ATIMO

VERWERKERSOVEREENKOMST

ATIMO PERSONEELSTECHNIEK B.V.

Atimo® Personeelstechniek B.V. / an AtiQx holding company

Computerweg 1, 3542 DP Utrecht / Tel. +31(0)85 040 21 23 / Fax +31 (0)85 040 21 26 / verkoop@atimo.nl / www.atimo.nl
IBAN: NL71 RABO 0311 4630 61 / BIC: RABONL2U / BTW nr: NL852365780B01 / KvK: 56928270

Inhoudsopgave

VERANTWOORDING EN VASTSTELLING

Verantwoording

Dit Data Pro Statement is opgesteld door:
Atimo Personeelstechniek B.V. (hierna te noemen Atimo), Computerweg 1, 3542 DP Utrecht.

Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met de functionaris gegevensbescherming via emailadres qualityassurance.nl@dormakaba.com of telefoonnummer +31 (0)85 – 040 2123.

Document logboek

Versie	Datum	Auteur	Toelichting versie
1.0	Mei 2018	Atimo	Initiële versie
1.2	Maart 2019	Atimo	Wijziging procedure melding datalekken
1.3	Juli 2019	Atimo	Lay-out en toevoeging ondertekening (vaststelling)
1.4	Juni 2020	Atimo	Toevoeging “Atimo Online” in 1.8 van het Data Pro Statement Toevoeging 2.2.9 en 2.2.10 van de Standaardclausules voor verwerkingen
1.5	Juli 2020	Atimo	Gewijzigde bijlage2: geheimhoudingsverklaring en toevoegingen aan bijlage 6: Protocol datalekken
1.5	Juli 2023	Atimo	Wijziging 2.8.4, Verwerking van Persoonsgegevens binnen de EU/EER
1.5	Juli 2023	Atimo	Wijziging van contactgegevens
1.5	September 2023	Atimo	Wijziging 1.7, Ondersteuning vanuit Atimo voor verwijdering van data

Vaststelling

Namens Opdrachtgever :		Namens Data processor :	
Naam	: _____	Naam	: _____
Functie	: _____	Functie	: _____
Datum	: _____	Datum	: _____
Handtekening	: _____	Handtekening	: _____

1 DEEL 1 - DATA PRO STATEMENT

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen de Verwerkersovereenkomst voor het product of de dienst van Atimo personeelstechniek B.V. .

1.1 Algemene Informatie

1.1.1 Partijen

Data Processor: Atimo Personeelstechniek B.V.
Computerweg 1
3542 DP Utrecht

Opdrachtgever: < naam opdrachtgever >
< Adres >
< Postcode > < Woonplaats >

1.1.2 Versie en Ingangsdatum

Dit Data Pro Statement document betreft versie 1.5 en heeft een ingangsdatum van 1 augustus 2020.
De in dit Data Pro Statement omschreven beveiligingsmaatregelen past Atimo regelmatig aan om ten aanzien van data protectie steeds voorbereid en actueel te blijven. Wij houden u op de hoogte van nieuwe versies via onze gebruikelijke kanalen.

1.1.3 Uitzonderingen

De volgende artikelen uit deze verwerkersovereenkomst zijn voor Partijen niet van toepassing:

- DEEL I Data Pro Statement
  - *Geen uitzonderingen*
- DEEL II Standaardclausules voor verwerking
  - *Geen uitzonderingen*
- BIJLAGEN
  - *Geen uitzonderingen*

1.2 Producten en Diensten

Dit Data Pro Statement is van toepassing op de volgende producten en diensten van Atimo.

1.2.1 Producten en Diensten

A. Time-Wize

B. Time-Wize Experience

C. Time-Wize Saphir

D. Consultancy voor de inrichting van bovengenoemde software applicaties

** Doorgehaalde Producten en/of Diensten zijn niet van toepassing binnen deze Verwerkersovereenkomst.*

1.2.2 Nadere toelichting

Voor A, B en C:
De software kan on-premise worden geïnstalleerd of beschikbaar zijn als SaaS (Atimo Online). Deze software kan worden ingezet voor alle branches waarbij de basisfunctionaliteit de registratie en verdere berekening van gewerkte uren van medewerkers/uitzendkrachten/inleners is. Deze gewerkte uren kunnen worden verbijzonderd: op kostenplaats/product/werkorder. Bij het gebruik van de module toegangsbeheer kunnen medewerkers worden geautoriseerd om ergens wel of niet naar binnen te mogen (terrein, pand, afdeling).

Er kunnen diverse interfaces worden ingesteld naar HRM- en ERP applicaties. Vanuit de ESS (Employee Self Service) en Management Self Service (MSS) functionaliteit kunnen medewerkers afwezigheden aanvragen en leidinggevenden (Management Self Service) hebben inzage in de bezetting op een afdeling om op basis daarvan verlofaanvragen te accorderen. De smartphone, tablet en laptop kunnen gebruikt worden voor ESS-gebruik. Met diezelfde smartphone kan een medewerker “klokken”, afwezigheden opgeven en heeft de medewerker inzicht in zijn/haar kloktijden.

Voor D:
Voor de inrichting van de applicatie biedt Atimo consultancy aan. Deze consultancy kan op locatie bij de klant worden uitgevoerd of desgewenst op kantoor bij Atimo. De specifieke consultancy zorgt ervoor dat het product wordt ingericht volgens de scope waarin de opdrachtgever de regelgeving en de instellingen heeft gedefinieerd. Dat kan een CAO zijn, bedrijfsregelingen of individuele regelingen.

1.3 Beoogd gebruik

Producten A, B en C zijn ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:

Atimo ontwikkelt in eigen beheer software voor urenmanagement, de basis is de berekening van gewerkte uren. Afhankelijk van de wijze van registreren van een medewerker kan het in bepaalde situaties relevant zijn dat, naast de naam, een uniek criterium van belang is. Bijvoorbeeld een pasnummer, een pincode, een barcode of een vingertemplate (biometrie). Indien een medewerker “klokt” met een smartphone dan is de smartphone feitelijk aan de medewerker gekoppeld. Maakt de medewerker gebruik van een tijdregistratieterminal dan is een identificatie van belang.

De stamgegevens van een medewerker kunnen vrij basaal worden ingevuld om het systeem te laten functioneren (pasnummer, naam en rooster). Opdrachtgevers kunnen op basis van bepaalde criteria selecties maken en dat impliceert dat het veld stamgegevens van een medewerker vrij te definiëren is. Dat wil zeggen dat bij product A, B en C in overleg met de opdrachtgever, de stamgegevens van een medewerker kunnen worden uitgebreid.

Gelet op de flexibiliteit in de inrichting van de softwareapplicatie is het uiteindelijk aan de opdrachtgever welke persoonsgegevens in de producten A, B en C worden vastgelegd.

Bij dit product is rekening gehouden met de verwerking van bijzondere persoonsgegevens.

In het geval de opdrachtgever gebruik maakt van biometrische lezing voor tijdregistratie- en/of toegangscontrole dan heeft Atimo maatregelen genomen die zijn vastgelegd in bijlage 1.

1.4 Privacy by Design

Atimo heeft bij het ontwerpen van haar producten *Privacy by Design* op de volgende wijze toegepast.

1.4.1 Medewerker gegevens

Het uitgangspunt is dat er standaard zo min mogelijk gegevens van medewerkers worden vastgelegd die nodig zijn voor het registeren en verantwoorden van uren. Indien er voor de juiste berekeningen aanvullende gegevens van een medewerker vastgelegd dienen te worden is het mogelijk deze af te schermen en via autorisaties in te stellen wie daartoe wel de mogelijkheid heeft. In overleg met de opdrachtgever wordt bepaald welke gegevens vastgelegd dienen te worden. In de (tijd-/toegangs) terminals wordt naast eventueel naam geen medewerker gegevens vastgelegd waarbij in een toegangsterminal ook geen naam van de medewerker wordt gekoppeld.

Deze autorisatie gebeurt op basis van een uniek criterium waarbij er een referentie is met betrekking tot de geheugenlocatie en de medewerker.

1.4.2 Data beveiliging

Bij data-export en waarbij gebruik wordt gemaakt van de back-up tool Time-Wize databasemanager worden de gegevens standaard geanonimiseerd en encrypted met een zelf te bepalen wachtwoord. Hiermee is het mogelijk om offside de verdere configuratie te realiseren en eventuele probleemanalyses uit te voeren.

Bij Atimo Online is het volgende relevant om te vermelden:

- Standaard wordt SSL toegepast (Data verbinding encryptie)
- Toepassing van Transparent Data Encryption (TDE*) - encrypts SQL Server
- Standaard 2 factor authentication (Saphir) (Gepland voor 4de kwartaal 2020)
- Passwordpolicy dat wil zeggen verplicht wachtwoordcomplexiteit en wachtwoord wijzigen na maximaal 90 dagen.

