Bijlage verwerkersbepalingen

JORO Solutions B.V.
Bijlage voor verwerkingen van persoonsgegevens.

Versie: 1.0
Datum: december 2024
Auteur: JORO Solutions

Inhoudsopgave

Dit document vormt samen met hoofdstuk 5 van de 'JORO Solutions B.V Algemene Voorwaarden', de Verwerkersovereenkomst zoals bedoeld in de Algemene Verordening Gegevensbescherming (AVG). In de offerte of overeenkomst van opdracht met JORO Solutions B.V wordt verwezen naar deze bijlage.

De partijen bij de verwerkersovereenkomst zijn de Opdrachtgever (hierna: "Verwerkingsverantwoordelijke") zoals benoemd in de Offerte of overeenkomst en JORO Solutions B.V. (hierna te noemen "Verwerker").

1. Samenhang met overige documenten

Partijen zijn overeengekomen dat Verwerker diensten verleent voor Verwerkingsverantwoordelijke.
Dit is vastgelegd in een separate offerte, dan wel overeenkomst. Deze Verwerkersovereenkomst vormt hiervan een onlosmakelijk onderdeel. In geval van strijdigheid van verschillende documenten of de bijlagen daarvan, geldt de volgende rangorde:

- Deze Verwerkersovereenkomst en de verwerkersbepalingen van de Algemene Voorwaarden, Aanvullende voorwaarden en verwerkersbepalingen;
- De Overeenkomst;
- De Algemene Voorwaarden en Aanvullende voorwaarden.

Definities uit de Algemene Voorwaarden van JORO Solutions B.V kunnen in dit document ook worden gebruikt en hebben dezelfde betekenis als daar gedefinieerd.

1.1 Instructies voor JORO Solutions B.V door Verwerkersverantwoordelijke

Hieronder staat een overzicht van de categorieën Persoonsgegevens, de aard en het doel van de verwerking, verwerkingshandelingen, de categorieën betrokkenen en bewaartermijn(en). Let op: de instructies hieronder worden gegeven door de Verwerkersverantwoordelijke en hebben betrekking op de verwerking van persoonsgegevens door JORO Solutions B.V in haar hoedanigheid van Verwerker. Per dienst heeft JORO Solutions B.V hieronder een aanzet gedaan om de categorieën persoonsgegevens, de aard en het doel van de verwerking, categorieën betrokkenen en de bewaartermijn te omschrijven. De Verwerkersverantwoordelijke controleert deze gegevens en vult deze eventueel aan voorafgaand aan het ondertekenen van een offerte of overeenkomst met JORO Solutions B.V.

1.1.1 Categorieën Persoonsgegevens

Bij "Implementatie en Optimalisatie AFAS Profit",
"Consultancy", "Support " en bij "Functioneel Beheer"
De volgende categorieën van persoonsgegevens worden verwerkt:

- Persoonlijke identificatiegegevens: Namen, adressen, geboortedata, Burgerservicenummers (BSN).
- Contactgegevens: Telefoonnummer, e-mailadres.
- Financiële gegevens: Bankrekeningnummers, salarisinformatie.
- Werk gerelateerde informatie: Functietitels, arbeidscontracten, prestatiebeoordelingen.
- Transactiegegevens: Bestelgeschiedenis, factuurinformatie.

Bij: “Salaris”
De volgende categorieën van persoonsgegevens worden verwerkt:

- Persoonlijke identificatiegegevens: Namen, adressen, geboortedata, Burgerservicenummers (BSN).
- Contactgegevens: Telefoonnummer, e-mailadres.
- Financiële gegevens: Bankrekeningnummers, salarisinformatie, belastinginformatie.
- Werk gerelateerde informatie: Functietitels, arbeidscontracten, urenstaten, verlof- en ziektedagen, prestatiebeoordelingen.
- Transactiegegevens: Loonstroken, betaalgegevens.

