevindingen uit audits, klachten en resultaten van klanttevredenheidsonderzoeken zijn net als aanvullende informatie van managers en medewerkers belangrijke input voor procesverbeteringen voor meer effectiviteit en efficiëntie.

We streven voortdurend naar een optimale dienstverlening. Uiteraard kunnen we een kritische opmerking over onze producten of services niet uitsluiten. Ontvangen wij een klacht, dan doen we er alles aan deze zo snel en goed mogelijk af te handelen. Ons Service Center verzorgt de registratie en bewaakt de voortgang van de afhandeling. Afhankelijk van de ernst, handelt directie of management de klacht af.

Wij analyseren klachten en opmerkingen over diensten en producten met regelmaat om tot verbeteracties te komen.

Informatie-beveiliging

VISMA | raet

Informatiebeveiliging

Visma | Raet voelt zich verantwoordelijk maar is ook wettelijke verplicht om zorg te dragen voor een veilige dienstverlening. Hiermee zijn wij ook verantwoordelijk voor de beveiliging van gegevens van onze relaties. Dit wordt gestuurd met behulp van het Informatiebeveiligingssysteem (ISMS) en vastgelegd in een Informatiebeveiligingsbeleid.

In het informatiebeveiligingsbeleid staan vier begrippen centraal:

- **Integriteit** - Is de informatie geautoriseerd aangepast?
- **Beschikbaarheid** - Is de informatie op de afgesproken momenten beschikbaar?
- **Vertrouwelijkheid** - Hebben alleen mensen en systemen toegang tot de informatie met de juiste autorisaties?
- **Controleerbaarheid** - Weten we wie, wat, wanneer met de informatie heeft gedaan?

Het informatiebeveiligingsbeleid van Visma | Raet geldt voor al onze bedrijfsonderdelen, domeinen, omgevingen en locaties. Het management/de directie is actief betrokken bij de praktische invulling en uitvoering van het informatiebeveiligingsbeleid en neemt hier expliciet verantwoording in.

We eisen ook van leveranciers dat zij voldoen aan afdoende beveiligingsmaatregelen en zekerheid verschaffen met betrekking tot de bescherming van privacy gevoelige gegevens. Bijvoorbeeld door ook te voldoen aan de internationale standaard voor informatiebeveiliging ISO/IEC 27001.

VISMA | raet

De ISO27001 norm

Deze norm beschrijft hoe je procesmatig met het beveiligen van informatie omgaat. Bij Visma | Raet staan de beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid van de informatie van onze klanten voorop.

Het informatiebeveiligingsbeleid van Visma | Raet is opgesteld conform de meest recente internationale norm ISO27001.

In een beheersraamwerk, policies en richtlijnen beschrijven we hoe het beleid uitgevoerd wordt. Beleid, richtlijnen en maatregelen worden jaarlijks intern en extern getoetst.

We hebben voor de bewaking van het informatiebeveiligingsbeleid een gecertificeerde security officer aangesteld. Deze is adviserend, sturend en controlerend op het volledige gebied van informatiebeveiliging voor zowel klantinformatie als de eigen bedrijfsinformatie.

Binnen de software ontwikkelorganisatie zorgen security engineers voor de vertaling van het beleid in de software.

Continuïteit

Visma | Raet heeft als doel de integriteit en vertrouwelijkheid van informatie en IT-voorzieningen optimaal te borgen en onderbreking van de bedrijfsprocessen te beschermen tegen storingen of calamiteiten.

Hiervoor hebben wij een proces en plannen opgesteld met organisatiebrede uitgangspunten voor de aspecten die noodzakelijk zijn voor de continuïteit van de bedrijfsvoering.

We identificeren gebeurtenissen die bedrijfsprocessen en systemen kunnen onderbreken met periodieke en gestandaardiseerde risicoanalyses op basis van waarschijnlijkheid (kans) en gevolgen (impact). De risicoanalyses maken onderdeel uit van het risico beheersbeleid.

Maatregelen zijn getroffen voor de handhaving of het herstel van bedrijfsactiviteiten en het beschikbaar stellen van informatie na een onderbreking of uitval van cruciale systemen, medewerkers of bedrijfsprocessen.

Uiteraard testen we deze continuïteitsmaatregelen op regelmatige basis zodat ze actueel en doeltreffend blijven.