* Wat is TDE?
TDE voert real-time I/O-codering en decodering van de gegevens en logbestanden uit.
De codering gebruikt een databasecoderingssleutel (DEK), die in het opstartrecord van de database wordt opgeslagen voor beschikbaarheid tijdens herstel. De DEK is een symmetrische sleutel die is beveiligd door een certificaat te gebruiken dat is opgeslagen in de hoofddatabase van de server of door een asymmetrische sleutel die wordt beschermd door een EKM-module. TDE beschermt gegevens "in rust", dat wil zeggen de gegevens en logbestanden. TDE biedt de mogelijkheid om te voldoen aan vele wetten, voorschriften en richtlijnen die in verschillende industrieën zijn vastgesteld.

Atimo levert een standaard applicatie die klant-specifiek wordt ingericht. Op het moment dat een opdrachtgever een issue meldt over de werking van de softwareapplicatie dan kan Atimo een back-up opvragen om een situatie bij haar op kantoor te simuleren.

Atimo maakt gebruik van een volledig nieuwe manier om een dump aan te leveren. Deze supporttool - Time-Wize databasemanager - is speciaal ontwikkeld naar aanleiding van de bepalingen in de AVG. De functionaliteiten waar Time-Wize databasemanager over beschikt, zorgen ervoor dat het aan de nieuwe regels wat betreft dataminimalisatie voldoet. Met Time-Wize databasemanager wordt een dump (back-up) van de gegevens uit Time-Wize gemaakt. In Time-Wize databasemanager worden de gegevens van de medewerkers automatisch geanonimiseerd, bepaalde gegevens worden niet getoond of het wordt zo ingevuld dat er niet na te gaan is over wie de informatie gaat.

De medewerkers zijn hierbij alleen nog te herkennen aan een uniek nummer. De gegevens worden hierbij samengevoegd in één bestand dat vervolgens wordt opgeslagen en versleuteld met een door de klant gekozen

wachtwoord. Zonder wachtwoord van de klant kan Atimo de dump niet gebruiken. Deze dump wordt samen met het password via de Atimo supportsite verstuurd. Na ontvangst kan de consultant op basis van deze dump en de beschreven probleemstelling van de klant aan de slag. Dat betekent dat terugkoppeling van de oplossing door de consultant gebeurt op basis van het unieke nummer of de fictieve naam die aan de persoon is gekoppeld.

Als een klant gebruik maakt van Atimo Online waarbij de data is geplaatst bij onze outsourcing partij Sentia, dan zal Atimo voor het simuleren van een issue dezelfde procedure volgen als hierboven beschreven.

1.5 Data Pro Standaardclausule

Atimo gebruikt de Data Pro Standaardclausules voor verwerkingen, welke als deel 2 aan dit document is toegevoegd.

1.6 Subverwerker

Atimo maakt gebruik van de volgende subverwerker(s):

Sentia B.V.
Einsteinbaan 4
3439 NJ Nieuwegein
Kamer van Koophandel 34124933

Sentia verzorgt bedrijfskritische IT-outsourcing op de door Atimo geleverde applicaties.
Sentia heeft kantoren in Amsterdam, Nieuwegein en Delft. Er zijn meer dan 115 continuïteits-engineers en -architects 24/7 werkzaam die 365 dagen per jaar paraat zijn om IT systemen en -platforms veilig te laten functioneren. Sentia is ISO 9001, ISO 27001, ISO 14001 en NEN 7510 gecertificeerd. Daarnaast kent Sentia een ISAE 3402 type 2 rapportage.

1.7 Ondersteuning vanuit Atimo

Atimo bewaart de geanonimiseerde back-up niet langer dan strikt noodzakelijk om op basis van een ingelegde call van een opdrachtgever een specifiek issue te simuleren. In geval van Atimo Online bewaart Atimo de gegevens voor een periode van maximaal 7 jaar. De bewaartermijn is de verantwoordelijkheid van de opdrachtgever. De opdrachtgever geeft Atimo schriftelijk opdracht om door haar gedefinieerde gegevens te verwijderen. Meer in zijn algemeenheid geeft de opdrachtgever Atimo schriftelijke instructies (zie artikel 2.3 deel 2 standaardclausules voor verwerkingen).

In dat kader is het van belang dat de opdrachtgever Atimo adequaat informeert over geautoriseerde medewerkers en dat ook personele wijzigingen in het applicatiebeheer, wijziging van bevoegdheden etc. aan Atimo wordt doorgegeven. Atimo kan geen verantwoording nemen voor het niet nakomen van deze afspraak.
Wij verwijzen hiervoor naar bijlage 3.

Aan het uitvoeren van deze werkzaamheden kunnen kosten verbonden zijn die zullen worden doorbelast. Atimo zal de opdrachtgever informeren als de gegevens zijn verwijderd. Indien de applicatie on-premise draait is het de verantwoordelijkheid van de opdrachtgever die zelf een periode kan bepalen. Atimo heeft hierop geen invloed. In geval van Atimo Online zal bij de beëindiging van de Service Level Agreement en nadat alle gegevens zijn verwijderd ook de Verwerkersovereenkomst worden beëindigd.

Het recht op dataportabiliteit betreft het recht om gegevens over te laten dragen in een gestructureerd, gangbaar en machine-leesbaar formaat. Atimo is wettelijk verplicht om binnen één maand schriftelijk of per email te reageren op een dergelijk verzoek. Bij complexe dataverzoeken heeft Atimo wettelijk gezien maximaal drie maanden de tijd om deze aan te leveren. Atimo zal de informatie in een gangbaar formaat aanleveren (csv). De tijd die hiermee gemoeid is, zal Atimo tegen het geldende helpdesktarief in rekening brengen bij de opdrachtgever.

1.8 Beëindiging van de overeenkomst

1.8.1 Verwijderen van persoonsgegevens

Na beëindiging van de overeenkomst met een opdrachtgever verwijdert Atimo de persoonsgegevens die hij voor opdrachtgever verwerkt binnen Atimo Online in principe binnen 3 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).

In de Service Level Agreement zoals Atimo die met de opdrachtgever is overeengekomen, is in artikel 13 opgenomen dat opdrachtgever de gegevens na beëindiging van de overeenkomst kan opvragen. Hier zijn kosten aan verbonden. Atimo zal met de opdrachtgever de inhoud daarvan afstemmen. Atimo zal bij het ter beschikking stellen, gebruik maken van een certificaat.

Indien de opdrachtgever bij het opzeggen van de overeenkomst niet aangeeft dat hij in het bezit wil komen van deze gegevens, dan zal Atimo binnen 3 maanden nadat de overeenkomst is beëindigd alle gegevens verwijderen. Dat wil zeggen dat er geen toegang tot de applicatie meer is, de database wordt verwijderd en alle data. Gelet op het feit dat Sentia dagelijks back-ups maakt en deze bewaart voor de laatste 7 dagen betekent het dat Atimo met het verwijderen van de gegevens binnen de termijn van 3 maanden hiermee rekening houdt. De meest recente back-up wordt binnen 48 uur gekopieerd naar een secundaire locatie waarbij de database encrypted is.

1.8.1.1 Retourneren van persoonsgegevens

Na beëindiging van de overeenkomst met opdrachtgever retourneert Atimo alle persoonsgegevens die hij voor opdrachtgever verwerkt binnen 3 maanden op de volgende manier. Op het moment dat de opdrachtgever de overeenkomst beëindigt en aangeeft de gegevens te willen ontvangen en akkoord te gaan met de kosten die hieruit voorvloeien, dan zal Atimo een volledige SQL back-up aan de opdrachtgever ter beschikking stellen.

1.9 Beveiligingsbeleid

1.9.1 Beveiligingsmaatregelen

Voor de gebruikers van Atimo Online verwijzen wij naar bijlage 4 Overview Security Measures Sentia Cloud.

Atimo maakt gebruik van informatie- en communicatietechnologie. Atimo draagt er nadrukkelijk zorg voor dat alle van opdrachtgever ontvangen gegevens, waarvan men weet of redelijkerwijs behoort te weten dat deze van vertrouwelijke aard zijn, geheim blijven. Atimo zal deze slechts gebruiken voor het doel waarvoor deze verstrekt zijn. Het is hierbij belangrijk dat zorgvuldig met klantgegevens wordt omgegaan. Dat betekent dat er door Atimo passende technische en organisatorische maatregelen zijn genomen om deze te beschermen. De getroffen beveiligingsmaatregelen moeten er kortom op gericht zijn onjuist gebruik binnen en buiten de Atimo-organisatie tegen te gaan.