Bij: “Oplossingen voor Data”:
De volgende categorieën van persoonsgegevens worden verwerkt:

- Persoonlijke identificatiegegevens: Namen, adressen, geboortedata, Burgerservicenummers (BSN).
- Contactgegevens: Telefoonnummer, e-mailadres.
- Financiële gegevens: Bankrekeningnummers, salarisinformatie, belastinginformatie.
- Werk gerelateerde informatie: Functietitels, arbeidscontracten, urenstaten, verlof- en ziektedagen, prestatiebeoordelingen.
- Transactiegegevens: Bestelgeschiedenis, factuurinformatie.

Bij: “Development Oplossingen”
De volgende categorieën van persoonsgegevens kunnen worden verwerkt, afhankelijk van de gegevens die door de systemen worden uitgewisseld:

- Persoonlijke identificatiegegevens: Namen, adressen, geboortedata, Burgerservicenummers (BSN).
- Contactgegevens: Telefoonnummer, e-mailadres.
- Financiële gegevens: Bankrekeningnummers, salarisinformatie, belastinginformatie.
- Werk gerelateerde informatie: Functietitels, arbeidscontracten, urenstaten, verlof- en ziektedagen, prestatiebeoordelingen.
- Transactiegegevens: Bestelgeschiedenis, factuurinformatie.

De Verwerkingsverantwoordelijke verklaart dat geen:
Bijzondere Persoonsgegevens worden verwerkt.
Verwerkingsverantwoordelijke verklaart eveneens dat geen fraudegevoelige Persoonsgegevens worden verwerkt buiten de BSN en het bankrekeningnummer.

Aard en doel van de verwerking
Bij “Implementatie en Optimalisatie AFAS Profit”,
“Consultancy”, “Support”, en bij “Functioneel Beheer”
Doel:

De verwerkingsactiviteiten hebben als doel de implementatie, configuratie, en het onderhoud van het ERP-systeem van de Verwerkingsverantwoordelijke te ondersteunen. Dit omvat technische ondersteuning, systeemupdates, en het oplossen van problemen.

Aard:

De Verwerker zal de volgende activiteiten uitvoeren:

- Gegevensverzameling: Het verzamelen van persoonsgegevens die noodzakelijk zijn voor de initiële opzet en configuratie van het ERP-systeem.
- Gegevensopslag: Het opslaan van persoonsgegevens in het ERP-systeem.
- Gegevensorganisatie en -structurering: Het organiseren en structureren van persoonsgegevens om een efficiënte werking van het ERP-systeem te waarborgen.
- Gegevensupdating en -wijziging: Het bijwerken en wijzigen van persoonsgegevens om de nauwkeurigheid en relevantie te behouden.
- Gegevensraadpleging: Het raadplegen van persoonsgegevens door bevoegde medewerkers van de Verwerker voor ondersteuningsdoeleinden.
- Gegevensverwijdering: Het verwijderen van persoonsgegevens op verzoek van de Verwerkingsverantwoordelijke of in overeenstemming met de bewaartermijnen.

Bij: JORO Solutions B.V

Doel:

De verwerkingsactiviteiten hebben als doel het ondersteunen van de salarisverwerking voor de Verwerkingsverantwoordelijke in hun eigen ERP-systeem. Dit omvat het berekenen van salarissen, het verwerken van loonstroken, het afhandelen van belastingverplichtingen en het verstrekken van rapportages.

Aard:

De Verwerker zal de volgende activiteiten uitvoeren:

- Gegevensinvoer en -verzameling: Het invoeren en verzamelen van salaris gerelateerde persoonsgegevens in het ERP-systeem van de Verwerkingsverantwoordelijke.
- Gegevensopslag: Het opslaan van salarisgegevens in het ERP-systeem.
- Gegevensorganisatie en -structurering: Het organiseren en structureren van salarisgegevens om een efficiënte salarisverwerking te waarborgen.
- Gegevensupdating en -wijziging: Het bijwerken en wijzigen van salaris- en stamgegevens om de nauwkeurigheid en relevantie te behouden.
- Gegevensraadpleging: Het raadplegen van salarisgegevens door bevoegde medewerkers van de Verwerker voor ondersteunings- en verwerkingsdoeleinden.
- Gegevensverwijdering: Het verwijderen van salarisgegevens op verzoek van de Verwerkingsverantwoordelijke of in overeenstemming met de bewaartermijnen.

