YOUSERVE
BY VISMA

infosheet

Visma YouServe in control

Als Visma YouServe in control is, ben jij in control

Als Visma YouServe in control is, ben jij in control.

Dit document laat zien hoe Visma YouServe hier invulling aan geeft.

Inhoud

YOUSERVE
BY VISMA

Inleiding

Als je bedrijfsprocessen of delen ervan 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 en de afgesproken dienstverlening aan actuele wet- en regelgeving.

Met andere woorden, je wilt weten hoe Visma YouServe in control is over jouw bedrijfsprocessen. Uitbesteding van werkzaamheden ontslaat je immers niet van je (eind)-verantwoordelijkheid voor processen waar je geen directe invloed op hebt.

Visma YouServe is al jaren een zeer betrouwbare partner op het gebied van HR-dienstverlening. Wij zijn een zelfstandig bedrijf binnen de Visma-groep. Visma YouServe levert services en software om HR-processen te professionaliseren, te digitaliseren of uit te besteden.

Als Visma YouServe in control is, ben jij in control. In dit document lees je hoe wij dit invullen.

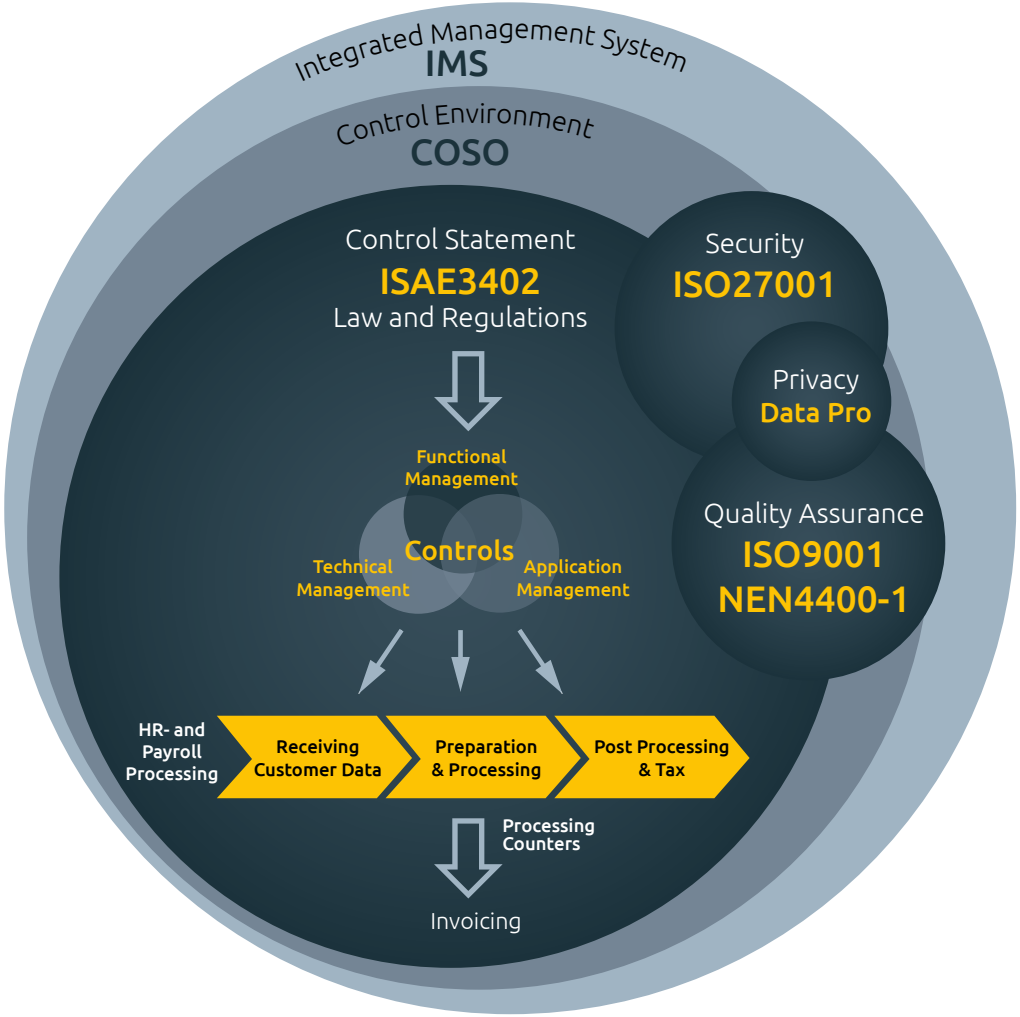
YOUSERVE BY VISMA

Visma YouServe in control

De dienstverlening van Visma YouServe 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 managen.

Visma YouServe heeft de aandachtsgebieden van de corporate governance uit de COSO control environment, ISO 9001, ISO 27001 en het Visma YouServe ISAE3402 raamwerk samengebracht in één systeem. De afdeling Compliance Management beheerst en controleert dit geïntegreerde managementsysteem (IMS: Integrated Management System).

Op deze afdeling werken specialisten op het gebied van procesmanagement, informatiebeveiliging- en kwaliteitsmanagement. In- en externe audits worden uitgevoerd op basis van het geïntegreerde raamwerk (zie model).



Model Integraal beheersraamwerk

YOUSERVE BY VISMA

Kwaliteit

De directie en de medewerkers van Visma YouServe onderkennen het belang van kwaliteit en streven continu naar een excellente en klantgerichte organisatie. Dit gebeurt onder meer door de implementatie van kwaliteitsstandaarden en ketenprocessen.

Kwaliteitssysteem

Visma YouServe gebruikt een kwaliteitsmanagementsysteem op basis van de meest recente normen. Hiermee besturen en beheersen wij de integrale kwaliteit van de organisatie. Het systeem omvat onder andere kwaliteitsdoelen, procesbeschrijvingen, taken, verantwoordelijkheden, beheersmaatregelen, procedures, werkinstructies, beleidsdocumenten, interne en externe audits.