Toegang tot klantdata

Via onze systemen verwerken wij een grote hoeveelheid persoonsgegevens van klanten. Het gebruik van deze gegevens door Visma | Raet is conform ons informatiebeveiligingsbeleid aan sterke restricties gebonden. Wij beschikken alleen over deze data ten behoeve van de dienstverlening zoals in de dienstverlenings-overeenkomst en verwerkersovereenkomst overeengekomen met de klant.

Het gebruik van persoonsgegevens voor testdoeleinden is op basis van privacywetgeving niet toegestaan zonder gemotiveerde verwerkingsgrondslag. Visma | Raet gebruikt daarom geen bestaande persoonsgegevens voor testdoeleinden zonder uitdrukkelijke toestemming van de verwerkingsverantwoordelijke. We zullen alleen bestaande persoonsgegevens gebruiken indien er geen alternatieven mogelijk zijn.

Beveiligingsmaatregelen

Visma | Raet heeft organisatorische, fysieke, technische en procedurele maatregelen getroffen om de beveiliging van gegevens en diensten op het verwachte en vereiste niveau te houden. Ons beveiligingsbeleid is gebaseerd op gelaagdheid, waardoor één kwetsbaarheid niet kan leiden tot het schaden van de vertrouwelijkheid van de beheerde gegevens.

Een kleine greep uit het uitgebreide scala van beveiligingsmaatregelen op verschillende niveaus:

- Beveiligde kantoorruimte - Op basis van het toegangsbeleid is er alleen toegang tot de werkomgeving op basis van noodzaak en voor externen alleen onder begeleiding van een medewerker.
- Beveiligde datacenters - De door ons gebruikte systemen bevinden zich altijd in gecertificeerde en beveiligde datacenters met 24/7 bemanning, speciale toegangscontrole met paspoortcontrole en camerabewaking.
- Firewalls - De systemen zijn beveiligd door ‘firewalls’.
- Intrusion Detection - Het netwerkverkeer wordt voortdurend bewaakt op verdachte acties en geblokkeerd als dat nodig is.
- Beveiligde backups - In de private Cloudomgeving maken we iedere nacht backups die we versleuteld op een andere, beveiligde, locatie bewaren. In de publieke Cloudomgeving maken we gebruik van de faciliteiten van het datacenter voor de opslag van backups op een andere fysieke locatie.
- Gespiegelde data - Gegevens worden continu van het datacenter gekopieerd naar uitwijklocaties.
- Beveiligde verbindingen - Gebruikers hebben alleen toegang tot applicaties via beveiligde verbindingen en versleuteld datatransport. Data op personal devices is versleuteld.

- Complexe wachtwoorden en uitgebreide controle - We verplichten gebruikers geen eenvoudig te achterhalen wachtwoorden te gebruiken. Gebruikers die herhaaldelijk een onjuist wachtwoord invoeren, worden automatisch geblokkeerd. De gelukte en mislukte aanmeldpogingen worden gelogd.
- Versleuteling wachtwoorden - Wachtwoorden worden versleuteld opgeslagen.
- Beveiligingsspecialisten - Visma en Visma | Raet hebben professionele medewerkers in vaste dienst met volledige focus op informatiebeveiliging.
- Regelmatige controle - Interne auditors en gespecialiseerde bedrijven testen voortdurend alle beveiligingssystemen.
- Continue monitoring - Samen met gespecialiseerde bedrijven controleren wij het dataverkeer van en naar de datacenters 24/7 op ‘afwijkend’ gedrag. Indien nodig grijpen wij direct in.
- Logging - We loggen toegang en gebruik van systemen zodat forensisch onderzoek mogelijk is bij vermoeden van misbruik.
- Viruscontrole - De systemen worden beschermd tegen misbruik door malware en virussen.
- Meer factor authenticatie - Naast het verkrijgen van toegang tot de systemen via gebruikersnaam en wachtwoord verplicht Visma | Raet 2 factor authenticatie of Single Sign-on oplossingen.

Penetratietest

Een penetratietest, of intrusion detection test, is een controle uitgevoerd door zowel Visma en Visma | Raet als door gespecialiseerde organisaties, ook wel ethical hackers genoemd. Gezamenlijk zetten wij al onze kennis van IT-kwetsbaarheden in om informatiesystemen en infrastructuren te testen op veiligheid.