Bij: JORO Solutions B.V Oplossingen voor Data

Doel:

De verwerkingsactiviteiten hebben als doel het aanbieden van een SaaS-oplossing voor het realiseren van koppelingen tussen softwaresystemen (bronsysteem en doelsysteem) voor de

Verwerkingsverantwoordelijke. Dit omvat het automatisch uitwisselen, synchroniseren, en transformeren van gegevens tussen deze systemen.

Aard:

De Verwerker zal de volgende activiteiten uitvoeren:

- Gegevensoverdracht: Het automatisch overdragen van persoonsgegevens van het bronsysteem naar het doelsysteem via de SaaS-koppeling.
- Gegevensvalidatie: Het valideren van de juistheid en volledigheid van de persoonsgegevens tijdens de overdracht.
- Gegevenstransformatie: Het transformeren van gegevensformaten en -structuren om compatibiliteit tussen de systemen te waarborgen.
- Gegevenssynchronisatie: Het automatisch synchroniseren van persoonsgegevens tussen het bronsysteem en het doelsysteem om consistentie te garanderen.
- Gegevensopslag: Tijdelijke opslag van persoonsgegevens in de SaaS-oplossing tijdens de overdracht en verwerking. Voor business intelligence-oplossingen wordt de data opgeslagen gedurende de volledige duur van het abonnement.
- Gegevenslogging: Het loggen van verwerkingsactiviteiten binnen de SaaS-oplossing voor monitoring en foutopsporing.
- Gegevensverwijdering: Afhankelijk van de situatie, het verwijderen van persoonsgegevens en/of het verwijderen van persoonsgegevens uit tijdelijke opslag na succesvolle overdracht en verwerking.

Bij: JORO Solutions B.V Development Oplossingen

Doel:

De verwerkingsactiviteiten hebben als doel het ontwikkelen, testen en implementeren van een softwarekoppeling tussen systemen voor de Verwerkingsverantwoordelijke. Dit omvat het bouwen, configureren en optimaliseren van de koppeling om een efficiënte gegevensuitwisseling tussen het bronsysteem en het doelsysteem te waarborgen.

Aard:

De verwerker (JORO Solutions B.V) zal de volgende activiteiten uitvoeren:

- Gegevensanalyse en -mapping: Analyse van gegevensstructuren en het maken van gegevensmapping om compatibiliteit tussen systemen te waarborgen.
- Gegevensoverdracht (testomgeving): Het testen van de gegevensoverdracht tussen systemen met gebruik van persoonsgegevens, indien nodig, in een gecontroleerde testomgeving.
- Gegevenstransformatie: Het ontwikkelen en implementeren van transformatielogica om gegevensformaten en -structuren te transformeren tussen het bronsysteem en het doelsysteem.

- Gegevensvalidatie en -verificatie: Validatie en verificatie van de juistheid en volledigheid van de gegevensoverdracht tijdens de ontwikkeling en testfase.
- Debuggen en foutoplossing: Identificeren en oplossen van fouten die optreden tijdens de ontwikkeling en testen van de koppeling.
- Gegevenslogging (testomgeving): Logging van verwerkingsactiviteiten voor monitoring, foutopsporing en auditdoeleinden tijdens de ontwikkeling en testfase.
- Gegevensverwijdering (testomgeving): Verwijdering van persoonsgegevens uit de testomgeving na afronding van de ontwikkeling en testfase.

2. Categorieën betrokkenen (de geïdentificeerde of identificeerbare natuurlijke persoon)

Bij “Implementatie en Optimalisatie AFAS Profit”, “Consultancy”, “Support”, en “Functioneel Beheer”
De persoonsgegevens hebben betrekking op de volgende categorieën van betrokkenen:

- Medewerkers: Huidige en voormalige werknemers van de Verwerkingsverantwoordelijke.
- Klanten: Personen die producten of diensten afnemen van de Verwerkingsverantwoordelijke.
- Leveranciers: Externe partijen die goederen of diensten leveren aan de Verwerkingsverantwoordelijke.