Visma YouServe biedt hiermee aan haar relaties voortdurend een hoog kwaliteitsniveau. Het kwaliteitssysteem borgt een goede afstemming tussen afdelingen onderling en is de basis voor permanente aandacht voor het verbeteren van werkwijze, producten en diensten.
Het kwaliteitssysteem van Visma YouServe is sinds 2023 ISO 9001 gecertificeerd volgens het kwaliteitsmanagementsysteem van Visma Software International AS. De scope van dit kwaliteitssysteem omvat de processen voor software product development en business support functies. Binnen deze scope vallen processen als product strategie, product security en de volledige ontwikkelcyclus van planning tot release. De business support processen in scope zijn marketing, sales, support, consulting, finance, HR en BPO.

Procesketen
Het procesmodel geeft de keten van de primaire processen weer. Per schakel in deze keten is een directielid eindverantwoordelijk voor de goede werking.

Kwaliteitsbewaking

Om te voldoen aan de ISO-eisen, richt Visma YouServe een doeltreffend en doelmatig auditproces in. Dit proces helpt om sterke en zwakke punten van het kwaliteitssysteem te beoordelen.

Audits zijn een belangrijk managementinstrument om onafhankelijk vast te stellen of wordt voldaan aan de normen. Ze geven inzicht in de effectiviteit en efficiëntie van de organisatie.

Een goed functionerend intern auditproces vormt de basis voor de externe audits. Afspraken hierover zijn vastgelegd in het auditbeleid.

Een gecertificeerde externe partner voert jaarlijks audits uit en bewaakt het kwaliteitsniveau voor het ISO 9001-certificaat. Het kwaliteitssysteem van Visma Software International AS – en daarmee ook Visma YouServe – is gecertificeerd volgens de ISO 9001:2015-norm.

Kwaliteitshandboek

Het kwaliteitssysteem van Visma YouServe is digitaal vastgelegd en voor iedere medewerker toegankelijk. Dit 'kwaliteitshandboek' bevat onder andere de processchema's, rollen, functies en systemen met bijbehorende beschrijvingen binnen Visma YouServe.

Procesverbetering

Visma YouServe 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 of efficiëntie.

Klachten

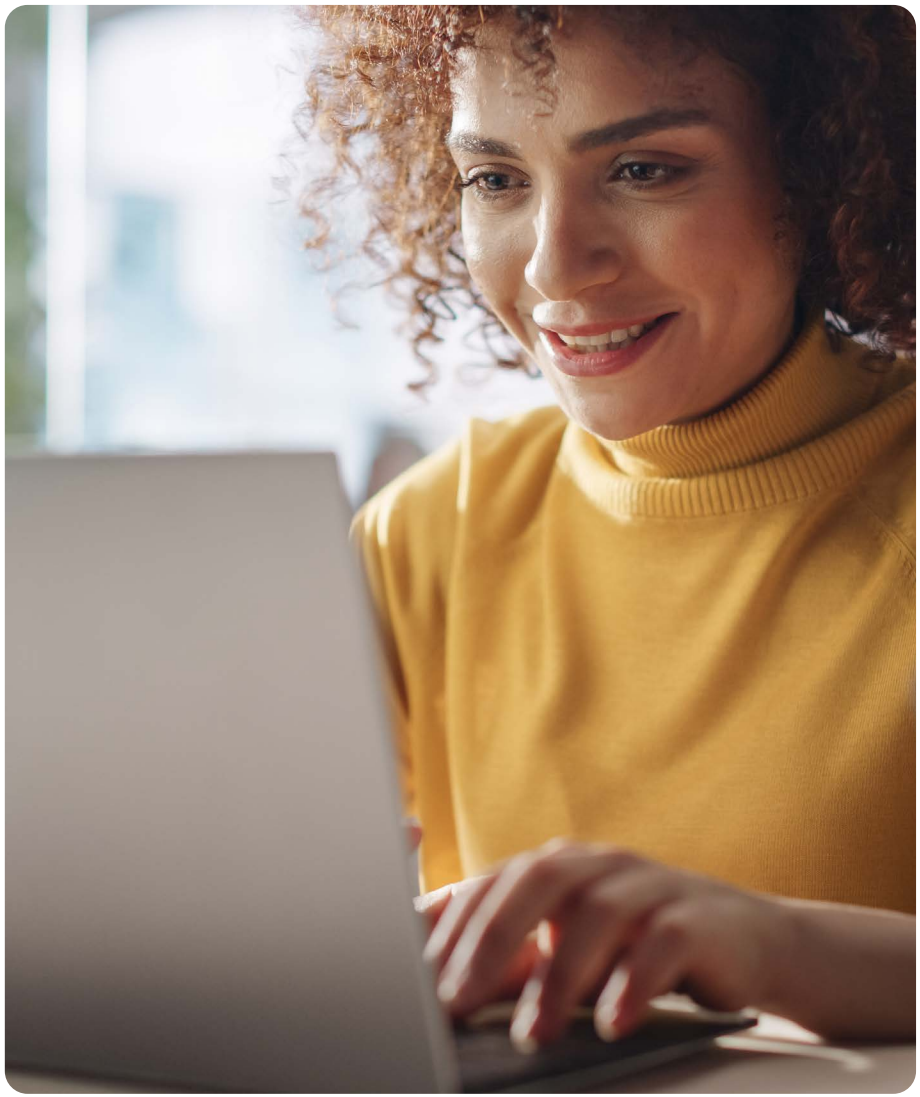
Visma YouServe streeft voortdurend naar optimale dienstverlening. Uiteraard kunnen we een klacht over onze producten of services niet uitsluiten. Wanneer wij een klacht ontvangen, dan doen we er alles aan om deze zo snel en goed mogelijk af te handelen. Een klachtendesk verzorgt de registratie en bewaakt de voortgang van behandeling. Afhankelijk van de ernst, handelt directie of management de klacht af. Wij analyseren de klachten met regelmaat om tot verbeteracties te komen.

De ISO 9001-norm

De ISO 9001-norm eist dat een organisatie:

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

In hoofdlijnen schrijft de norm voor dat Visma YouServe vastlegt hoe zij processen beheerst en de benodigde middelen beschikbaar stelt om producten volgens klanteisen te leveren. De norm vraagt bewaking van processen en producten en een analyse van de resultaten zodat verbeteringen mogelijk zijn.