Wij voeren voor al onze SaaS-oplossingen regelmatig penetratietests uit. Minimaal een keer per jaar worden externe penetratietests uitgevoerd. Na grotere functionele of technische aanpassingen in software of infrastructuur voeren we aanvullende penetratietests uit op basis van een risico inschatting.

De details van de resultaten van deze tests zijn niet openbaar, maar de security officer classificeert en registreert mogelijke kwetsbaarheden als security issue en handelt ze vervolgens af. Elke constatering van een risico voor de veiligheid van informatie is voor ons aanleiding direct maatregelen te treffen.

Om te voorkomen dat we blind varen op één externe partij laat Visma | Raet de tests uitvoeren door verschillende organisaties.

Zie voor details en de meest recente informatie ons infosheet: Penetratietests

Standaarden

Visma | Raet implementeert eigen en relevante marktstandaarden voor de beveiliging van privacygevoelige gegevens. Al onze beveiligingsmaatregelen passen binnen de kaders van deze standaarden.

Een greep uit de gebruikte standaarden en best practices:

- ISO27001 - De ISO standaard voor informatiebeveiligingssystemen.
- ISO27002 - Overzicht van met richtlijnen voor informatiebeveiligingsmaatregelen.
- ICT-beveiligingsrichtlijnen voor webapplicaties - Documentatie van het Nationaal Cyber Security Centrum (onderdeel van ministerie van Veiligheid en Justitie) met beveiligingsrichtlijnen voor ontwikkeling en deployment van webapplicaties.
- OWASP top 10 - Het Open Web Application Security Project (OWASP) heeft een lijst opgesteld met de tien grootste beveiligingsrisico's voor webapplicaties.
- Microsoft SDL and the CWE/SANS Top 25 - Een door Microsoft samengestelde lijst van de 25 meest gevaarlijke programmeerfouten en kwetsbaarheden bij softwareontwikkeling.
- Visma Security Programma (VSP) - Visma's eigen security model voor het toetsen van de beveiliging en privacy van Cloud Software.
- Visma Cloud Development Methodiek - Het secure development programma van Visma.
- BIO richtlijnen - Baseline Informatiebeveiliging Overheid (BIO) is een normenkader voor de beveiliging van de informatiehuishouding van de Overheid.
- Richtsnoeren beveiliging persoonsgegevens - Nadere invulling van 'passende' beveiligingsmaatregelen over privacywetgeving.
- NCSC Cloudcomputing & Security - Informatie van het Nationaal Cyber Security Centrum over clouddiensten en mogelijke risico's.
- Beleidsregels Meldplicht datalekken - De beleidsregels van de Nederlandse Autoriteit Persoonsgegevens helpen organisaties bij de vaststelling van een datalek dat zij moeten melden bij de Autoriteit Persoonsgegevens.
- Data Pro Code - Gedragscode en certificering voor verwerkers van persoonsgegevens met een nadere invulling van de AVG.

Personeel

Medewerkers van Visma | Raet verklaring geheimhouding van gegevens in de ruimste zin van het woord, zowel tijdens als na afloop van de arbeidsovereenkomst. Deze geheimhoudingsplicht geldt ook voor alle andere informatie waar de medewerker in het kader van de arbeidsovereenkomst kennis van heeft.

De Visma | Raet of externe medewerkers mogen over deze informatie geen enkele mededeling doen aan derden, waaronder interne of externe medewerkers van Visma tenzij dit voor een behoorlijke uitoefening van hun functie noodzakelijk is.

Schending van dit artikel kan voor Visma | Raet een dringende reden zijn voor ontslag op staande voet.

Visma | Raet kent een referentie check. Dat betekent dat antecedenten van vorige werkgevers onderzocht worden en dat in situaties waar medewerkers kennis kunnen nemen van zeer gevoelige of vertrouwelijke informatie of hoge eisen gesteld worden aan de integriteit van de informatie, een antecedentenonderzoek uitgevoerd kan worden. Bij zeer gevoelige informatie kan een Verklaring Omtrent het Gedrag (VOG) vereist zijn.

Zowel medewerkers als ingehuurde personeelsleden zijn zich bewust van hun taken en verantwoordelijkheden. Daarbij waarborgen wij dat zij deze taken en verantwoordelijkheden naar behoren vervullen en dat al het personeel geschikt is voor hun rol.