De door de opdrachtgever verstrekte geanonimiseerde back-ups zijn vanwege de taken voortkomend uit hun functie in te zien door:

- Consultants van de support-afdeling
- Consultants van de R&D afdeling
- Projectconsultants.

Andere medewerkers kunnen back-ups niet inzien. Degenen die inzage hebben in back-ups hebben geheimhoudingsplicht zoals vastgelegd in de bijlage 2. De geheimhoudingsplicht is ook vastgelegd in de individuele arbeidsovereenkomsten en het personeelshandboek dat Atimo hanteert. Atimo en Sentia zullen al het mogelijke doen om fysieke en logische toegang tot gegevens door onbevoegden te voorkomen en om informatie van de opdrachtgever geheim te houden. Voor de borging van veiligheid en vertrouwelijkheid richten Sentia en Atimo hun systemen en uitvoeringspraktijk zodanig in dat het risico op toegang tot gegevens en ontsluiting van informatie door onbevoegden minimaal is.

1.9.2 Kwaliteitsnorm

Atimo heeft zich geconformeerd aan de volgende kwaliteitsnorm:

- NEN-ISO-9001:2015

Atimo zal in het kader van artikel 2.7 van de standaardclausules voor verwerkingen een register bijhouden van activiteiten die voor de opdrachtgever worden uitgevoerd. Dit kan periodiek bij Atimo worden opgevraagd.

1.10 Datalek protocol

1.10.1 Meldplicht datalekken

1. Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens zoals bedoeld in de AVG. De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking. Datalekken kunnen onder andere ontstaan door:
   - moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, mailware besmetting);
   - technisch falen (ICT-storingen);
   - menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username/wachtwoord aan collega's en externen);
   - calamiteit (brand datacentrum, wateroverlast);
   - verloren USB stick of laptop;
   - het onrechtmatig verwerken van gegevens.

2. Atimo dient de verwerkingsverantwoordelijke (Opdrachtgever) in kennis te stellen van iedere inbreuk op de beveiliging (van welke aard dan ook) die (mede) betrekking heeft of kan hebben op de verwerking van Persoonsgegevens. Dit dient binnen 24 uur gemeld te worden nadat een datalek bij Atimo bekend is geworden. Daartoe zal Atimo, indien en voor zover mogelijk, de in bijlage 6 bedoelde informatie verstrekken zodat de verwerkingsverantwoordelijke indien nodig melding kan doen bij de toezichthoudende autoriteit.

3. Atimo informeert verwerkingsverantwoordelijke ook na de melding op grond van artikel 5.1 van de overeenkomst over ontwikkelingen betreffende het datalek en de maatregelen die Atimo, indien van toepassing en voor zover redelijkerwijs van haar verwacht mag worden, heeft genomen om de omvang van het datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen.

4. Atimo erkent dat verwerkingsverantwoordelijke onder omstandigheden wettelijk verplicht is om een inbreuk op de beveiliging (van welke aard dan ook) die (mede) betrekking heeft of kan hebben op de Persoonsgegevens die Atimo verwerkt, aan autoriteiten en/of betrokkenen te melden. Een dergelijke melding door verwerkingsverantwoordelijke zal nimmer als tekortkoming in de nakoming van deze overeenkomst of onderliggende overeenkomst of anderszins als onrechtmatige handeling worden beschouwd. Atimo zal alle maatregelen treffen die redelijkerwijs van haar verwacht mag worden om de (mogelijke) schade te beperken en verwerkingsverantwoordelijke ondersteunen bij meldingen aan betrokkenen en/of autoriteiten.

2 DEEL II – STANDAARDCLAUSULES VOOR VERWERKINGEN

versie: juli 2020

Vormt samen met het Data Pro Statement de Verwerkersovereenkomst en is een bijlage bij de Overeenkomst en de daarbij behorende bijlagen zoals toepasselijke algemene voorwaarden

2.1 Definities

Onderstaande begrippen hebben in deze Standaardclausules voor verwerkingen, in het Data Pro Statement en in de Overeenkomst de volgende betekenis:

a) **Autoriteit Persoonsgegevens (AP)**: toezichthoudende autoriteit, zoals omschreven in artikel 4, sub 21 AVG.

b) **AVG**: de Algemene Verordening Gegevensbescherming.

c) **Data Processor**: partij die als ICT-leverancier in het kader van de uitvoering van de Overeenkomst als verwerker Persoonsgegevens verwerkt ten behoeve van diens Opdrachtgever.
Zie §1.1.1 in deel 1 van het Data Pro Statement.

d) **Data Pro Statement**: statement van Data Processor waarin hij onder andere informatie geeft met betrekking tot het beoogd gebruik van zijn product of dienst, getroffen beveiligingsmaatregelen, sub-verwerkers, datalekken, certificeringen en omgang met rechten van Data subjects.

e) **Data subject (betrokkene)**: een geïdentificeerde of identificeerbare natuurlijke persoon wiens persoonsgegevens worden verwerkt.

f) **Opdrachtgever**: partij in wiens opdracht Data Processor persoonsgegevens verwerkt. De Opdrachtgever kan zowel verwerkingsverantwoordelijke (“controller”) zijn als een andere verwerker.
Zie §1.1.1 in deel 1 van het Data Pro Statement.

g) **Overeenkomst**: de tussen Opdrachtgever en Data Processor geldende overeenkomst, op basis waarvan de ICT-leverancier diensten en/of producten levert aan Opdrachtgever, waarvan de Verwerkersovereenkomst onderdeel vormt.

h) **Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals omschreven in artikel 4, sub 1 AVG, die Data Processor in het kader van de uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst verwerkt.

i) **Verwerkersovereenkomst**: deze Standaardclausules voor verwerkingen, die tezamen met het Data Pro Statement (of vergelijkbare informatie) van Data Processor de Verwerkersovereenkomst vormen als bedoeld in artikel 28, lid 3 AVG.

2.2 Algemeen

2.2.1 Toepassingsgebied

Deze Standaardclausules voor verwerkingen zijn van toepassing op alle verwerkingen van Persoonsgegevens die Data Processor doet in het kader van de levering van zijn producten en diensten en op alle Overeenkomsten en aanbiedingen. De toepasselijkheid van Verwerkersovereenkomsten van Opdrachtgever wordt uitdrukkelijk van de hand gewezen.

2.2.2 Aanpassingen op het Data Pro Statement

Het Data Pro Statement, en met name de daarin opgenomen beveiligingsmaatregelen, kan van tijd tot tijd door Data Processor worden aangepast aan veranderende omstandigheden. Data Processor zal Opdrachtgever van significante aanpassingen op de hoogte stellen. Indien Opdrachtgever in redelijkheid niet akkoord kan gaan met de aanpassingen, is Opdrachtgever gerechtigd binnen 30 dagen na kennisgeving van de aanpassingen de Verwerkersovereenkomst schriftelijk gemotiveerd op te zeggen.

2.2.3 Basis voor verwerking

Data Processor verwerkt de Persoonsgegevens namens en in opdracht van Opdrachtgever overeenkomstig de met Data Processor overeengekomen schriftelijke instructies van Opdrachtgever.

2.2.4 Verwerkingsverantwoordelijke

Opdrachtgever, dan wel diens klant, is de verwerkingsverantwoordelijke in de zin van de AVG, heeft de zeggenschap over de verwerking van de Persoonsgegevens en heeft het doel van en de middelen voor de verwerking van de Persoonsgegevens vastgesteld.

2.2.5 Verwerker

Data Processor is verwerker in de zin van de AVG en heeft daarom geen zeggenschap over het doel van en de middelen voor de verwerking van de Persoonsgegevens en neemt derhalve geen beslissingen over onder meer het gebruik van de Persoonsgegevens.

2.2.6 Uitvoering

Data Processor geeft uitvoering aan de AVG zoals neergelegd in deze Standaardclausules voor verwerkingen, het Data Pro Statement en de Overeenkomst. Het is aan Opdrachtgever om op basis van deze informatie te beoordelen of Data Processor afdoende garanties biedt met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van de AVG voldoet en de bescherming van de rechten van Data subjects voldoende zijn gewaarborgd.

2.2.7 AVG-verplichting Opdrachtgever

Opdrachtgever staat er tegenover Data Processor voor in dat hij conform de AVG handelt, dat hij zijn systemen en infrastructuur te allen tijde adequaat beveiligt en dat de inhoud, het gebruik en/of de verwerking van de Persoonsgegevens niet onrechtmatig zijn en geen inbreuk maken op enig recht van een derde.