Bij “Salaris”
De persoonsgegevens hebben betrekking op de volgende categorieën van betrokkenen:
• Medewerkers: Huidige en voormalige werknemers van de Verwerkingsverantwoordelijke.

Bij “Oplossingen voor Data” en “Development Oplossingen”
De persoonsgegevens hebben betrekking op de volgende categorieën van betrokkenen:

- Medewerkers: Huidige en voormalige werknemers van de Verwerkingsverantwoordelijke.
- Klanten: Personen die producten of diensten afnemen van de Verwerkingsverantwoordelijke.
- Leveranciers: Externe partijen die goederen of diensten leveren aan de Verwerkingsverantwoordelijke.

2.1 Duur van de verwerking

De persoonsgegevens zullen worden verwerkt voor de duur van de contractuele relatie tussen de Verwerkingsverantwoordelijke en JORO Solutions B.V, en zo lang als noodzakelijk is voor het vervullen van de overeengekomen (SaaS-)diensten. Na beëindiging van de overeenkomst worden de persoonsgegevens verwijderd of geretourneerd aan de Verwerkingsverantwoordelijke, tenzij een wettelijke verplichting verdere opslag vereist.

3. Beschrijving van technische en organisatorische beveiligingsmaatregelen

3.1 Organisatorische beveiligingsmaatregelen

De volgende organisatorische maatregelen heeft JORO Solutions B.V getroffen ter beveiliging van o.a. persoonsgegevens:

3.1.1 Toegangsbeheer

- Autorisatiebeleid: Alleen geautoriseerde medewerkers krijgen toegang tot persoonsgegevens. Toegang wordt verleend op basis van de rol en verantwoordelijkheden van de medewerker.
- Sterke authenticatie: Gebruik van twee-factor authenticatie (2FA) voor toegang tot systemen die persoonsgegevens bevatten.
- Periodieke herziening: Regelmatige evaluatie en bijwerking van toegangsrechten om ervoor te zorgen dat alleen actuele medewerkers toegang hebben.

3.1.2 Bewustwording en training

- Regelmatige training: Medewerkers ontvangen regelmatige training over gegevensbescherming, privacyregelgeving (zoals de AVG), en het belang van het beschermen van persoonsgegevens.
- Bewustwordingscampagnes: Regelmatige interne campagnes om het bewustzijn van gegevensbeschermingskwesties te verhogen.

3.1.3 Beleid en procedures

- Gegevensbeschermingsbeleid: Een gedocumenteerd gegevensbeschermingsbeleid dat de richtlijnen en procedures beschrijft voor het omgaan met persoonsgegevens.
- Incidentbeheerprocedure: Een duidelijk omschreven procedure voor het melden en beheren van beveiligingsincidenten en datalekken.
- Retentiebeleid: Beleid voor het bewaren en verwijderen van persoonsgegevens om ervoor te zorgen dat gegevens niet langer bewaard worden dan noodzakelijk.
- Screening: Relevante werknemers zijn gescreend en bekend met het vakgebied informatiebeveiliging.
- Geen opslagmedia: Er wordt geen gebruik gemaakt van USB-sticks of andere draagbare media om bedrijfsgegevens op te slaan.
- Continuïteitswaarborgen: Er zijn bedrijfscontinuïteitsbeheer en continuïteitsplannen, en deze worden periodiek geüpdatet.

3.1.4 Contractuele waarborgen

- Geheimhoudingsverklaringen: Medewerkers en contractanten ondertekenen geheimhoudingsverklaringen om te waarborgen dat zij de vertrouwelijkheid van persoonsgegevens respecteren.
- Verwerkersovereenkomsten: Contracten met sub-verwerkers bevatten duidelijke afspraken over gegevensbescherming en beveiliging.

3.1.5 Monitoring en audit

- Loggen en toezicht: Op kritieke software is sprake van het bijhouden van toegangs- en verwerkingslogs om ongeautoriseerde toegang en gebruik van persoonsgegevens te detecteren.
- Interne en externe audits: Regelmatige audits en beoordelingen van beveiligingsmaatregelen om naleving van gegevensbeschermingsbeleid en regelgeving te waarborgen.