Wet- en Regelgeving

VISMA | raet

Wet- en Regelgeving

Sociale en fiscale wet- en regelgeving, het arbeidsrecht maar zeker ook de privacywetgeving hebben grote invloed op de processen van onze relaties en voor onze producten en diensten. Dit geldt voor zowel de salaris- als de HR-(gerelateerde)systemen.

Wij hebben onze processen zo ingericht dat we wijzigingen in de landelijke wetgeving tijdig onderkennen en onze systemen, dienstverlening en interne processen hierop kunnen aanpassen. Hierbij interpreteren we de wetgeving eenduidig voor onze verschillende systemen en diensten.

Samengevat zorgt Visma | Raet voor een:

- Tijdige signalering en juiste interpretatie van aankomende wijzigingen in landelijke wet- en regelgeving.
- Eenduidige interpretatie en implementatie van wet- en regelgeving in systemen.
- Snelle reactie op nieuwe ontwikkelingen in landelijke wet- en regelgeving.
- Duidelijke communicatie over de gevolgen van gewijzigde wet- en regelgeving.
- Dialoog met regelgevers en koepelorganisaties over uitvoerbaarheid van wet- en regelgeving.

Privacy

De dienstverlening van Visma | Raet draait om de verwerking van persoons-, salaris- en daaraan gerelateerde gegevens en het waarborgen van de privacy van persoonsgegevens. Wetgeving met betrekking tot het Verwerken van persoonsgegevens is binnen de EER vastgelegd in de Algemene Verordening Gegevensbescherming (AVG).

De AVG stelt onder andere eisen aan de vorm en inhoud van afspraken die opdrachtgevers als verwerkingsverantwoordelijke en leveranciers als sub-verwerker met Visma | Raet in onze rol als verwerker maken.

De AVG verplicht ons dat we:

- handelen volgens de wet;
- bindende afspraken maken met verwerkingsverantwoordelijken en sub-verwerkers;
- persoonsgegevens alleen verstrekken aan derden als dat voortvloeit uit de wet of uit het doel van de verwerking;
- de technische en organisatorische beveiliging voldoende waarborgen;
- de toevertrouwde persoonsgegevens geheim houden;
- persoonsgegevens verwerken in landen met een passend beschermingsniveau;
- een functionaris gegevensbescherming (FG) aanstellen als interne toezichthouder en adviseur;
- de verwerkingsverantwoordelijke tijdig informeren over datalekken;
- het ‘privacy by design’ en ‘privacy by default’ principe hanteren bij software-ontwikkeling.

De Data Pro Code

De Data Pro Code is een, door de Autoriteit Persoonsgegevens goedgekeurde, gedragscode volgens artikel 40 van de AVG in Nederland. Deze gedragscode is geïnitieerd door de IT-brancheorganisatie NLdigital. Alle organisaties die het Data Pro-certificaat hebben verkregen zijn geregistreerd in het Data Pro Register.

Deze gedragscode is van toepassing voor Visma | Raet als verwerker van persoonsgegevens.

We tonen sinds 2020 door middel van een certificaat aan dat we voldoen aan de gedragscode Data Pro en dat we daardoor op een verantwoorde manier omgaan met persoonsgegevens van klanten.

Ons Data Pro Statement vormt samen met onze dienstverleningsovereenkomst de basis voor de verwerkersovereenkomst voor de producten en diensten die Visma | Raet voor je verzorgt.

Verwerkersovereenkomst

De AVG stelt ook eisen aan de klanten van Visma | Raet, als ‘eigenaar’ van persoonsgegevens. Een verwerkingsverantwoordelijke moet vaststellen dat Visma | Raet in voldoende mate invulling geeft aan eerdergenoemde eisen. Wij bieden hiervoor een gestandaardiseerde ‘verwerkersovereenkomst’ aan op onze website. Na ondertekening maakt deze deel uit van de dienstverleningsovereenkomst.

Samengevat zorgen we ervoor dat:

- We een standaard up-to-date verwerkersovereenkomst beschikbaar stellen via onze website.
- Het gedrag van medewerkers en getroffen maatregelen voldoen aan de vereisten van de AVG.
- We een eventueel datalek direct na signalering in behandeling nemen.
- We je zo spoedig mogelijk na ontdekking van een datalek informeren.
- We alle informatie aan jouw specialisten verstrekken zodat je als verwerkingsverantwoordelijke tijdig melding kan doen van meldingsplichtige datalekken bij de Autoriteit Persoonsgegevens.
- We je in geval van een datalek op de hoogte houden over de voortgang en de getroffen maatregelen.
- We zekerheid bieden door middel van audits, certificaten en assurance rapportages dat maatregelen geïmplementeerd zijn en ook zo worden uitgevoerd.

