



infosheet

# Visma | YouServe in control

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

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

## Inhoudsopgave

YouServe in control	4
Kwaliteit	5
Informatiebeveiliging	8
Personeel	13
Wet- en regelgeving	15
IT-beheersprocessen	20
Certificaten en rapportages	22

## 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, via haar rechtsvoorganger Visma | Raet, al jaren een zeer betrouwbare partner op het gebied van HR-dienstverlening. Sinds 2021 zijn wij een zelfstandig bedrijf binnen de Visma-groep. Visma | YouServe levert services en software om HR-processen te professionaliseren, te digitaliseren of uit te besteden.

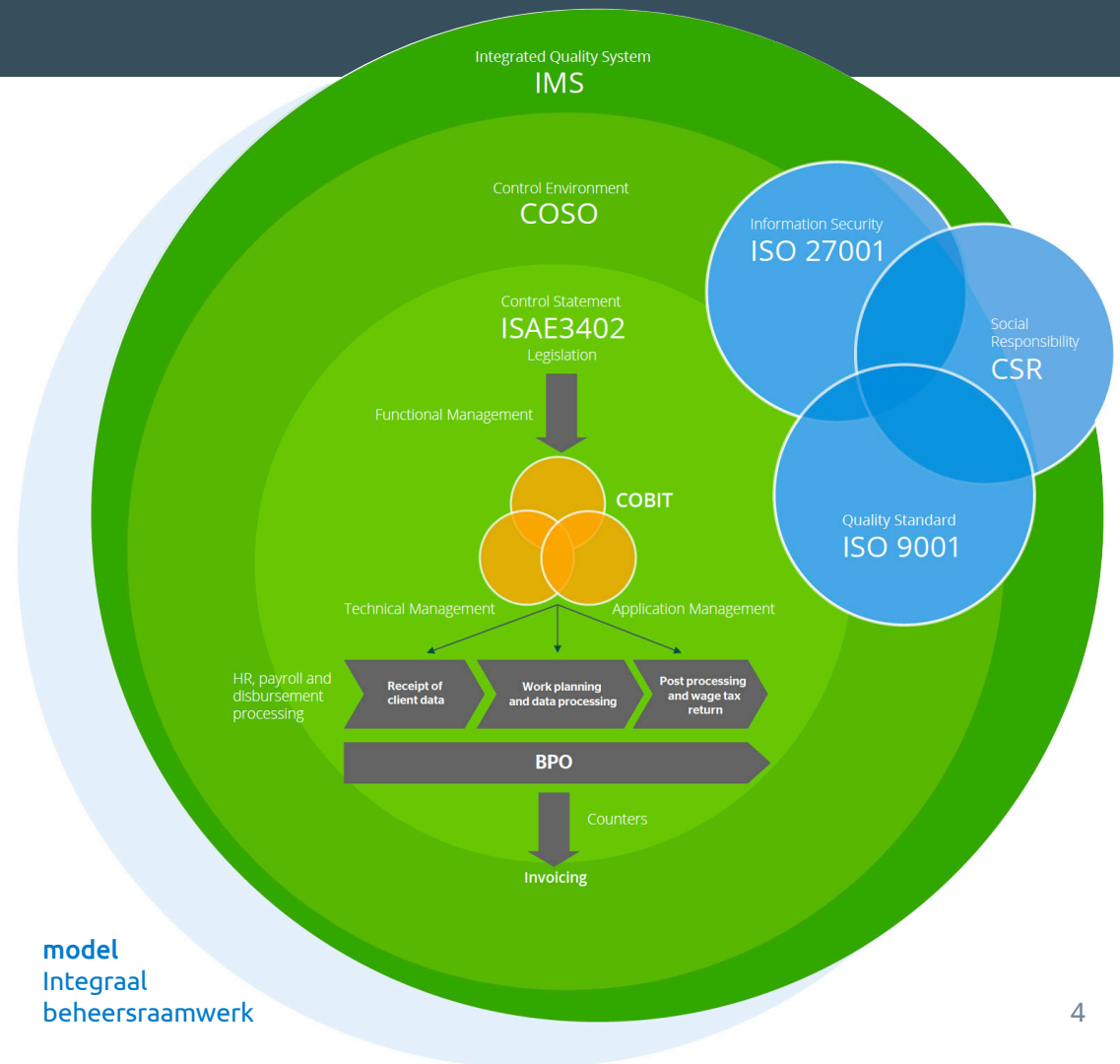
Als Visma | YouServe **in control** is, ben jij **in control**. In dit document lees je hoe wij dit invullen.