Informatiebeveiliging

Visma YouServe is verantwoordelijk voor en wettelijk verplicht tot een veilige dienstverlening. Hiermee zijn wij ook verantwoordelijk voor de beveiliging van gegevens van onze relaties. Deze visie is vastgelegd in een Informatiebeveiligingsbeleid.

In dit beleid staan vier begrippen centraal:

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

Als onderdeel van de Visma Group is ons informatiebeveiligings-beleid gebaseerd op het Visma Security Programma. Dit programma biedt richtlijnen en oplossingen op drie gebieden:

- **Visma Application Security Program**
  Beleid en maatregelen voor het veilig ontwikkelen en leveren van producten, inclusief de betrokken infrastructuur in de klantdienstverlening.
- **Visma Infrastructure Security Program**
  Beleid en maatregelen op het gebied van de infrastructuur van Visma YouServe, zoals bijvoorbeeld endpoint protectie.
- **Visma People Security Program**
  Beleid en maatregelen om het bewustzijn en de kennis binnen Visma YouServe over informatiebeveiliging te vergroten, zoals het jaarlijkse trainingen en het aanbieden van een passwordmanager.

Binnen het Visma Security Programma wordt een Security Maturity Index voor alle Visma-bedrijven bijgehouden op basis waarvan beslissingen genomen kunnen worden om het security-niveau te verbeteren. Via visma.com/trust-centre/security kun je meer informatie vinden over het Visma Security Programma.

Naast de maatregelen op Visma Group-niveau heeft Visma YouServe waar nodig eigen beleid en richtlijnen specifiek voor de dienstverlening van Visma YouServe. Het informatiebeveiligingsbeleid van Visma YouServe geldt voor al onze bedrijfsonderdelen, domeinen, omgevingen en locaties. Ook de eisen die wij aan onze leveranciers stellen, horen daarbij. Visma YouServe eist daarom dat leveranciers voldoen aan de internationale standaard voor informatiebeveiliging ISO/IEC 27001, bij voorkeur gecertificeerd.

De ISO 27001-norm

Het informatiebeveiligingsbeleid van Visma YouServe is opgesteld conform de meest recente internationale norm ISO 27001. In een beheersraamwerk met maatregelen, beleid en richtlijnen beschrijven we hoe we dit beleid uitvoeren. We beoordelen en testen het beleid jaarlijks.

Het directieteam van Visma YouServe is verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid en is in die rol beslissingsbevoegd. De Business Information Security Officer is vanuit het Compliance team uitvoerend verantwoordelijk met een controlerende en adviserende rol.

Continuïteit van de dienstverlening

Visma YouServe 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 opgesteld met organisatiebrede uitgangspunten voor de naleving van het informatiebeveiligingsbeleid die noodzakelijk zijn voor de continuïteit van de bedrijfsvoering. We identificeren gebeurtenissen die bedrijfsprocessen kunnen onderbreken met gestandaardiseerde risicoanalyses op basis van waarschijnlijkheid (kans) en gevolgen (impact).

We hebben maatregelen genomen voor de handhaving of het herstel van bedrijfsactiviteiten en het beschikbaar stellen van informatie na een onderbreking of uitval van cruciale medewerkers of bedrijfsprocessen. Uiteraard testen we de continuïteitsplannen op regelmatige basis zodat ze actueel en doeltreffend blijven. Dit proces testen we op opzet, bestaan en werking.

Toegang tot klantdata

Via onze systemen verwerken wij een grote hoeveelheid klantgegevens. Het gebruik van klantdata door Visma YouServe is aan sterke restricties gebonden. Dit alles maakt deel uit van het informatiebeveiligingsbeleid. Wij beschikken alleen over data ten behoeve van de dienstverlening overeengekomen met de klant. Het gebruik van klantdata voor testdoeleinden is op basis van privacywetgeving niet toegestaan zonder gemotiveerde verwerkingsgrondslag. Visma YouServe gebruikt geen data voor testdoeleinden zonder uitdrukkelijke toestemming van de verwerkingsverantwoordelijke.

Beveiligingsmaatregelen

Visma YouServe heeft organisatorische, fysieke, technische en procedurele maatregelen getroffen om de beveiliging van gegevens en diensten op het verwachte en vereiste niveau te houden. De getroffen maatregelen zijn een samenhangend geheel van voorzieningen op het niveau van de Visma Group en de eigen beheersmaatregelen van Visma YouServe.
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 datacenters:** Onze servers bevinden zich altijd in gecertificeerde en zwaar beveiligde datacenters met 24/7 bemanning, speciale toegangscontrole met paspoortcontrole en camerabewaking.
- **Intrusion Prevention Systems:** Het netwerkverkeer wordt voortdurend automatisch bewaakt op verdachte acties en geblokkeerd als dat nodig is.
- **Beveiligde back-ups:** Iedere nacht maken we back-ups die we versleuteld op een andere, beveiligde, locatie bewaren.
- **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.
- **DDoS-bescherming:** We filteren kwaadwillend verkeer en laten alleen legitiem verkeer door tijdens een DDoS-aanval.
- **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.

Ook loggen we de gelukte en mislukte aanmeldpogingen.

- **Wachtwoorden versleuteld opgeslagen:** Wachtwoorden worden onleesbaar opgeslagen in de database en zijn moeilijk door hackers te achterhalen.
- **Beveiligingsspecialisten:** Naast een Business Information Security Officer heeft elk development team minimaal één security engineer aangesteld. Daarnaast is er een dedicated Chief Information Security Officer vanuit Visma Security nauw betrokken bij de uitvoering van het informatiebeveiligingsbeleid.
- **Regelmatige controle:** Interne auditors en gespecialiseerde bedrijven testen voortdurend alle beveiligingssystemen.
- **Continue monitoring:** Samen met Visma Security 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 een vermoeden van misbruik.
- **Viruscontrole:** Visma YouServe beschermt de cloudoplossingen tegen misbruik door malware en virussen.
- **2 factor authenticatie:** Naast het verkrijgen van toegang tot de systemen via gebruikersnaam en wachtwoord biedt Visma YouServe elektronische certificaten en/of 2 factor authenticatie via een mobiele app. Eventueel te combineren met single sign-on.