3.1.6 Risicobeheer

- Risicoanalyses: Periodieke identificatie en beoordeling van risico's met betrekking tot de verwerking van persoonsgegevens.
- Beveiligingsmaatregelen aanpassen: Aanpassen van beveiligingsmaatregelen op basis van de resultaten van risicoanalyses om nieuwe en veranderende bedreigingen te mitigeren.
- Wijzigingsbeleid: Wijzigingen in gegevens of in informatieverwerking worden voor software uitgevoerd onder een procedure voor wijzigingsbeheer.
- Escrow: De mogelijkheid voor de Verwerkingsverantwoordelijke voor het afsluiten van een continuïteitregeling (escrow) voor situaties waarin de Verwerker niet meer aan haar verplichtingen kan voldoen.

3.1.7 Fysieke beveiliging

- Beveiligde werkomgeving: Fysieke toegangscontrole tot gebouwen en ruimtes waar persoonsgegevens worden verwerkt of opgeslagen.
- Beveiliging van hardware: Beveiliging van apparaten die toegang hebben tot persoonsgegevens, inclusief versleuteling van gegevensdragers en het veilig wissen van gegevens bij afdanking van apparatuur.
- Alarmsysteem: Maatregelen tegen inbraak, waaronder een inbraakalarm.

3.1.8 Naleving en verantwoording

- Verantwoordelijke Data Security Officer (DSO): Aanwijzing van een DSO die verantwoordelijk is voor het toezicht op de naleving van gegevensbeschermingsbeleid en -procedures.
- Documentatie: Gedetailleerde documentatie van alle verwerkingsactiviteiten en de genomen beveiligingsmaatregelen om verantwoording af te kunnen leggen aan toezichthoudende autoriteiten.

3.2 Technische beveiligingsmaatregelen

De volgende technische maatregelen heeft JORO Solutions B.V getroffen ter beveiliging van o.a. persoonsgegevens:

3.2.1 Versleuteling

- Data-at-rest: Alle persoonsgegevens worden versleuteld opgeslagen, zowel op servers als op externe opslagmedia (zoals laptops).
- Data-in-transit: Persoonsgegevens worden versleuteld tijdens de overdracht via netwerken, bijvoorbeeld door gebruik van TLS (Transport Layer Security) of VPN (Virtual Private Network).

3.2.2 Toegangscontrole

- Authenticatie: Gebruik van sterke wachtwoorden en multi-factor authenticatie (MFA) of in combinatie met biometrie voor toegang tot systemen die persoonsgegevens bevatten.
- Autorisatie: Toegang tot persoonsgegevens is beperkt tot geautoriseerde gebruikers op basis van rolgebaseerde toegangscontrole (RBAC).

- Logging en monitoring: Toegangspogingen en activiteiten met betrekking tot persoonsgegevens op kritieke software worden gelogd en regelmatig gemonitord.

3.2.3 Beveiliging van netwerken en systemen

- Firewall: Gebruik van firewalls om ongeautoriseerde toegang tot het netwerk te voorkomen.
- Anti-malware: Gebruik van up-to-date anti-malware oplossingen om te beschermen tegen virussen, spyware en andere schadelijke software.

3.2.4 Software- en systeembeveiliging

- Patch management: Regelmatig updaten en patchen van software en systemen om bekende kwetsbaarheden te dichten.
- Beveiligde configuraties: Configureren van systemen volgens beveiligingsrichtlijnen en best practices om risico's te minimaliseren.
- Penetratietesten: Regelmatig uitvoeren van penetratietesten om beveiligingslekken te identificeren en te verhelpen. Zie ook hieronder, 3.3 Doorlopende verbetering.

3.2.5 Back-up en herstel

- Regelmatige back-ups: Regelmatig maken van versleutelde back-ups van persoonsgegevens om gegevensverlies te voorkomen. Hiervan is alleen sprake als dat expliciet is afgesproken.
- Herstelprocedures: Ontwikkelen en testen van gegevensherstelprocedures om snel te kunnen herstellen van gegevensverlies.