## ► 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 beheert en controleert dit geïntegreerde managementsysteem (IMS: Integrated Management System)

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



## ► Kwaliteit

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

### 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 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 kwaliteitssysteem van Visma | YouServe is, via haar rechtsvoorganger Visma Raet, sinds 1997 ISO 9001 gecertificeerd. De scope van dit kwaliteitssysteem omvat: "Leveren en implementeren van SaaS-producten en diensten voor HR- en salarisprocessen, inkomensberekening en BPO Services".

**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

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

Het auditproces is een managementinstrument 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 goedlopend intern auditproces vormt de basis voor de externe audits. De afspraken over de kwaliteitsbewaking zijn vastgelegd in het auditbeleid.

Een gecertificeerde partner voert jaarlijks audits uit en bewaakt het niveau voor het ISO 9001 - certificaat. Het kwaliteitssysteem van Visma | YouServe is gecertificeerd conform de ISO 9001:2015 standaard.

## 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. Ontvangen wij een klacht, dan doen we er alles aan 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.
- Totstandkoming producten en diensten bewaakt.
- Productfouten beheerst en problemen oplost.
- In de norm beschreven activiteiten als klachten en leveranciersbeoordeling registreert en administreert.
- Invulling geeft aan een aantal 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 en wettelijke verplicht voor 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?

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, policies en richtlijnen beschrijven we hoe we dit beleid uitvoeren. We beoordelen en testen het beleid jaarlijks.

Visma | YouServe heeft voor de bewaking van het informatiebeveiligingsbeleid een stuurgroep met beslissingsbevoegdheid, werkgroepen (operationeel) en security officers (adviserend, sturend en controlerend) aangesteld.



## Continuïteit

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 getroffen 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 klantdata. Het gebruik van klantdata door Visma | YouServe is aan sterke restricties gebonden. Dit alles maakt onderdeel 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. 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.
- **Eigen servers en firewalls:** De servers zijn in fysiek afgesloten ruimten beveiligd door zelf geconfigureerde 'firewalls'
- **Intrusion Prevention Systems:** Het netwerkverkeer wordt voortdurend automatisch bewaakt op verdachte acties en geblokkeerd als dat nodig is.
- **Beveiligde backups:** Iedere nacht maken we backups 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:** In het geval van een DDoS kunnen we het legitieme verkeer filteren van het malafide.
- **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:** Visma | YouServe heeft professionele medewerkers fulltime in 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:** 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 de mogelijkheid om gebruik te maken van 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 <https://www.visma.com/trust-centre/security/>

## Penetratietest

Een penetratietest, of intrusion detection test, is een controle uitgevoerd door zowel Visma | YouServe als 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 cloud solutions maandelijks een interne penetratietest uit en minimaal een keer per jaar een externe penetratietest. Na grotere functionele of technische aanpassingen in software of infrastructuur voeren we aanvullende penetratietests uit. 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 | YouServe de tests uitvoeren door verschillende organisaties.

## Standaarden

Visma | YouServe implementeert 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:

- ISO 27001: De ISO standaard voor informatiebeveiligingsystemen (ook wel Information Security Management Systems - ISMS genoemd).
- ISO 27002: Lijst van best practices met aanbevelingen voor informatiebeveiligingsmaatregelen.
- COBIT: Control Objectives for Information and Related Technology is een raamwerk voor het gestructureerd inrichten en beoordelen van IT-beheeromgevingen.  
Het raamwerk is uitermate geschikt voor organisaties om aan te tonen dat ze voldoen aan regelgeving, zoals bijvoorbeeld Sarbanes Oxley voorschrijft.
- 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.
- 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-NL Cloud Computing & Security: Informatie van het Nationaal Cyber Security Centrum over clouddiensten en mogelijke risico's.