Meer informatie over informatiebeveiliging binnen de Visma groep kun je vinden via visma.com/trust-centre/security.

Security- en penetratietesten

Het Visma Security Programma schrijft diverse security-testen op applicatieniveau voor:

- **Statische applicatie security test (SAST)**
  Door het toepassen van SAST worden vroegtijdig kwetsbaarheden in de software gevonden. Het scannen op deze kwetsbaarheden wordt minimaal 1x per 30 dagen gedaan.
- **Dynamische applicatiebeveiligingstest (DAST)**
  Waar SAST zich richt op het analyseren van de broncode, kijkt DAST naar bedreigingen van buitenaf. Met behulp van een DAST-scanner worden gesimuleerde aanvallen uitgevoerd op de applicatie om kwetsbaarheden in kaart te brengen. De scan controleert onder andere op risico's uit de OWASP Top 10 . De OWASP Top 10 is een lijst van de tien meest kritieke beveiligingsrisico's voor webapplicaties, opgesteld door de Open Worldwide Application Security Project (OWASP).

Deze lijst wordt wereldwijd erkend als dé standaard voor webapplicatiebeveiliging. Gevonden kwetsbaarheden moeten door developmentteams binnen vastgestelde termijnen worden opgelost.

- **Penetratietesten**
  Volgens de voorschriften van het Visma Security Programma dient er minimaal 1x per 18 maanden een penetratietest te worden uitgevoerd. Penetratietesten worden uitgevoerd door een hoogopgeleid team van Visma Pentest met relevante certificeringen. De testen zijn ontworpen om zwakke plekken en kwetsbaarheden op applicatieniveau te identificeren, gebaseerd op best practices uit de industrie zoals de OWASP Top 10.
  Het testteam van Visma Pentest is volledig gescheiden en onafhankelijk van Visma Youserve, zowel op het niveau van de juridische eenheid als op managementniveau.

Alle bovenstaande testen, inclusief de afhandeling van de gevonden kwetsbaarheden, worden gemonitord door zowel Visma Security als het compliance team van Visma YouServe. De details van de resultaten van deze tests zijn niet openbaar, maar de Business Security Officer, waar nodig in samenspraak met Visma Security, classificeert en registreert mogelijke kwetsbaarheden als security issue en zorgt voor tijdige afhandeling. Elke constatering van een risico voor de veiligheid van informatie is voor ons aanleiding direct maatregelen te treffen.

Standaarden

ISO 27001 is de internationale norm voor informatiebeveiliging. Het doel is ervoor te zorgen dat organisaties de gegevens van hun klanten op een veilige manier behandelen, waarbij vertrouwelijkheid, beschikbaarheid en integriteit worden gegarandeerd. Visma YouServe is gecertificeerd volgens ISO27001:2022. Om aan deze norm te blijven voldoen, beoordeelt Visma YouServe voortdurend bedreigingen en risico's en neemt de juiste beveiligingsmaatregelen om onze diensten en de gegevens die we verwerken te beschermen tegen storingen, schade en inbreuk. De norm vereist daarom ook een managementsysteem voor informatiebeveiliging om de effectiviteit van onze beveiligingsmaatregelen continu te verbeteren.

Naast de ISO27001-norm past Visma YouServe ook de informatiebeveiligingsprogramma's toe die voor de hele Visma groep gelden. Via de website visma.com/trust-centre/security is meer informatie beschikbaar over deze programma's.

Personeel

Bij indiensttreding ondertekenen werknemers van Visma YouServe een arbeidsovereenkomst waar ook een geheimhoudingsbepaling onderdeel van is. Deze geheimhoudingsplicht geldt ook voor alle andere informatie waar de medewerker in het kader van de arbeidsovereenkomst kennis van heeft verkregen. De medewerker moet bekend zijn met het vertrouwelijke karakter van de informatie, hier een redelijkerwijs vermoeden van hebben of hier expliciet over zijn ingelicht.

Daarnaast geldt de Visma Code of Conduct voor alle werknemers. Deze gedragscode is onderdeel van de Arbeidsvoorwaardenregeling en biedt een overzicht van de verantwoordelijkheden die alle Visma medewerkers dragen. Het is een blauwdruk die ons eraan herinnert altijd ethisch te handelen, rechtmatig en bewust van wat het beste is voor onze klanten, onze medewerkers en de samenleving als geheel.
Wanneer Visma YouServe tijdelijke werknemers inschakelt, geldt via de overeenkomst met de partij waar wij deze werknemers inhuren ook een geheimhoudingsverklaring. De Visma Code of Conduct is ook voor deze groep werknemers van kracht.

Informatiebeveiliging

We hebben een reeks maatregelen ingevoerd voor de borging van de informatiebeveiliging op personeelsniveau. Als onderdeel van de contractuele verplichting stemmen nieuwe medewerkers en ingehuurd personeel in met Visma Code of Conduct. In deze gedragscode zijn onder meer de verantwoordelijkheden van de medewerker voor informatiebeveiliging vastgelegd.
Als onderdeel van deze verantwoordelijkheden is opgenomen dat de medewerker:

- handelt volgens het beveiligingsbeleid;
- bedrijfsmiddelen beschermt tegen ongeoorloofde toegang, openbaarmaking, wijziging, vernietiging of verstoring;
- beveiligingsgebeurtenissen of andere beveiligingsrisico's aan de organisatie rapporteert;
- richtlijnen voor aanvaardbaar gebruik van elektronische communicatievoorzieningen naleeft.

Visma YouServe past Pre Employment Screening (PES) toe wanneer iemand bij ons in dienst komt. Zo is het gebruikelijk een VOG te vragen van medewerkers die werken met zeer gevoelige of vertrouwelijke informatie. Ook een antecedentenonderzoek kan deel uitmaken van het sollicitatieproces. De identiteit van een nieuwe medewerker wordt vastgesteld met een controle van een officieel erkend legitimatiebewijs.