2.2.8 Opgelegde bestuurlijke boete

Een aan Opdrachtgever door de AP opgelegde bestuurlijke boete in het kader van een schending van de AVG kan niet worden verhaald op Data Processor.

2.2.9 Vrijwaring

Opdrachtgever zal Data Processor vrijwaren van aanspraken van derden in verband met de uitvoering van deze Verwerkersovereenkomst, tenzij Opdrachtgever aantoont dat deze aanspraken een (rechtstreeks) gevolg zijn van een tekortkoming van Data Processor in de uitvoering van deze Verwerkersovereenkomst.

2.2.10 Geheimhouding

Na beëindiging van deze Verwerkersovereenkomst blijven de bepalingen, die naar hun aard bestemd zijn om ook nadien van kracht te blijven, waaronder begrepen de geheimhoudingsverplichting (2.5) en de vrijwaring (2.2.8 en 2.2.9), onverminderd van kracht.

2.3 Beveiliging

2.3.1 Beveiligingsmaatregelen

Data Processor treft de technische en organisatorische beveiligingsmaatregelen, zoals omschreven in zijn Data Pro Statement. Bij het treffen van de technische en organisatorische beveiligingsmaatregelen heeft Data Processor rekening gehouden met de stand van de techniek, de uitvoeringskosten van de beveiligingsmaatregelen, de aard, omvang en de context van de verwerkingen, de doeleinden en het beoogd gebruik van zijn producten en diensten, de verwerkingsrisico's en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van Data subjects die hij gezien het beoogd gebruik van zijn producten en diensten mocht verwachten.

2.3.2 Bijzondere categorieën van Persoonsgegevens

Tenzij expliciet anders vermeld in het Data Pro Statement is het product of de dienst van Data Processor niet ingericht op de verwerking van bijzondere categorieën van Persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten.

2.3.3 Aard van beveiligingsmaatregelen

Data Processor streeft ernaar dat de door hem te treffen beveiligingsmaatregelen passend zijn voor het door Data Processor beoogde gebruik van het product of de dienst.

2.3.4 Niveau van beveiligingsmaatregelen

De omschreven beveiligingsmaatregelen bieden, naar het oordeel van de Opdrachtgever, rekening houdend met de in artikel 2.3.1 genoemde factoren een op het risico van de verwerking van de door hem gebruikte of verstrekte Persoonsgegevens afgestemd beveiligingsniveau.

2.3.5 Aanpassen van beveiligingsmaatregelen

Data Processor kan wijzigingen aanbrengen in de getroffen beveiligingsmaatregelen indien dat naar zijn oordeel noodzakelijk is om een passend beveiligingsniveau te blijven bieden. Data Processor zal belangrijke wijzigingen vastleggen, bijvoorbeeld in een aangepast Data Pro Statement, en zal Opdrachtgever waar relevant van die wijzigingen op de hoogte stellen.

2.3.6 Verzoek tot Aanpassing van beveiligingsmaatregelen

Opdrachtgever kan Data Processor verzoeken nadere beveiligingsmaatregelen te treffen. Data Processor is niet verplicht om op een dergelijk verzoek wijzigingen door te voeren in zijn beveiligingsmaatregelen. Data Processor kan de kosten verband houdende met de op verzoek van Opdrachtgever doorgevoerde wijzigingen in rekening brengen bij Opdrachtgever. Pas nadat de door Opdrachtgever gewenste gewijzigde beveiligingsmaatregelen schriftelijk zijn overeengekomen en ondertekend door Partijen, heeft Data Processor de verplichting deze beveiligingsmaatregelen daadwerkelijk te implementeren.

2.4 Inbreuk in verband met Persoonsgegevens

2.4.1 Melding van inbreuk Persoonsgegevens aan Opdrachtgever

Data Processor staat er niet voor in dat de beveiligingsmaatregelen onder alle omstandigheden doeltreffend zijn. Indien Data Processor een inbreuk in verband met Persoonsgegevens (zoals bedoeld in artikel 4 sub 12 AVG) ontdekt, zal hij Opdrachtgever zonder onredelijke vertraging informeren, doch uiterlijk binnen 24 uur nadat de inbreuk door Data Processor is vastgesteld. In het Data Pro Statement (onder datalekprotocol) is vastgelegd op welke wijze Data Processor Opdrachtgever informeert over inbreuken in verband met Persoonsgegevens.

2.4.2 Melding van inbreuk Persoonsgegevens aan AP of Data subject

Het is aan de verwerkingsverantwoordelijke (Opdrachtgever, of diens klant) om te beoordelen of de inbreuk in verband met Persoonsgegevens waarover Data Processor heeft geïnformeerd gemeld moet worden aan de AP of Data subject. Het melden van inbreuken in verband met Persoonsgegevens, die op grond van artikel 33 en 34 AVG moeten worden gemeld aan de AP en/of Data subjects, blijft te allen tijde de verantwoordelijkheid van de verwerkingsverantwoordelijke (Opdrachtgever of diens klant). Data Processor is niet verplicht tot het melden van inbreuken in verband met persoonsgegevens aan de AP en/of de Betrokkene en zal deze derhalve niet aan de AP en/of de Betrokkene melden. Deze verantwoordelijkheid ligt uitsluitend bij de Opdrachtgever.

Data Processor zal, indien nodig, nadere informatie verstrekken over de inbreuk in verband met Persoonsgegevens en zal zijn medewerking verlenen aan noodzakelijke informatievoorziening aan Opdrachtgever ten behoeve van een melding als bedoeld in artikel 33 en 34 AVG.

2.4.3 Doorbelasten van kosten aan Opdrachtgever

Data Processor kan de redelijke kosten die hij in dit kader maakt in rekening brengen bij Opdrachtgever tegen zijn dan geldende tarieven.

2.5 Geheimhouding

2.5.1 Geheimhoudingsplicht

Data Processor waarborgt dat de personen die onder zijn verantwoordelijkheid Persoonsgegevens verwerken een geheimhoudingsplicht hebben.

2.5.2 Verstrekken van Persoonsgegevens aan derden

Data Processor is gerechtigd de Persoonsgegevens te verstrekken aan derden, indien en voor zover verstrekking noodzakelijk is ingevolge een rechterlijke uitspraak, een wettelijk voorschrift of op basis van een bevoegd gegeven bevel van een overheidsinstantie.

2.5.3 Vertrouwelijkheid van informatie

Alle door Data Processor aan Opdrachtgever verstrekte toegangs- en/of identificatiecodes, certificaten, informatie omtrent toegangs- en/of wachtwoordenbeleid en alle door Data Processor aan Opdrachtgever verstrekte informatie die invulling geeft aan de in het Data Pro Statement opgenomen technische en organisatorische beveiligingsmaatregelen zijn vertrouwelijk en zullen door Opdrachtgever als zodanig worden behandeld en slechts aan geautoriseerde medewerkers van Opdrachtgever kenbaar worden gemaakt (zoals gedefinieerd in bijlage 3). Opdrachtgever ziet erop toe dat zijn medewerkers de verplichtingen uit dit artikel naleven.

2.6 Looptijd en beëindiging

2.6.1 Onderdeel van de Overeenkomst

Deze Verwerkersovereenkomst maakt onderdeel uit van de Overeenkomst en iedere daaruit voortkomende nieuwe of nadere overeenkomst, treedt in werking op het moment van totstandkoming van de Overeenkomst en wordt gesloten voor onbepaalde tijd.

2.6.2 Beëindiging van deze Verwerkersovereenkomst

Deze Verwerkersovereenkomst eindigt van rechtswege bij beëindiging van de Overeenkomst of enige nieuwe of nadere overeenkomst tussen partijen.

2.6.3 Verwijderen van Persoonsgegevens bij beëindiging

Data Processor zal, in geval van einde van de Verwerkersovereenkomst, alle onder zich zijnde en van Opdrachtgever ontvangen Persoonsgegevens binnen de in het Data Pro Statement opgenomen termijn verwijderen op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessable), of, indien overeengekomen, in een machine leesbaar formaat terug bezorgen aan de Opdrachtgever.

2.6.4 Kosten bij beëindiging Verwerkersovereenkomst

Data Processor kan eventuele kosten die hij maakt in het kader van het in artikel 2.6.3 gestelde in rekening brengen bij Opdrachtgever. Hierover kunnen nadere afspraken worden neergelegd in het Data Pro Statement.

2.6.5 Staken van verwijderen van Persoonsgegevens bij beëindiging

Het bepaalde in artikel 2.6.3 geldt niet indien een wettelijke regeling het geheel of gedeeltelijk verwijderen of terugbezorgen van de Persoonsgegevens door Data Processor belet. In een dergelijk geval zal Data Processor de Persoonsgegevens enkel blijven verwerken voor zover noodzakelijk uit hoofde van zijn wettelijke verplichtingen. Het bepaalde in artikel 6.3 geldt eveneens niet indien Data Processor verwerkingsverantwoordelijke in de zin van de AVG is ten aanzien van de Persoonsgegevens.