Naast marktstandaarden past Visma | YouServe ook de informatiebeveiligingsprogramma's toe die voor de hele Visma-groep gelden. Via de website <https://www.visma.com/trust-centre/security/products-and-services/> 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 ondermeer 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 aan 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. In de jaarlijkse HRcyclus 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 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 persoons-, salaris- en daaraan gerelateerde gegevens en het waarborgen van de privacy van persoonsgegevens. In het kader 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 verwerkingsverantwoordelijke 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 datalekken.
- het 'privacy by design' en 'privacy by default' principe wordt gehanteerd bij software-ontwikkeling.
- er bindende verwerkersafspraken zijn gemaakt met verwerkingsverantwoordelijken en subverwerkers.

Bovengenoemde aspecten zijn onderdeel van ons privacybeleid, informatie- beveiligingsbeleid en normenkader en maakt toetsing op basis van ISAE 3402 en ISO 27001 mogelijk.

### Meldplicht datalekken

Bij inbreuk van persoonsgegevens (een 'datalek'), moet de verwerkingsverantwoordelijke dit melden bij de Autoriteit Persoonsgegevens. Behalve als het onwaarschijnlijk is dat de 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. 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 | YouServe er alles aan om een datalek te voorkomen. Gebeurt dit toch dan melden we het incident 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.

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 melding kan doen 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 verwerkingsverantwoordelijke 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 bijvoorbeeld 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 autorisatieaanvragen 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 in de relevante onderdelen Cobit en 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**

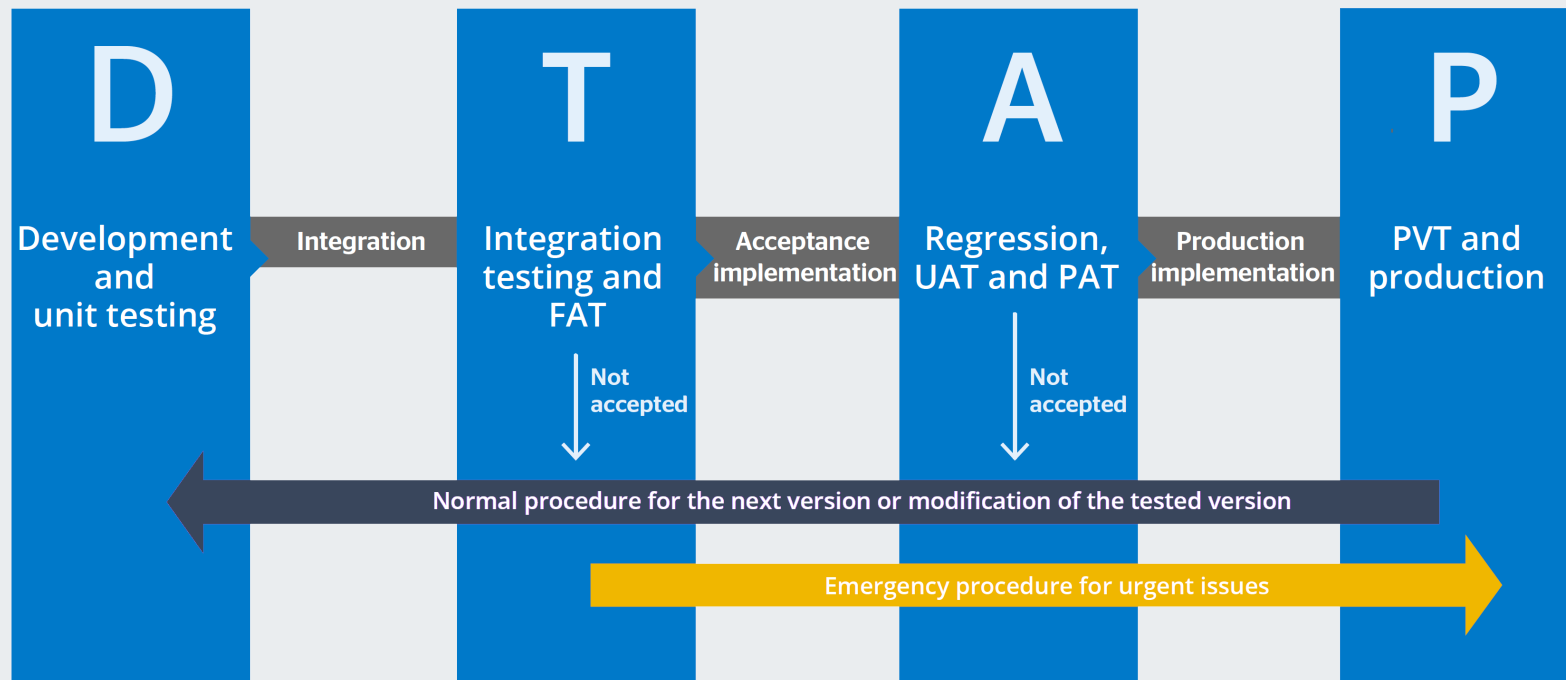
DTAP is een algemeen gebruikte afkorting voor de fasering binnen productontwikkeling: Development, Test, Acceptation en Production. Wij leveren onze systemen met een fysieke scheiding tussen de ontwikkel-, test-, acceptatie-, en de productieomgeving. Applicaties ontwikkelen we volgens een agile