Opleidingsniveau

Visma YouServe heeft functies beschreven in functiegroepen en functiematrices. Deze omvatten minimaal 80 procent van de reguliere werkzaamheden van een medewerker. In deze functiematrices staan ook het opleidings- en kennisniveau beschreven. Manager en medewerker maken aanvullende afspraken in het doelstellingengesprek.

Het management van Visma YouServe biedt haar medewerkers de mogelijkheid trainingen en opleidingen te volgen voor een correcte beoefening van de functie. Als onderdeel van het Visma Security Program volgen softwareontwikkelaars een secure code training. Daarnaast is er vanuit de Visma Group een jaarlijkse cyclus van trainingen op het gebied van privacy, security en anti-corruptie. In de jaarlijkse HR-cyclus bespreekt het management vorderingen, kennis en vaardigheden van de medewerker en stuurt bij waar nodig. Ook beoordeelt Visma YouServe haar management jaarlijks op kennis en kwaliteiten.

Wet- en regelgeving

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

Landelijke wetgeving

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 YouServe 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.
- Dialoog met regelgevers en koepelorganisaties over uitvoerbaarheid van wet- en regelgeving.

Privacy wetgeving

De dienstverlening van Visma YouServe draait om de verwerking van personeels- en salarisgegevens en het waarborgen van de privacy van deze persoonsgegevens. Op grond van de Algemene Verordening Gegevensbescherming (AVG) is Visma YouServe daarom aangeduid als ‘verwerker’. De AVG stelt eisen aan de vorm en inhoud van afspraken die opdrachtgevers (verwerkingsverantwoordelijken) en leveranciers met Visma YouServe maken. Daarnaast stelt deze wet ook een aantal zelfstandige verplichtingen en beperkingen aan Visma YouServe als verwerker.

In het kader van de AVG zorgt Visma YouServe er voor dat:

- we handelen volgens de wet;
- persoonsgegevens alleen worden verwerkt op basis van schriftelijke instructies van verwerkingsverantwoordelijken zoals uitgewerkt in de dienstverleningsovereenkomst of de wet;
- gegevens alleen worden verstrekt aan derden als dat voortvloeit uit de wet of uit het doel van de verwerking (met algemene toestemming van de verwerkingsverantwoordelijke);
- de technische en organisatorische beveiliging voldoende wordt gewaarborgd;
- de toevertrouwde gegevens geheim worden gehouden;
- gegevens verwerkt worden in landen met een passend beschermingsniveau;
- een functionaris gegevensbescherming (FG) is aangesteld als interne toezichthouder en adviseur;
- de verwerkingsverantwoordelijke tijdig wordt geïnformeerd over inbreuken in verband met persoonsgegevens;
- het 'privacy by design' en 'privacy by default' principe wordt gehanteerd bij softwareontwikkeling.
- er bindende verwerkersafspraken zijn gemaakt met verwerkingsverantwoordelijken en subverwerkers.

De hiervoor genoemde aspecten zijn onderdeel van ons privacybeleid, informatie- en beveiligingsbeleid en normenkader en maken toetsing op basis van ISAE 3402 en ISO 27001 mogelijk.

AI-wetgeving

Artificial Intelligence (AI) speelt een steeds grotere rol in de samenleving en daarmee ook in de dienstverlening van Visma YouServe. De Visma Group heeft richtlijnen, gebaseerd op de Europese wetgeving (EU AI Act) vastgesteld voor het verantwoordelijk omgaan met AI binnen de organisatie. Visma YouServe houdt zich onverkort aan deze Visma-richtlijnen en heeft AI onderdeel gemaakt van het privacy- en beveiligingsbeleid.

Meldplicht datalekken

Bij een inbreuk op persoonsgegevens (een 'datalek'), moet de verwerkingsverantwoordelijke dit melden bij de Autoriteit Persoonsgegevens, als deze inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De verwerkingsverantwoordelijke moet de inbreuk zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, melden. In het geval de inbreuk bovendien een mogelijk hoog risico inhoudt voor de rechten en vrijheden van

natuurlijke personen, moet de verwerkingsverantwoordelijke het ook aan de betrokkene(n) meedelen.

Uiteraard doet Visma YouServe er alles aan om een datalek te voorkomen. Gebeurt dit toch, dan melden we het incident zo snel mogelijk aan de betrokken verwerkingsverantwoordelijke(n). 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.

Kort samengevat, Visma YouServe:

- zorgt dat gedrag van medewerkers en maatregelen voldoen aan de vereisten van de AVG;
- neemt een eventueel datalek direct na signalering in behandeling;
- informeert je zo spoedig mogelijk na ontdekking;
- verstrekt alle informatie aan jouw specialisten zodat je als verwerkingsverantwoordelijke de situatie kan beoordelen om te bepalen of er een melding moet worden gedaan bij de Autoriteit Persoonsgegevens;
- houdt je op de hoogte over de voortgang en de getroffen maatregelen;
- biedt zekerheid door middel van audits, certificaten en assurance rapportages dat maatregelen geïmplementeerd zijn en ook zo uitgevoerd worden.

AVG en verwerkersovereenkomst

De AVG stelt ook eisen aan de relaties van Visma YouServe, als ‘eigenaar’ van persoonsgegevens. Een verwerkings-verantwoordelijke moet vaststellen dat Visma YouServe in voldoende mate voldoet aan bovengenoemde eisen. Visma YouServe biedt hiervoor een gestandaardiseerde verwerkersovereenkomst. Wij voegen deze na ondertekening toe aan de dienstverleningsovereenkomst.

AVG en medische gegevens

Medische gegevens vastgelegd in een verzuimapplicatie worden opgeslagen in een afgeschermd deel van de Visma YouServe systemen. HR-specialisten zonder toegang tot medische gegevens op basis van Nederlandse wetgeving hebben alleen toegang tot procesgegevens en niet tot medische gegevens.