2.7 Rechten Data subject, Data Protection Impact Assessment (DPIA) en Auditrechten

2.7.1 Rechten van Data subject

Data Processor zal, waar mogelijk, zijn medewerking verlenen aan redelijke verzoeken van Opdrachtgever die verband houden met bij Opdrachtgever door Data subjects ingeroepen rechten van Data subjects. Indien Data Processor direct door een Data subject wordt benaderd, zal hij deze waar mogelijk doorverwijzen naar Opdrachtgever.

2.7.2 Data Protection Impact Assessment

Indien Opdrachtgever daartoe verplicht is, zal Data Processor na een daartoe redelijk gegeven verzoek zijn medewerking verlenen aan een gegevensbeschermingseffectbeoordeling (DPIA) of een daaropvolgende voorafgaande raadpleging zoals bedoeld in artikel 35 en 36 AVG.

2.7.3 Verwijderingsverzoeken

Data Processor zal zijn medewerking verlenen aan verzoeken van Opdrachtgever tot het verwijderen van persoonsgegevens voor zover Opdrachtgever dit niet zelf kan uitvoeren.

2.7.4 Data Pro Statement

Data Processor kan de naleving van zijn verplichtingen op grond van de Verwerkersovereenkomst aantonen door middel van een geldig Data Pro Certificaat of daaraan ten minste gelijkwaardig certificaat of auditrapport (Third Party Memorandum) van een onafhankelijke deskundige, indien hij over een dergelijk certificaat of auditrapport beschikt.

2.7.5 Controleren van de naleving van de afspraken

Data Processor zal daarnaast op verzoek van Opdrachtgever alle verdere informatie ter beschikking stellen die in redelijkheid nodig is om nakoming van de in deze Verwerkersovereenkomst gemaakte afspraken aan te tonen. Indien Opdrachtgever desondanks aanleiding heeft aan te nemen dat de verwerking van Persoonsgegevens niet conform de Verwerkersovereenkomst plaatsvindt, dan kan hij maximaal éénmaal per jaar door een onafhankelijke, gecertificeerde, externe deskundige die aantoonbaar ervaring heeft met het soort verwerkingen dat op basis van de Overeenkomst wordt uitgevoerd, op kosten van de Opdrachtgever hiernaar een audit laten uitvoeren. De audit zal beperkt zijn tot het controleren van de naleving van de afspraken met betrekking tot verwerking van de Persoonsgegevens zoals neergelegd in deze Verwerkersovereenkomst. De deskundige zal een geheimhoudingsplicht hebben ten aanzien van hetgeen hij aantreft en zal alleen datgene rapporteren aan Opdrachtgever dat een tekortkoming oplevert in de nakoming van verplichtingen die Data Processor heeft op grond van deze Verwerkersovereenkomst. De deskundige zal een afschrift van zijn rapport aan Data Processor verstrekken. Data Processor kan een audit of instructie van de deskundige weigeren indien deze naar zijn mening in strijd is met de AVG of andere wetgeving of een ontoelaatbare inbreuk vormt op de door hem getroffen beveiligingsmaatregelen.

2.7.6 Verbetermaatregelen

Partijen zullen zo snel mogelijk in overleg treden over de uitkomsten in het rapport. Partijen zullen de voorgestelde verbetermaatregelen die in het rapport zijn neergelegd opvolgen voor zover dat van hen in redelijkheid kan worden verwacht. Data Processor zal de voorgestelde verbetermaatregelen doorvoeren voor zover deze naar zijn oordeel passend zijn rekening houdend met de verwerkingsrisico's verbonden aan zijn product of dienst, de stand van de techniek, de uitvoeringskosten, de markt waarin hij opereert, en het beoogd gebruik van het product of de dienst.

2.7.7 Kosten inzake voorgestelde verbetermaatregelen

Data Processor heeft het recht om de kosten die hij maakt in het kader van het in dit artikel gestelde in rekening te brengen bij Opdrachtgever.

2.8 Sub-verwerkers

2.8.1 Gebruik van derde partijen (sub-verwerkers)

Data Processor heeft in het Data Pro Statement vermeld of, en zo ja welke derde partijen (sub-verwerkers) Data Processor inschakelt bij de verwerking van de Persoonsgegevens.

2.8.2 Toestemming tot gebruik van derde partijen (sub-verwerkers)

Opdrachtgever geeft toestemming aan Data Processor om andere sub-verwerkers in te schakelen ter uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst.

2.8.3 Wijziging in het gebruik van derde partijen (sub-verwerkers)

Data Processor zal Opdrachtgever informeren over een wijziging in de door de Data Processor ingeschakelde derde partijen bijvoorbeeld middels een aangepast Data Pro Statement. Opdrachtgever heeft het recht bezwaar te maken tegen voornoemde wijziging door Data Processor. Data Processor draagt ervoor zorg dat de door hem ingeschakelde derde partijen zich aan eenzelfde beveiligingsniveau committeren ten aanzien van de bescherming van de Persoonsgegevens als het beveiligingsniveau waaraan Data Processor jegens Opdrachtgever is gebonden op grond van het Data Pro Statement.

2.8.4 Verwerking van Persoonsgegevens binnen de EU/EER

Data Processor (en de eventueel door haar ingeschakelde sub-verwerkers) verwerkt de persoonsgegevens van zijn opdrachtgevers binnen de EU/EER. De Data Processor zal voor opdrachtgevers in landen buiten de EU/EER ook persoonsgegevens verwerken indien de Europese Commissie (EC) volgens een adequaatheidsbesluit heeft vastgesteld dat het beveiligingsniveau passend is.

2.9 Overige bepalingen

2.9.1 Rechten en Plichten gerelateerde overeenkomsten

Deze Standaardclausules voor verwerkingen vormen tezamen met het Data Pro Statement een integraal onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst, waaronder begrepen de van toepassing zijnde algemene voorwaarden en/of beperkingen van aansprakelijkheid, zijn derhalve ook van toepassing op de Verwerkersovereenkomst.

3 BIJLAGEN

3.1 **BIJLAGE 1** – Biometrische gegevens voor tijdregistratie en/of toegangscontrole

Binnen het productenpakket van Atimo kunnen biometrische lezers worden toegepast voor tijdregistratie- en toegangscontroletoepassingen. Biometrie wordt gezien als bijzonder persoonsgegeven. In het kader van naleving van de AVG kan in veel gevallen voor een tijdregistratietoepassing een alternatief worden geboden op dezelfde terminal door gebruik te maken van voorhoudlezing of een pincode. Voor toegangscontrole is biometrische lezing toegestaan.

Hoe werkt het?
De biometrische lezer maakt een scan van een vingerafdruk. Dit “plaatje” wordt in de scanner al omgevormd tot een code (een hash). Deze code is de uitkomst van een algoritme en is niet meer te herleiden naar de medewerker. Het is dus onmogelijk om van een opgeslagen code binnen de applicatie via re-engineering de eigenlijke vingerafdruk te reproduceren. De code wordt zowel in de lezer als op de server opgeslagen, maar wel apart van de database. Het gevolg hiervan is dat als er een geanonimiseerde dump van de applicatie wordt gemaakt – bijvoorbeeld om een bepaalde situatie te simuleren – dan is dat exclusief het bestand met deze codes.

Een ander type biometrische lezer (Multi spectrale variant) daar wordt de scan (dat is dus niet de vingercode, maar het dieper liggende patroon) gelezen op een desktop lezer. Deze scan wordt tijdelijk opgeslagen en wordt daarna naar een controller gestuurd om er een code (hash) van te maken. Daarna wordt de scan verwijderd. In deze situatie is zowel de scan als de code indirect te herleiden naar een medewerker. Het is echter niet zo dat je direct de medewerker naam of het personeelsnummer ziet. Je moet echter ook de (beveiligde) database hebben om te kunnen bepalen welke medewerker erbij hoort.