ontwikkelmethodiek waarin we naast de ontwikkeling uitgebreid aandacht besteden aan verschillende testmethoden.

Het belangrijkste doel van het DTAP-model is de waarborging van een strikte scheiding tussen ontwikkel-, test- en

productieomgeving. Integriteit en beschikbaarheid van de productieomgeving speelt hierbij een belangrijke rol. We gebruiken de productieomgeving voor de dagelijkse gegevensverwerking en dienstverlening aan onze klanten.



## ► Certificaten en rapportages

Visma | YouServe beschikt over ISO 27001, ISO 9001, Data Pro en MVO certificaten, laat penetratietests uitvoeren en levert op verzoek ISAE3402 type II rapportages.

**ISAE3402 type II rapportages:** Visma | YouServe beschikt, via haar rechtsvoorganger Visma | Raet, sinds 2006 over rapportages (SOC reports) of control statements voor bedrijfsprocessen en IT-processen, de verwerking van HR- en salarissystemen en voor de BPO dienstverlening. In deze rapportages verklaart een accountant of de dienstverlening van Visma | YouServe rondom de HR en salarisverwerking en de BPO dienstverlening voor haar klanten betrouwbaar, en 'in control' is.

**ISO 27001 certificaat:** Visma | YouServe beschikt, via haar rechtsvoorganger Visma | Raet, sinds 2011 over bewijs dat de informatiebeveiliging op hoogstaand niveau geregeld is conform deze internationale standaard. In de Verklaring van Toepasselijkheid is beschreven welke onderdelen van de norm van toepassing zijn.

**ISO 9001 certificaat:** Dit certificaat is het internationale keurmerk voor het kwaliteitsmanagementsysteem. Visma | YouServe heeft, via haar rechtsvoorganger Visma | Raet, sinds 1997 een ISO 9001-certificaat. Dit wordt ieder jaar tussentijds getoetst en eens in de drie jaar vindt hercertificering plaats.

**Intrusientest rapporten:** Voor onderzoek van de weerbaarheid van systemen, netwerkinfrastructuur en applicaties die onderdeel zijn van onze dienstverlening laten we het hele jaar onafhankelijke onderzoeken uitvoeren in de vorm van intrusientests of penetratietests. Op verzoek leveren wij een samenvatting van de resultaten.

**MVO certificaat:** Bij Visma | YouServe 'we care about people'. We meten ons succes niet alleen in financiële termen, maar ook in de bijdrage aan de wereld en de samenleving. MVO gaat over maatschappelijke betrokkenheid, het verminderen van de ecologische footprint en het creëren van waarde. Visma | YouServe richt zich vooral op het hoofdspoor 'People'.

