Bijlage verwerkersbepalingen

Fhris B.V.

Bijlage voor verwerkingen van persoonsgegevens.

Versie: 1.0.1
Datum: juni 2026
Auteur: Fhris

Inhoudsopgave

Dit document vormt samen met hoofdstuk 3 van de '**Fhris Algemene Voorwaarden**'', de Verwerkersovereenkomst zoals bedoeld in de Algemene Verordening Gegevensbescherming. In de offerte of overeenkomst van opdracht met Fhris wordt verwezen naar deze bijlage.

De partijen bij de verwerkersovereenkomst zijn de Opdrachtgever (hierna: "**Verwerkingsverantwoordelijke**") zoals benoemd in de Offerte of overeenkomst en Fhris B.V. (hierna "**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:

1. deze Verwerkersovereenkomst en de verwerkersbepalingen van de Algemene Voorwaarden, Aanvullende voorwaarden en verwerkersbepalingen;
2. de Overeenkomst;
3. de Algemene Voorwaarden en Aanvullende voorwaarden.

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

2 Instructies voor Fhris 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 gedaan door de Verwerkersverantwoordelijke en hebben betrekking op de verwerking van persoonsgegevens door Fhris in haar hoedanigheid van Verwerker. Per dienst heeft Fhris hieronder een aanzet gedaan om de categorieën persoonsgegevens, de aard en 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 Fhris.

1.	Categorieën Persoonsgegevens	**Bij "Salarisverwerking", "Consultancy", "Fhris Portaal" en bij "Fhris White Label"** De volgende categorieën van persoonsgegevens worden verwerkt: • **Persoonlijke identificatiegegevens**: Namen, namen van gezinsleden, adressen, geboortedata, burgerservicenummers (BSN). • **Contactgegevens**: Telefoonnummer, e-mailadres. • **Financiële gegevens**: Bankrekeningnummers, salarisinformatie, belastinginformatie. • **Werkgerelateerde informatie**: Functietitels, arbeidscontracten, urenstaten, verlof- en ziektedagen, prestatiebeoordelingen, plan van aanpak inzake Wet

		Verbetering Poortwachter (WVP) inzake verzuiimbegeleiding. • **Transactiegegevens**: Loonstroken, betaalgegevens.
2.	Aard en doel van de verwerking	**Bij "Salarisverwerking", "Fhris Portaal" en bij "Fhris White Label"** **Doel:** De verwerkingsactiviteiten hebben als doel het ondersteunen van de salarisverwerking voor de Verwerkingsverantwoordelijke in hun eigen HRM-systeem, via Fhris Portaal, of via Fhris White Label. 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 salarisgerelateerde persoonsgegevens. • **Gegevensopslag**: Het opslaan van salarisgegevens in het HRM-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: "Consultancy"** **Doel** Het inrichten van AFAS-HRM ten behoeve van salarisverwerking en of HR-processen. Verder ook het beschikbaar stellen van gegevens aan derden in opdracht van de klant.

		Aard: De verwerker 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. • **Gegevensvalidatie en -verificatie:** Validatie en verificatie van de juistheid en volledigheid van de gegevensoverdracht tijdens de ontwikkeling en testfase. • **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.
3.	Categorieën betrokkenen (de geïdentificeerde of identificeerbare natuurlijke persoon)	**Bij "Salarisverwerking", "Consultancy", "Fhris Portaal" en bij "Fhris White Label"** De persoonsgegevens hebben betrekking op de volgende categorieën van betrokkenen: • **Medewerkers:** Huidige en voormalige werknemers van de Verwerkingsverantwoordelijke. • **Gebruikers:** Gebruikers van SaaS software van Fhris.
4.	Duur van de verwerking	De persoonsgegevens zullen worden verwerkt voor de duur van de contractuele relatie tussen de Verwerkingsverantwoordelijke en de Verwerker, en zolang als noodzakelijk is voor het vervullen van de overeengekomen (SaaS-)diensten. Na beëindiging van de overeenkomst worden de persoonsgegevens op verzoek verwijderd, verwijderd na het verstrijken van wettelijke bewaartermijnen, 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 Fhris 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.
- **Geen opslagmediums**: 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.

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.

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 Fhris 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 i.c.m. 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 die expliciet is afgesproken.
- **Herstelprocedures:** Ontwikkelen en testen van gegevensherstelprocedures om snel te kunnen herstellen van gegevensverlies.

3.2.6 Gegevensminimalisatie en pseudonimisering

- **Gegevensminimalisatie:** Beperken van de verzameling en opslag van persoonsgegevens tot wat strikt noodzakelijk is voor de verwerkingsdoeleinden.

3.2.7 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 analyseren om herhaling te voorkomen.

3.2.8 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.

3.2.9 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.

3.2.10 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.

3.3 Doorlopende verbetering

Fhris 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.

- Medewerkers worden periodiek over dataveiligheid en de omgang met privacygevoelige informatie geïnformeerd.

4 Rapportage

Indien gewenst rapporteert Verwerker periodiek aan Verwerkingsverantwoordelijke over de door Verwerker genomen maatregelen over de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin. U kunt hiervoor contact opnemen met onze helpdesk over beveiligingsincidenten via email. Fhris kan hiervoor kosten in rekening brengen.

4.1 Contactgegevens en dienstspecifieke maatregelen

1.	Data Security Officer (DSO):	Rebecca van der Ven
2.	Datalek (waakdienst en contact):	Indien er sprake is van een (potentieel) Datalek kan Verwerkingsverantwoordelijke contact opnemen met Rebecca van der Ven, telefoonnummer: 040 200 5500, e-mail: r.vanderven@fhris.nl.

5 Subverwerkers

Overzicht van door de Verwerker ingeschakelde subverwerker(s):

Subverwerker	Beschrijving dienst	Gegevens buiten de EER	(Sub) Verwerkersovereenkomst
STP Connect	Koppeling voor het delen van gegevens uit loonadministratiesoftware met verzekeraars	Nee	Ja
AFAS	HRM systeem waarop Fhris Portaal en Fhris White Label is gebaseerd	Nee	Ja
Hubbl	AI-services	Nee	Ja