3.2 **BIJLAGE 2** – Geheimhoudingsverklaring voor medewerkers

Ondergetekende: [volledige naam medewerker]

wonende aan de [adres, postcode] , te [plaats], verder te noemen ”Medewerker”

Neemt het volgende in aanmerking:

a) Werknemer is zich er goed van bewust dat zijn werkgever, Atimo Personeelstechniek B.V., en de aan haar gelieerde ondernemingen en klanten, er veel waarde aan hechten dat bedrijfsgevoelige zaken en/of vertrouwelijke informatie van haar/hun en/of haar/hun klanten of van relatie(s) van beiden, niet worden gedeeld met derden.
b) Het gaat daarbij om informatie die als vertrouwelijk is aangemerkt of waarvan werknemer behoort te begrijpen dat deze vertrouwelijk is en waarmee hij uit hoofde van zijn functie in contact is gekomen en/of nog zal komen.
c) Het prijsgeven van deze informatie kan namelijk schade toebrengen aan Atimo Personeelstechniek B.V. en de aan haar gelieerde ondernemingen en/of haar/hun klanten.
d) Om de voormelde redenen is werknemer bereid hiervoor een op zijn arbeidscontract aanvullende geheimhoudingsverklaring te ondertekenen.

Verklaart het volgende:

1. Inhoud van de geheimhouding

1.1 Bij de uitvoering van zijn werkzaamheden bij/voor Atimo Personeelstechniek B.V. is werknemer in contact gekomen en/of zal hij nog in contact komen met vertrouwelijke informatie.

1.2 Onder vertrouwelijke informatie als bedoeld in 1.1 wordt in ieder geval doch niet uitsluitend verstaan: gegevens van zowel Atimo Personeelstechniek B.V. als van klanten, toeleveranciers of derden zoals informatie, documenten of andere goederen, ongeacht de aard of vorm, ongeacht of deze schriftelijk, digitaal dan wel mondeling is verstrekt, die hij gericht of onbedoeld tot zich krijgt bij de uitvoering van zijn werkzaamheden, waaronder begrepen technische, financiële en zakelijke informatie, (voorgenomen) zakelijke transacties, contracten en contacten, rapporten, plannen, handels- en werkwijzen, computerprogrammatuur, broncode, computerbestanden, ontwerpen, modellen, knowhow, bedrijfsgeheimen en met name ook persoonsgegevens (ofwel elk gegeven dat tot een natuurlijk persoon herleidbaar is), ongeacht of deze informatie is aangemerkt of gemarkeerd als zijnde “vertrouwelijk” of “geheim” en waarvan werknemer weet of redelijkerwijs behoort te weten dat deze van vertrouwelijke aard is.

1.3 Werknemer zal in overeenstemming met deze verklaring alle vertrouwelijke informatie strikt geheimhouden en zal:
   a) De vertrouwelijke informatie uitsluitend gebruiken voor het doel waarvoor de vertrouwelijke informatie aan werknemer ter beschikking is gesteld;
   b) Geen vertrouwelijke informatie distribueren, bekendmaken of verspreiden aan anderen dan de personen die geautoriseerd zijn en die redelijkerwijs kennis moeten hebben van dergelijke informatie voor het doel waarvoor de vertrouwelijke informatie aan werknemer ter beschikking is gesteld;
   c) Vertrouwelijke informatie op geen enkele wijze aan derden openbaren of bekend maken, direct noch indirect, schriftelijk noch mondeling;
   d) Vertrouwelijke informatie met dezelfde zorgvuldigheid behandelen als hij zou doen met zijn eigen informatie van gelijk belang die vertrouwelijk behandelt dient te worden.

e) Alle dragers van vertrouwelijke informatie veilig bewaren en de toegang tot dergelijke dragers beperken slechts tot andere medewerkers die redelijkerwijs dergelijke toegang dienen te hebben voor het doel waarvoor de vertrouwelijke informatie aan werknemer ter beschikking is gesteld;
f) Atimo Personeelstechniek B.V. onmiddellijk in kennis stelt op het moment dat hij ervan op de hoogte is geraakt dat vertrouwelijke informatie toegankelijk is of is geweest van een ander die niet gerechtigd is toegang te hebben tot de vertrouwelijke informatie;
g) Alle instructies van Atimo Personeelstechniek B.V. of de verwerkingsverantwoor-delijke met betrekking tot het waarborgen van vertrouwelijkheid van informatie, waaronder instructies met betrekking tot omgang met persoonsgegevens zorgvuldig opvolgen.

2. Duur van de geheimhouding en teruggave gegevens

2.1. Deze geheimhouding geldt zowel tijdens als na het dienstverband van werknemer met Atimo Personeelstechniek B.V.

2.2. Op verzoek van Atimo Personeelstechniek B.V., maar in ieder geval nadat de samenwerking met Atimo Personeelstechniek B.V. is beëindigd, zal werknemer onmiddellijk alle dragers met vertrouwelijke informatie alsmede alle kopieën daarvan die in zijn bezit zijn, retourneren en vervolgens zorgdragen voor vernietiging van de vertrouwelijke informatie voor zover deze nog op dragers aanwezig is die niet aan Atimo Personeelstechniek B.V. toebehoren.

3. Gevolgen schending geheimhouding

Door werknemer wordt ingezien en erkend dat overtreding of niet-nakoming van deze geheimhoudingsverklaring voor zijn werkgever Atimo Personeelstechniek B.V. aanleiding kan vormen om zijn arbeidsovereenkomst te beëindigen, al dan niet op grond van een dringende reden voor ontslag op staande voet.

Aldus geparafeerd, getekend en verklaard op [datum ondertekening] te [plaats] door:

3.3 **BIJLAGE 3** – Instructie van de Opdrachtgever aan Data Processor

Bedrijfsnaam opdrachtgever :

Adres :

Postcode/woonplaats :

Contactpersoon opdrachtgever :

De volgende contactpersonen worden per (datum) geautoriseerd binnen de door Data Processor geleverde applicatie:

Datum	Naam	Bevoegdheden	emailadres

Overige instructies:

Rechtsgeldig ondertekend op (datum) …… door:

Naam: ……

Functie: ……

Ingangsdatum : ……

3.4 **BIJLAGE 4** – Overview Security Measures Sentia Cloud

Alleen van toepassing voor de online omgeving (SaaS).

SENTIA

Table of Contents

SENTIA

INTRODUCTION

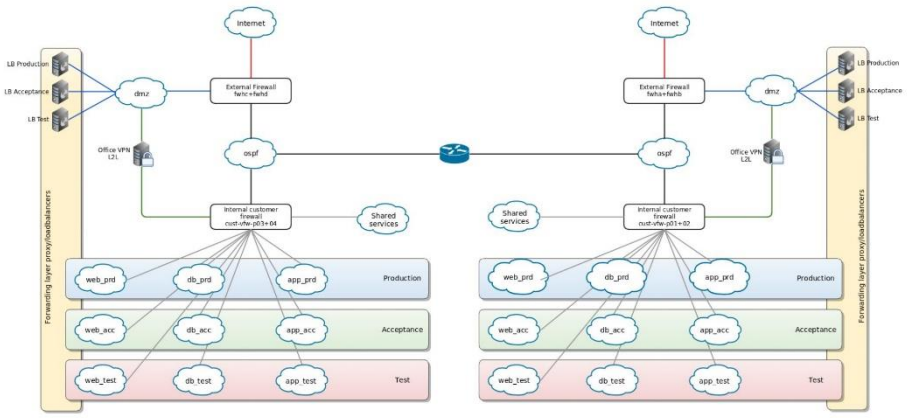
SENTIA CLOUD

The infrastructure for the Sentia Cloud is located at three independent data center locations, at Telecity Amsterdam, Equinix Amsterdam, and Global Switch Amsterdam. at a distance of approximately 10 km from each other. The data centers are connected by a redundant glass fiber to provide backup and disaster recovery services among others.
The servers and services are managed from the Amsterdam and Nieuwegein offices. For continuity reasons, engineers can work from home via a VPN connection. Each data center is connected to the Internet through different ISP's to provide redundant Internet connections.
The combination of the data centers make the following customer service continuity available:

- Backups are stored default at the other data center. This method keeps the data "internal" and easy to restore in case of a disaster;
- The data stored on the SANs in one data center is replicated to the SANs in the other data center;
- Sentia provides database replication or mirroring for customers with high availability requirements on the data in their databases.