Een onafhankelijke partij heeft dit uitgewerkt en vastgelegd in een rapport en certificaat, dat wij delen met onze rechtsvoorganger Visma | Raet.

### Zekerheid uitbesteding

Sinds 2005 beschikte rechtsvoorganger Visma | Raet over een Statement on Auditing Standard number 70 (SAS70)-rapport. Met SAS70, een Amerikaanse standaard legde Visma | Raet verantwoording af over getroffen beheersmaatregelen over de aan haar uitbestede (financiële) processen.

Sinds 2010 is de Amerikaanse SAS70 standaard vervangen door de meer internationale ISAE3402 standaard. Rechtsvoorganger Visma | Raet heeft deze standaard als een van de eerste dienstverleners geïmplementeerd. Visma | YouServe zet deze wijze van zekerheid bieden voort.

De ISAE3402-mededeling is specifiek bedoeld voor gebruik bij de jaarrekeningcontrole en geeft een goed beeld hoe Visma | YouServe de HR-, salarisverwerking en bruto-netto berekeningen op beheerste wijze uitvoert en 'in control' is. Geaccrediteerde accountants voeren de beoordeling uit en stellen de rapportage op.

Klanten van Visma | YouServe kunnen het volledige digitale rapport ontvangen op basis van een geheimhoudingsverklaring. Ook bespreken we het rapport met een beperkt aantal gerenommeerde accountantsorganisaties. Zij beschikken vervolgens over het rapport voor controledoeleinden bij gezamenlijke relaties. Als wij externe dienstverleners of sub-serviceorganisaties inzetten, vragen wij ze om een eigen TPM 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. Wijzigingen vinden plaats als er:

- Wijzigingen zijn in relevante wet- en regelgeving.
- Gewijzigde normering of standaarden zijn.
- Incidenten, gewijzigd risico-inzicht of gewijzigde resultaten van de risicoanalyse zijn.
- Commerciële redenen zijn die uitbreiding van de scope verlangen.
- Een relevante wijziging is in dienstverlening en/of productportfolio.
- Wijzigingen zijn in de technische infrastructuur.
- Relevante nieuwe of gewijzigde interne processen zijn.
- (Andere) dringende redenen zijn voor uitbreiding of scoping van (bestaande) controls.

## Risicomanagement

Het risicobeleid bepaalt het risicomanagement van Visma | YouServe en is van toepassing op alle bedrijfsonderdelen en ondersteunende bedrijven. 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 hoge 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.

Als wij 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 en 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.



## Over Visma | YouServe

Elke onderneming drijft op mensen. Zij maken het verschil. Daarom is het zaak om je mensen als je grootste goed te behandelen. Ze gelukkiger te maken én te houden. Dat doe je met Human Resource Management in optima forma.

Visma | YouServe biedt je hiervoor elke vorm van ontzorging. Ongeacht waar jij bent in je HR-journey. Van het ondersteunen van je salaris- en personeelsadministratie tot het behalen van je HR-doelstellingen. Wij zijn een full service HRM & payroll dienstverlener voor het zakelijke segment. Wat ons uniek maakt is dat wij niet alleen software leveren, maar vooral een kennishuis en dienstverlener zijn. Met onze services en software optimaliseren we HR-processen en nemen we je werk uit handen. Zo houd jij tijd over voor de ultieme waardevermeerdering van je onderneming: betrokken en gelukkige medewerkers.

Vernieuwend, deskundig, betrouwbaar, relevant en nieuwsgierig tot op het bot. Altijd op zoek naar wat mensen drijft en wat ze verder brengt. Zo maken we medewerkers én ondernemingen gelukkiger. Maximaal gefaciliteerd.

Daarom werk je met Visma | YouServe. Omdat mensen je grootste kapitaal zijn.

## Contact

+31 88 23 02 700 | [info@youserve.nl](mailto:info@youserve.nl) | [youserve.nl](http://youserve.nl) | 

Omdat mensen je **grootste kapitaal** zijn