In het medisch logboek worden gegevens versleuteld (encrypted) opgeslagen. Ook aan dit logboek gekoppelde persoonsgegevens

worden versleuteld. Toegang tot medische gegevens is alleen mogelijk op basis van inlognaam/wachtwoord en een persoonlijk beveiligingscertificaat (SSL certificaat). Ook wel bekend als 2-factor authenticatie.

Visma YouServe autoriseert de medische module zodat de beheerafdeling van de eigen organisatie geen toegang heeft tot medische gegevens. Visma YouServe toetst autorisatie aanvragen op basis van een aantal overeen te komen criteria waaronder de BIG-registratie (Wet Beroepen in de Individuele Gezondheidszorg).

AVG en de overdracht van medische dossiers

Dankzij toegangsautorisatie hebben uitsluitend personen gebonden aan de medische eed van geheimhouding, toegang tot de medische gegevens. Deze beveiligingsmaatregelen functioneren bij overdracht van de gegevens, bijvoorbeeld bij wijziging van arbodienst. Wij zien erop toe dat de medische gegevens en de overige gegevens niet bij onbevoegden terechtkomen. Ook hier leven wij de richtlijnen van de Autoriteit Persoonsgegevens na. Zo heeft de Autoriteit Persoonsgegevens in juni 2007 een standpunt ingenomen over de wijze van overdracht van arbodossiers aan een opvolgende arbodienst, conform de actuele wet- en regelgeving.

IT-beheersprocessen

Visma YouServe hanteert ISO 27002 als normenkader voor de IT-beheersprocessen. Het ontwikkelproces maakt daar deel van uit. Het ontwikkelproces is opgenomen in het kwaliteitsmanagementsysteem van Visma YouServe en wordt jaarlijks getoetst op opzet, bestaan en werking.

Het ontwikkelproces start na:

- een ontwikkelopdracht voor nieuwe functionaliteit of onderhoudswerkzaamheden;
- gewijzigde wetgeving;
- geconstateerde softwarefouten.

DTAP

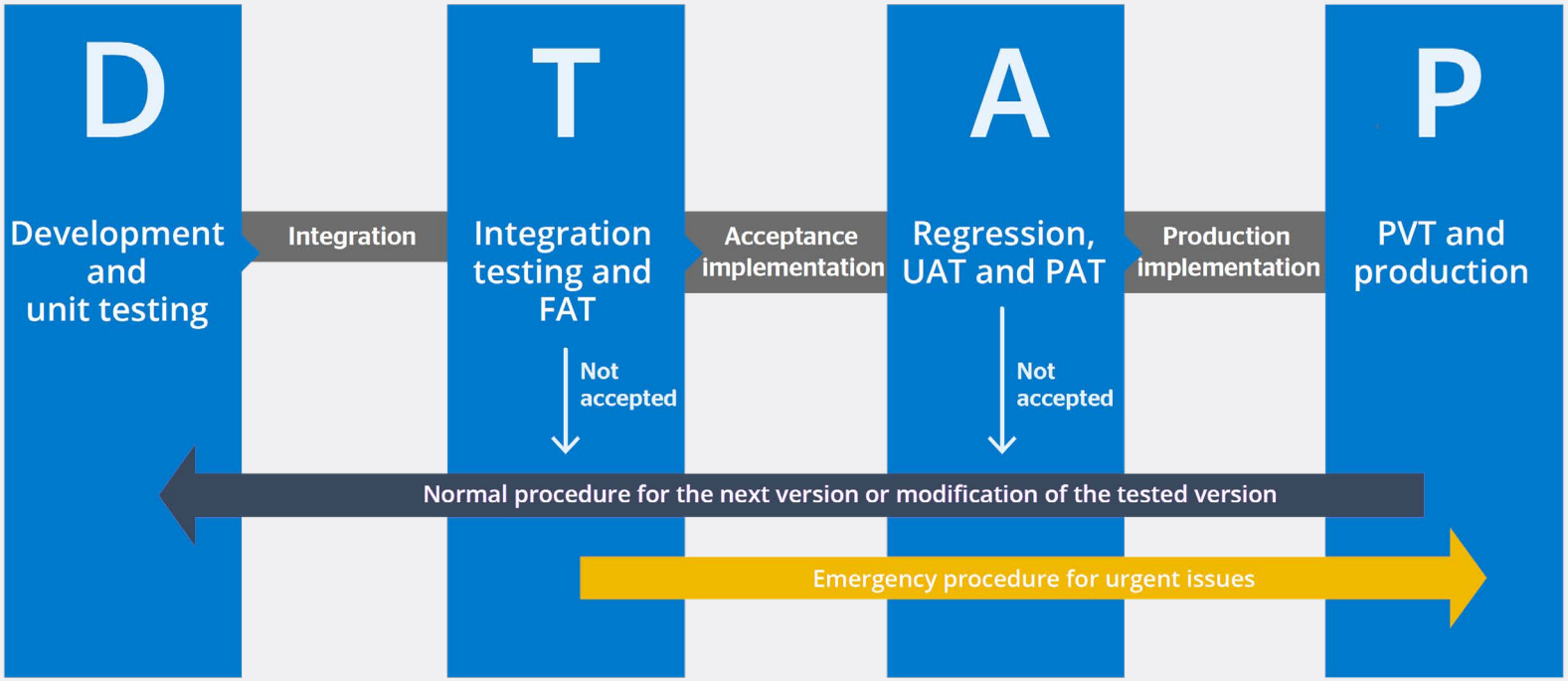
DTAP is een algemeen gebruikte afkorting voor de fasering binnen productontwikkeling: Development, Test, Acceptation en Production. Wij leveren onze systemen met een fysieke scheiding tussen de ontwikkel-, test-, acceptatie-, en de productieomgeving.

Applicaties ontwikkelen we volgens een agile ontwikkelmethodiek waarin we naast de ontwikkeling uitgebreid aandacht besteden aan verschillende testmethoden.

YOUSERVE BY VISMA

Het belangrijkste doel van het DTAP-model is de waarborging van een strikte scheiding tussen de ontwikkel-, test- en productieomgeving. Integriteit en beschikbaarheid van de productieomgeving spelen hierbij een belangrijke rol.