Single points of failure are kept to a minimum:

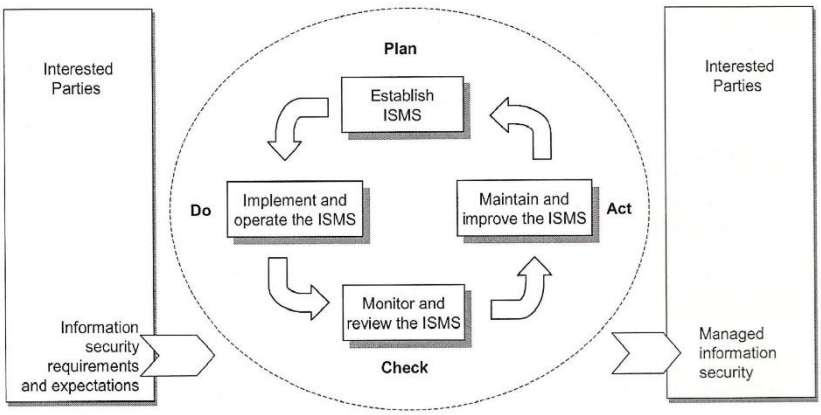
- Internet connections are provided by independent Internet Service Providers;
- Firewalls are combined in an automatic fail-over cluster;
- Switches and network paths are redundant for both the network as well as the storage switches;
- Data is located at SANs which have a redundant disk, hardware and network configuration;
- Servers providing processing power and memory for the Virtual Machines work in a cluster where the VM's migrate to another server in case one of the servers in a cluster fails.



example infrastructure at two datacenters

MANAGEMENT SYSTEM

Sentia manages Quality, Security and Environment (QSE) via the QSE Handbook. This handbook describes the policies and work instructions; it is the way Sentia works. The handbook is based on the ISO High Level Structure and contains general and specific guidelines for ISO 9001, ISO 14001, and ISO 27001.
The Plan, Do, Check, Act method ensures a cycle of continuous improvement.



ISO 27001

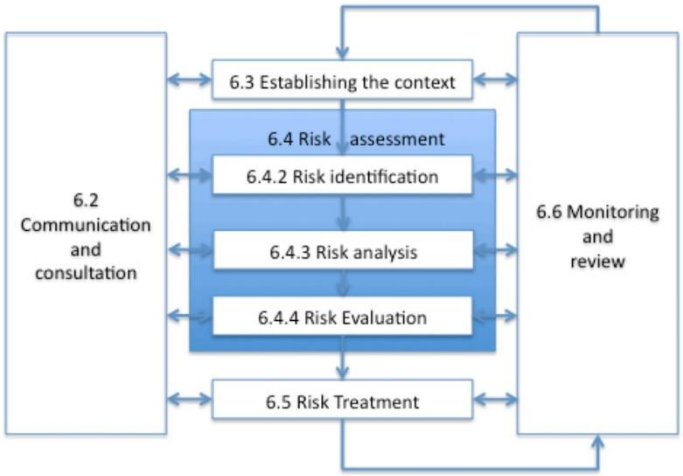
Sentia controls security by implementation of a Management System based on the ISO 27001/27002 standard.
Backed by a Risk Treatment Plan (RTP) following from the Risk Assessment, projects are developed to handle the risks. A good example is the implementation of a DDoS solution to face DDoS attacks.
Besides the risk assessment and treatment, the following ISO 27001 processes are conducted every year:

- Internal audit: the internal auditor checks whether the policies confirm with the actual actions;
- Management Review: the management reviews the operation of the ISMS and judges its effectiveness and efficiency;
- External audit: every year the management system is audited by an external, independent party (in our case BSI).

RISK ASSESSMENT

The 3-yearly full Risk assessment and quarterly check on actions resulting from the Risk Assessment (Risk Treatment Plan), addresses the risks Sentia is facing and the follow-up. This method is a risk based approach to detect, prioritize and mitigate or solve threats to the data of the Sentia customer.

The purpose of risk management is to ensure that Sentia has an appropriate response to the risks that have an adverse impact on the organization, its capability, goals, objectives and strategy.



Risk management process (bron: ISO31000)

SENTIA

INFORMATION AND COMMUNICATION

- Communication is mainly done via SIS:
  - Changes are tracked in SIS;
  - Quality: the customer is asked to review the way a call is solved;
  - Security: only approved contacts can create/view/update calls.
- Security issues are communicated to customers via e-mail lists and/or https://status.sentia.com;
- Incident management; update the customer regularly during an incident;
- Change management; inform and consult with the customer and colleagues about a change;
- There is a status page https://status.sentia.com on which relevant QSE topics can be shared with customers or other external parties.

There is no periodic communication about environmental topics, however, stakeholders are shared in an environmental dashboard with information about energy usage.

MONITORING

The systems of Sentia's customers are extensively monitored to ensure the continuity of the services delivered. This is input for both the Incident Management process and for trend analysis.

Sentia monitors the customer's environment on:

- CPU, memory and disk space usage. When a critical value (normally 90% used) is hit, a Sentia engineer contacts the customer to discuss whether resources should be added.
- Availability of the web application: every 5 minutes the Sentia monitoring system checks whether the web application is available.
- The availability of the servers and services is defined in the SLA.

SENTIA

SECURITY ADMINISTRATION

RISK MANAGEMENT

The PDCA model used in the Sentia Management System ensures a proces of continual improvement in which the risks of all stakeholders are determined and addressed.

- Every three years a new risk assessment will be performed;
- The risks are documented in the wiki, in a combined risk assessment/risk treatment report;
- The risk assessment/risk treatment plan will be approved by Sentia's CTO or MT;
- The security officer will follow up on the actions defined in the risk treatment plan (on a quarterly basis minimum);
- The risk treatment plan will be one of the inputs for the management review.

Risks are prioritized based on the threat level and the business impact level.

HARDENING

Systems managed by Sentia are hardened by using a predefined checklist with the desired settings.

An important part of System Administration is guaranteeing the continuity of the safety of the deployed Systems and Services. To this end, Sentia executes the following tasks:

- Implementation of security updates on the supported software;
- Periodic execution of internal security scans;
- Possibilities for setting up an external security scan.

In the implementation of security updates, a distinction is made between five update types: Remote Root, Remote User, Local Root, Denial of Service and non-critical updates.

The Compliance department of Sentia monitors security newsletters, forums, and other information sources to stay informed about new security vulnerabilities. Compliance informs the teams on new updates. The engineers and team leads determine whether:

- the update is relevant for the service;
- the update is critical and needs to be planned as soon as possible;
- to either plan in a Maintenance Window or to delay the update to a later, more convenient moment.

When Sentia considers a security threat to be highly acute, a security update can be implemented without prior contact with Client.

In addition to implementing security updates, Sentia scans the infrastructure for security-related vulnerabilities. On a regular basis, Sentia performs a scan of the Systems and Services itself (an internal scan) This internal security scan utilizes standard software tools to scan the servers and supported Services from the perspective of a non-privileged user. These tools have daily feeds that are automatically updated with up-to-date vulnerability information. In SIS, a Security Incident is created for critical issues to ensure these are handled accordingly.

SENTIA

Besides the above the following security related processes are in place:

Network and system security:

- Firewall cluster with a default deny policy, on both inbound as well as outbound traffic;
- Encryption of critical connections, like VPN to and in between the offices, ssh connections to Linux based servers and RDC to Windows based servers;
- DDoS protection by the NaWas service.

Access Control

Physical security

Applicable locations for physical security:

a) Data centers are physically secured by
   - Registration via data center portal
   - Fences
   - 24x7 guard
   - ID check (without a passport or driver's license no entrance to the DC)
   - Closed cabinets
   - Temparature controlled

b) The Sentia offices are electronically secured by a personal access badge.

Logical access control

Logical access control is maintained by the following measurements:

a) Default deny policy for both incoming as outgoing connections.

b) Access control on need to manage basis. via a centralized user access control system (LDAP for Linux platforms and Active Directory for Windows platforms.)

c) Sentia engineers use public/private key combination or username and password to connect to the Linux systems For the Windows systems engineers login (with username and password) via the Remote Desktop Protocol.

SENTIA

Backup & Restore Management

Sentia is dependent on a few requirements to supervise the continuity of the services rendered to Client's end-users by the Systems and Services in scope of the SLA. An essential requirement is having access to periodical backups of the systems, Sentia distinguishes between three types of backups .

- full backup: a full backup of all the files on the system;
- data backup: backup consisting of user-data on the system;
- configuration backup: backup consisting of the system configuration files.

If the platform setup allows it, Sentia will strive to store the backups off-site. In addition, secured connections are used as much as possible to transport the backup data to the backup servers. The backup process is closely monitored.

Supplier management

Sentia partners with tier III data centers to provide secure and robust hosting conditions. Sentia-owned networking services are extensively monitored for delays, disruptions and intrusions.

An important aspect in the preservation of quality are competent suppliers. The most important suppliers for Sentia are the data centers and ISP's (Internet Service Providers). Every year Sentia evaluates their suppliers. Criteria are (ISO) certification, performance and communication.

At Sentia we realize our core services are dependent on outsourced services provided by some critical third parties. In general, critical providers are reviewed periodically during the internal 9001 (quality) audit. Security aspects are part of the purchasing process.