Meldplicht Datalekken

Bij inbreuk op de privacy van persoonsgegevens (een ‘datalek’), moet de verwerkingsverantwoordelijke dit melden bij de Autoriteit Persoonsgegevens (AP). Behalve als het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Bij een datalek op de beveiliging van persoonsgegevens moet de verwerkingsverantwoordelijke dit direct en uiterlijk binnen 72 uur na ontdekking melden bij de Autoriteit. Wanneer de inbreuk bovendien waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, moet de verwerkingsverantwoordelijke het ook aan de betrokkene(n) meedelen.

Uiteraard doet Visma | Raet er alles aan om een datalek te voorkomen, zoals in dit document staat beschreven. Gebeurt dit toch dan melden we het privacy incident of inbreuk op de beveiligingsmaatregelen zo snel mogelijk. Ook krijg je alle beschikbare en vereiste informatie en houden we je op de hoogte over de voortgang van de getroffen maatregelen zodat je kunt blijven voldoen aan de AVG.

Certificaten en Rapportages

Certificaten en rapportages

Visma | Raet beschikt over certificaten, laat penetratietests uitvoeren en levert op verzoek ISAE3402 type II rapportages. Onderstaand een opsomming van de belangrijkste assurance documenten.

Data Pro adherence: De Data Pro Code is ontwikkeld door NLDigital, de brancheverenigingvoor ICT bedrijven in Nederland en is de eerste goedgekeurde gedragscode onder de AVG in Europa. Hiermee tonen wij niet alleen aan dat wij voldoen aan de wetgeving maar ook dat privacy op hoog niveau geïmplementeerd en verankerd is in de organisatie.

ISAE3402 type II rapportage: Visma | Raet beschikt sinds 2006 over SOC rapportages (Control Statements) voor de HR- en salarissystemen en de generieke IT beheersmaatregelen. In deze rapportages verklaart een accountant dat de dienstverlening van Visma | Raet betrouwbaar en 'in control' is.

ISO16175 certificaat: Door middel van dit certificaat tonen we aan dat onze module personeelsdossier voldoet aan principes en functionele eisen voor software om digitale informatie te creëren en te beheren in kantooromgevingen.

ISO27001 certificaat: Visma | Raet beschikt sinds 2011 over dit certificaat dat aangeeft dat het ISMS van Visma | Raet getoetst is conform deze internationale standaard. In de Verklaring van Toepasselijkheid is beschreven welke onderdelen van de norm van toepassing zijn.

ISO9001 certificaat: Dit certificaat is het internationale keurmerk voor het kwaliteitsmanagementsysteem. Visma | Raet heeft sinds 1997 een ISO9001-certificaat.

NEN4400-1 certicaat: Het SNA-keurmerk is een privaat certificeringssysteem, waarbij ondernemingen zich vrijwillig aanmelden en hun administraties frequent laten inspecteren op hun verplichtingen uit arbeid, waardoor het risico voor de inlener en uitbesteder van werk wordt beperkt.

Over Visma | Raet

Visma | Raet maakt het HR leven makkelijker. Zodat er meer tijd is voor zaken die er in het leven toe doen. Met de slimme SaaS HR & payroll-oplossingen van Visma | Raet worden repetitieve en administratieve taken geautomatiseerd wat het HR-leven stukken makkelijker maakt. Zo ontstaat er rust en ruimte om te doen wat écht belangrijk is, zoals het verder helpen van mens en maatschappij. Denk hierbij niet alleen aan de extra tijd en aandacht voor het ontwikkelen van medewerkers en het binden en boeien van nieuw talent, maar ook aan tijd en aandacht voor patiënten, leerlingen en burgers. Zo werken we samen aan een mooie duurzame wereld.

Visma | Raet is onderdeel van het Noorse Visma AS, marktleider in Scandinavië en behoort tot de top 10 van Europese business-softwarehuizen. De Visma-groep heeft ruim 1.4 miljoen klanten, 14.000 medewerkers en een jaaromzet van 2.0571 miljoen euro (EBITDA 591 miljoen euro) in 2022. Kijk voor meer informatie op: www.vismaraet.nl of bel +31(0)88 – 23 02 300.

VISMA | raet