3.3 Gegevensminimalisatie en pseudonimisering

3.3.1 Gegevensminimalisatie

- Beperking van gegevensverzameling: Beperk de verzameling en opslag van persoonsgegevens tot wat strikt noodzakelijk is voor de verwerkingsdoeleinden.

3.3.2 Incidentbeheer

- Incident Response Plan: Implementatie van een incident response plan voor het beheren en reageren op beveiligingsincidenten en datalekken.
- Incident logging: Loggen van alle beveiligingsincidenten en het analyseren ervan om herhaling te voorkomen.

3.3.3 Beveiliging van applicaties

- Secure Development Lifecycle (SDLC): Integreren van beveiligingspraktijken in alle fasen van softwareontwikkeling.
- Code review en vulnerability scanning: Regelmatig uitvoeren van code reviews en vulnerability scans om beveiligingsproblemen in applicaties te identificeren en te verhelpen.

3.3.4 Monitoring en auditing

- Doorlopende monitoring: Implementatie van continue monitoring van systemen en netwerken om verdachte activiteiten snel te detecteren.

- Audit logging: Gedetailleerde audit logs bijhouden van toegang tot persoonsgegevens.

3.3.5 Fysieke beveiliging van IT-infrastructuur

- Beveiligde datacenters: Gebruik van datacenters met fysieke beveiligingsmaatregelen zoals toegangscontrole, bewakingscamera's en beveiligingspersoneel.
- Apparaatbeveiliging: Bescherming van servers en andere apparatuur tegen fysieke toegang door ongeautoriseerde personen.

3.4 Doorlopende verbetering

JORO Solutions B.V neemt de volgende maatregelen om zwakke plekken te identificeren ten aanzien van de verwerking van persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Verwerkingsverantwoordelijke.

- Eens per twee jaar laat JORO Solutions B.V een externe partij een zogenaamde grey-box pentest uitvoeren op haar Azure-omgeving, applicaties en website(s).
- Medewerkers worden periodiek geïnformeerd over dataveiligheid en de omgang met privacygevoelige informatie.

4. Rapportage

Indien gewenst rapporteert de Verwerker periodiek aan de Verwerkingsverantwoordelijke over de door de Verwerker genomen maatregelen, de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin. U kunt hiervoor contact opnemen met onze helpdesk over beveiligingsincidenten via beveiligingsincidenten@jorosolutions.nl.

4.1 Contactgegevens en dienstspecifieke maatregelen

Data Security Officer (DSO):
Verwerker beschikt over de volgende certificeringen:
ISO 27001

5. Sub verwerkers

Overzicht van door de Verwerker ingeschakelde sub verwerker(s):

Sub verwerker	Beschrijving dienst	Gegevens buiten de EER
AFAS Software (https://www.afas.nl)	ERP Systeem	Nee / Ja
123-webhost (https://www.123-webhost.net)	Hosting provider	Nee / Ja
Microsoft 365 (https://www.microsoft.com/nl-nl/microsoft-365)	Microsoft Online Services	Nee / Ja

1) Bijzondere Persoonsgegevens. Bijvoorbeeld:
    1) Ras of etniciteit;
    2) Gezondheid;
    3) Genetische gegevens;
    4) Biometrische gegevens met oog op unieke identificatie;

5) Religieuze of levensbeschouwelijke overtuiging;
6) Politieke opvattingen;
7) Lidmaatschap vakvereniging; alsmede
8) Strafrechtelijke veroordelingen en overtredingen.

1) Persoonsgegevens die als (fraude)gevoelig worden beschouwd, niet zijnde Bijzondere Persoonsgegevens. Bijvoorbeeld:
   1) Identificatienummers (BSN, personeelsnummer);
   2) Financiële en economische gegevens (bankgegevens, salarisgegevens);
   3) Kopieën identiteitsbewijzen;
   4) Inloggegevens (van medewerkers die feitelijk gebruik maken van de overeengekomen dienst namens de Verwerkingsverantwoordelijke).