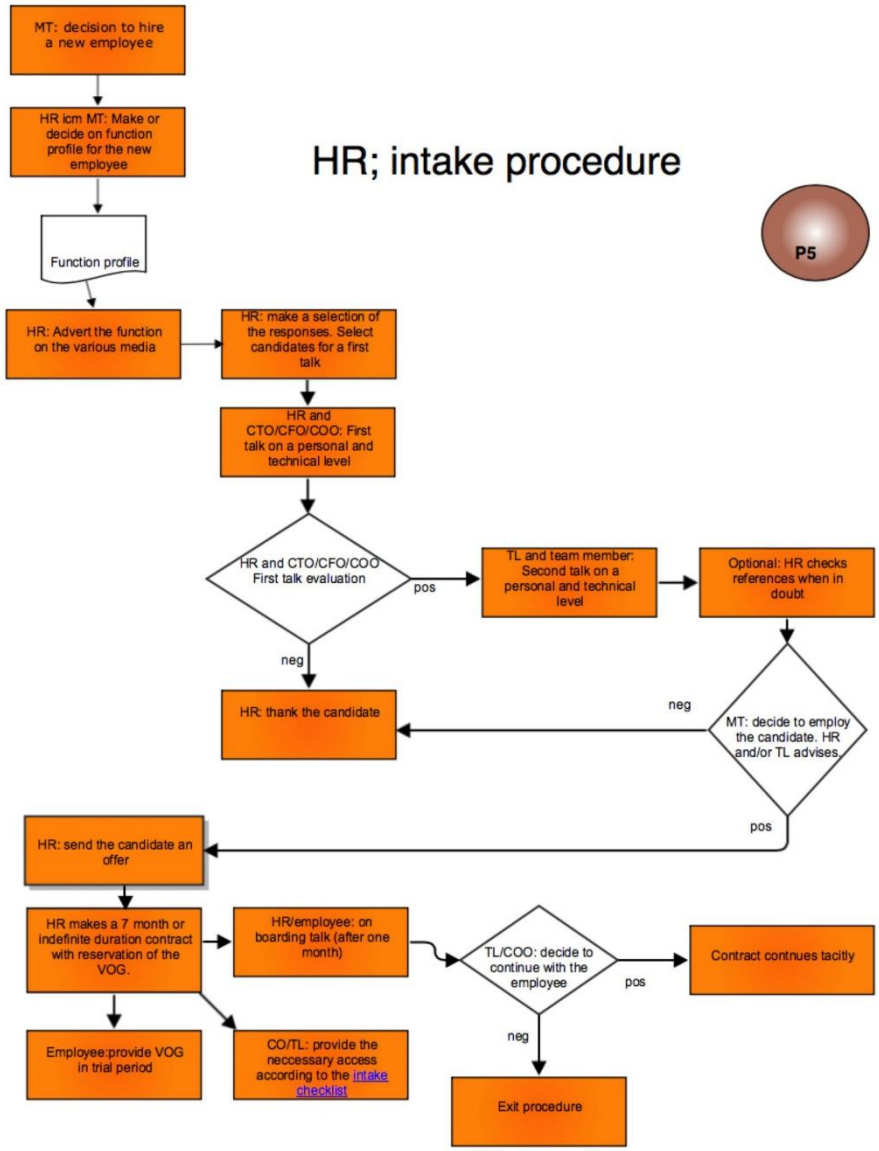
- Data centres: Sentia controls the data centre services by the default monitoring system as well as via the monthly reports provided by the data centres;
- ISP's: the services delivered by Internet Service Providers are checked by the monitoring system as well as Service Delivery Reports.

Hardware

Sentia is responsible for supplying the hardware components of the infrastructure. In case hardware issues occur, Sentia will take responsibility in planning repairs and overseeing the hardware support contract of the hardware supplier.

HR

The Sentia engineers perform the day-to-day business on our customer's systems. To make sure the engineer is competent, Sentia's HR has the following procedure:



SENTIA

- at intake the competence of the employee is assessed.
- non-disclosure clauses are part of the contract signed by the employee.
- proof of good conduct (VOG) is required.

During employment the employee is guided from a job to a career with the PRO (Persoonlijk, Resultaat en Ontwikkeling) method:

- For every function HR defines a profile describing the tasks that go with the function;
- Every 6 months the Team Lead and HR discuss the progress with the employee;
- The result of the evaluation is a Growth Document describing personal goals and development.

3.5 **BIJLAGE 5** – Remote ondersteuning middels GO2ASSIST of Team Viewer

De Atimo helpdesk biedt ondersteuning op afstand met GoToAssist Corporate van Citrix Online. Met dit programma kijken onze consultants remote op afstand mee op het beeldscherm van de Time-Wize® gebruikers. Zo kunnen zij eventuele problemen snel analyseren en oplossen. Ook in deze situatie worden we in het kader van de AVG gezien als verwerker.

Beveiliging van de pc en de gegevens van de klant
Essentieel onderdeel van de beveiliging van GoToAssist Corporate is dat dit programma volledig op consensus gebaseerd is:

- De supportsessies worden door Atimo gestart en er wordt een unieke sessiecode aan de klant afgegeven.
- In het inlogproces wordt de klant altijd om toestemming gevraagd voordat er wordt gestart met schermdeling, externe pc-besturing of het overbrengen van bestanden, diagnostische gegevens of andere informatie.
- Als de klant toestemming heeft gegeven voor remote control en schermdeling, kan hij/zij altijd zien wat de consultant doet.
- De klant kan op elk moment de besturing weer overnemen, de sessie pauzeren of stoppen.
- Lokale beveiligingscontroles op de pc van de klant worden nooit opgeheven; de klant of de consultant moet alle gebruikelijke verificatiegegevens voor Windows of toepassingen invoeren.

Hoge beveiligingsstandaarden
Citrix Online heeft een ijzersterke reputatie wat betreft veilige externe verbindingen. De beveiligde communicatiearchitectuur van GoToAssist Corporate maakt gebruik van gangbare SSL- (Secure Sockets Layer) en 128-bits AES-codering (Advanced Encryption Standard). Deze standaarden worden ook gebruikt voor internetbankieren. De sessiegegevens worden end-to-end gecodeerd. In tegenstelling tot andere producten voor externe ondersteuning, kunnen beveiligingsmaatregelen van Citrix Online nooit uitgeschakeld worden.

End-to-end-verificatie wordt uitgevoerd met het protocol “Secure Remote Password” (SRP). SRP is bestand tegen een breed scala aan aanvallen vanaf internet, waaronder zowel passief afluisteren als actief wachtwoord kraken.

De Atimo helpdesk biedt als alternatief ook ondersteuning op afstand met Team Viewer. Met dit programma kijken onze consultants remote op afstand mee op het beeldscherm van de Time-Wize® gebruikers. Zo kunnen zij eventuele problemen snel analyseren en oplossen. Ook in deze situatie worden we in het kader van de AVG gezien als verwerker.

Beveiliging van de pc en de gegevens van de klant
Essentieel onderdeel van de beveiliging van Team viewer is dat dit programma volledig op consensus gebaseerd is:

- De supportsessies worden door de klant gestart en er wordt een unieke sessiecode aan de medewerker van Atimo afgegeven.
- Als de klant toestemming heeft gegeven voor remote control en schermdeling, kan hij/zij altijd zien wat de consultant doet.
- De klant kan op elk moment de besturing weer overnemen, de sessie pauzeren of stoppen.
- Lokale beveiligingscontroles op de pc van de klant worden nooit opgeheven; de klant of de consultant moet alle gebruikelijke verificatiegegevens voor Windows of toepassingen invoeren.

Uitzonderingssituaties
Atimo maakt standaard gebruik van GoToAssist of Team Viewer. In uitzonderlijke gevallen kan in overleg met de opdrachtgever schriftelijk worden overeengekomen dat hiervan wordt afgeweken en onder welke voorwaarden. Mogelijkerwijs zijn hier extra kosten aan verbonden.

3.6 **BIJLAGE 6** – Informatieverstrekking bij een datalek

Als u een beveiligingsincident hebt ontdekt, neemt u binnen 24 uur contact op met de Verwerkingsverantwoordelijke op.

Atimo dient de volgende vragen te beantwoorden:

1. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?
   Geef dit a.u.b. zo specifiek mogelijk aan.

2. Geef een samenvatting van het beveiligingslek / beveiligingsincident / datalek: wat is er gebeurd?
   Vermeld hier ook de naam van het betrokken systeem.

3. Wat is de oorzaak (root cause) van het beveiligingsincident?
   Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?

4. Welke typen persoonsgegevens zijn betrokken bij het beveiligingsincident?
   Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.

5. Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident?
   Geef a.u.b. een minimum en maximum aantal personen.

6. Omschrijving groep personen om wiens gegevens het gaat.
   Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals kinderen.

7. Zijn de contactgegevens van de betrokken personen bekend?
   Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek, kunnen we deze personen in dat geval bereiken?