We gebruiken de productieomgeving voor de dagelijkse gegevensverwerking en dienstverlening aan onze klanten.



DTAP-model

Certificaten en rapportages

Visma YouServe beschikt over ISO 27001, ISO 9001, Data Pro Certificering, laat penetratietesten uitvoeren en levert op aanvraag ISAE3402 type II rapportages.

ISAE3402 type II rapportages

Een van de meest effectieve manieren waarop wij over interne beheersingsmaatregelen communiceren, is door middel van een Service Auditor's Report. Er zijn twee soorten Service Auditor's Reports: Type I en Type II. Een Type I-rapport beschrijft de beschrijving van de interne beheersingsmaatregelen van de serviceorganisatie op een specifiek tijdstip. Een Type II-rapport omvat niet alleen de beschrijving van de interne beheersingsmaatregelen van de serviceorganisatie, maar omvat ook een gedetailleerde externe toetsing van de interne beheersingsmaatregelen van de serviceorganisatie over een periode van minimaal zes maanden. Een ISAE3402 type II rapport voor een rapportageperiode van een jaar is op aanvraag beschikbaar voor klanten.

ISO 27001 certificaat

ISO 27001 is de internationale norm voor informatiebeveiliging. Het doel is ervoor te zorgen dat organisaties de gegevens van hun klanten op een veilige manier behandelen, waarbij vertrouwelijkheid, beschikbaarheid en integriteit worden gegarandeerd. Om aan deze norm te voldoen, beoordeelt Visma YouServe voortdurend bedreigingen en risico's en neemt de juiste beveiligingsmaatregelen om onze diensten en de gegevens die we verwerken te beschermen tegen storingen, schade en inbreuk. De norm vereist daarom ook een managementsysteem voor informatiebeveiliging om de effectiviteit van onze beveiligingsmaatregelen continu te verbeteren. Dit maakt dat jij als klant kunt vertrouwen op de betrouwbaarheid van ons beveiligingsbeleid.

ISO 9001 certificaat

Dit certificaat is het internationale keurmerk voor het kwaliteitsmanagementsysteem. Het kwaliteitssysteem van Visma YouServe is ISO 9001 gecertificeerd volgens het kwaliteitsmanagementsysteem van Visma Software International

AS. De scope van dit kwaliteitssysteem omvat de processen voor software product development en business support functies. Binnen deze scope vallen processen als product strategie, product security en de volledige ontwikkelcyclus van planning tot release. De business support processen in scope zijn marketing, sales, support, consulting, finance, HR en BPO.

Data pro certificering

De Data Pro Code is een uitwerking van de verplichtingen voor verwerkers zoals opgenomen in artikel 28 van de AVG. Deze uitwerking is geïnitieerd door de IT-brancheorganisatie NL Digital en heeft geresulteerd in een gedragscode met concrete richtlijnen. De Data Pro Code is een, door de Autoriteit Persoonsgegevens goedgekeurde, gedragscode volgens artikel 40 van de AVG. De toetsing op deze gedragscode vindt plaats door Scope Europe.

Penetratietestrapporten

Als onderdeel van het Visma Security Programma worden verschillende testen op de weerbaarheid van onze systemen uitgevoerd.
Op verzoek leveren wij een samenvatting van de resultaten.

MVO rapportage

Maatschappelijk verantwoord ondernemen is voor Visma YouServe het voortdurend streven naar een goede balans tussen economische groei, sociale verantwoordelijkheid en het beschermen van het milieu. We werken aan een sterke onderneming met gelukkige klanten en medewerkers. Tegelijkertijd willen we ervoor zorgen dat we de wereld niet uitputten voor de huidige én toekomstige generaties. Deze benadering van maatschappelijke verantwoordelijkheid is van toepassing op al onze activiteiten en op onze hele waardeketen. Ons MVO-rapport kan worden gedownload via onze website.

Zekerheid uitbesteding

Het ISAE3402 type II rapport is specifiek bedoeld voor gebruik bij de jaarrekeningcontrole en geeft een goed beeld hoe Visma YouServe de ontwikkeling en levering van HR- en Payroll-applicaties en de BPO-dienstverlening op beheerste wijze uitvoert en ‘in control’ is. Geaccrediteerde accountants voeren de beoordeling uit en klanten van Visma YouServe kunnen het volledige digitale rapport ontvangen op basis van een geheimhoudingsverklaring. Als wij externe dienstverleners of sub-serviceorganisaties in scope van het ISAE3402-rapport inzetten, vragen wij ze om een eigen TPM verklaring of ISAE3402-rapport.

Zo krijgen wij zekerheid over de totale keten van uitbestede processen en activiteiten. Jaarlijks besluit de directie of de scope van de rapportage wijzigt. Redenen voor het aanpassen van de scope kunnen de volgende ontwikkelingen zijn:

- Wijzigingen in relevante wet- en regelgeving
- Wijzigingen in normeringen of standaarden
- Incidenten, gewijzigd risico-inzicht of gewijzigde resultaten van de risicoanalyse
- Commerciële redenen die leiden tot een wijziging van de scope
- Een relevante wijziging in dienstverlening en/of productportfolio
- Wijzigingen in de technische infrastructuur
- Relevante nieuwe of gewijzigde interne processen

Risicomanagement

Het risicobeleid bepaalt het risicomanagement van Visma YouServe. Wij zijn een risicomijdende organisatie en passen risicomanagement toe op verschillende interne en externe aspecten van de organisatie en dienstverlening zoals:

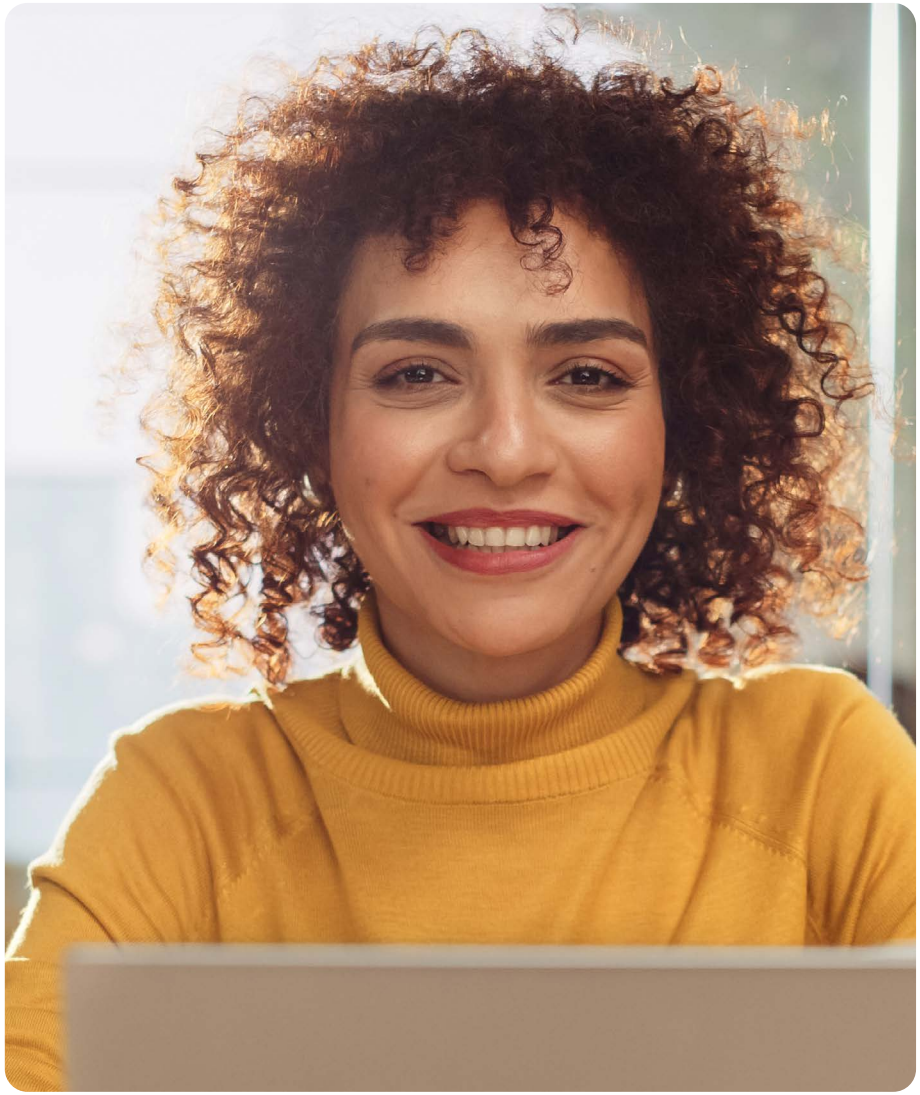
- Ondernemingsstrategie
- Wetgeving
- Informatiebeveiliging en privacy
- Operationele beheersing
- Financiële beheersing
- Reputatie en anti-corruptie
- Maatschappelijke verantwoordelijkheid
- Continuïteit

Risico's en maatregelen worden vastgelegd en beheerd met behulp van een Governance Risk & Compliance (GRC) tool. Deze tool maakt de samenhang en impact van risico's van genoemde aspecten, bedrijfsprocessen en producten inzichtelijk.

Externe audits

Het grote aantal organisaties dat werkt met onze systemen maakt het helaas niet mogelijk dat klanten zelf audits of reviews uitvoeren voor gedetailleerd inzicht in de wijze van onze procesverwerking. Het risico op ernstige verstoringen van het productieproces is te groot. Door middel van externe audits door geaccrediteerde partijen die resulteren in een ISAE3402 type II rapport en ISO 27001 certificering tonen wij aan een werkend geheel van beheersmaatregelen te hebben en dat wij 'in control' zijn op de dienstverlening die wij bieden.

Als wij genoodzaakt door wetgeving of bijzondere situaties toch een audit met een relatie overeenkomen, voert – om voor de hand liggende redenen – altijd een onafhankelijke en geaccrediteerde partij dit uit. Omdat veel organisaties werken met onze software richten we een eventuele audit zo in dat verstoring van de reguliere bedrijfsvoering niet plaatsvindt. De audit moet ruim van tevoren bij ons bekend zijn. Op basis van een concreet auditplan kunnen wij aangeven onder welke voorwaarden we meewerken. Voordat we hier aan meewerken kijken we eerst of een vergelijkbare audit niet eerder is uitgevoerd en hier een rapport of certificaat voor beschikbaar is.



YOUSERVE
BY VISMA

Daarom Visma YouServe

Alles voor gelukkige mensen

Elke organisatie drijft op mensen. Hoe digitaal je ook bent, mensen maken het verschil. Daarom is het zaak om je mensen gelukkiger te maken. Maximaal gefaciliteerd en gemotiveerd. Dat doe je met HRM op topniveau.

Unieke specialist in HR en salarisadministratie

Visma YouServe biedt je hiervoor elke vorm van ontzorging. Met onze nuchtere aanpak en 60+ jaar ervaring in HR en salarisadministratie, weten wij organisaties op elke gewenste manier te ontzorgen. Met uitgebreide services, advies en software - van ons of van derden, wij connecten het. Alles om jouw HR-zaken gewoon goed te regelen. Om jou zo veel mogelijk werk uit handen te nemen. Je te helpen je HRM naar een hoger plan te tillen. Noem ons gerust dé salarisspecialist. Het kennishuis of de softwareprovider voor HR mag ook. Wij zijn het alledrie.

Met de juiste HR-support kun je zoveel meer

Als dé partner voor je HR en payroll zorgen wij voor een zo sterk mogelijk fundament van je HRM. We zijn betrokken, betrouwbaar, relevant, lokaal en altijd bereikbaar. Alles om je medewerkers gelukkiger te maken. Daarom werk je met Visma YouServe. Dat betaalt zich altijd uit.

+31 88 23 02 700 | info@youserve.nl | www.youserve.nl |

YouServe. Betaalt zich altijd uit.