Verwerkersovereenkomst

AFAS verwerkt onder andere persoonsgegevens voor en in opdracht van de klant omdat de klant een software gebruikersovereenkomst met AFAS heeft. AFAS en de klant zijn daarom verplicht volgens de Algemene Verordening Gegevensbescherming (AVG) om een Verwerkersovereenkomst te sluiten. Omdat AFAS een standaard applicatie (AFAS Profit, AFAS InSite/OutSite, AFAS Pocket) met de daarbij behorende standaard dienstverlening (AFAS Support/Consultancy en AFAS Online) levert, heeft AFAS de verwerkingsovereenkomst opgenomen in de Algemene Voorwaarden en SLA. AFAS is in deze de 'verwerker' en de klant de 'verwerkingsverantwoordelijke'. AFAS en de klant verplichten zich over en weer om de Algemene Verordening Gegevensbescherming (AVG) na te leven. Voor de definities van begrippen wordt aangesloten bij de AVG. AFAS zal de persoonsgegevens alleen verwerken voor en in opdracht van de klant en om uitvoering te geven aan de overeenkomst.

Instructies verwerking

De verwerking bestaat uit het beschikbaar stellen van de AFAS applicaties met de door de klant ingevoerde en gegenereerde data. AFAS zal geen gegevens toevoegen, aanpassen of verwijderen zonder dat de klant daar specifieke instructie voor gegeven heeft. Die instructie kan via een verzoek of via de applicatie worden gegeven.

Binnen de applicaties, die AFAS beschikbaar stelt, zijn verschillende soorten persoonsgegevens vast te leggen. AFAS is zich ervan bewust dat de klant al deze, en eventueel nog zelf aan te maken persoonsgegevens of categorieën, kan invoeren en dat AFAS deze dan zal verwerken. De klant is zelf verantwoordelijk voor de beoordeling of het doel en aard van de verwerking past bij de dienstverlening die AFAS doet.

AFAS verzamelt geanonimiseerde gegevens over het gebruik van haar producten en diensten. Deze gegevens ondersteunen AFAS om inzicht te krijgen of, hoe en hoe vaak bepaalde onderdelen van het product gebruikt worden. De geanonimiseerde gegevens zullen uitsluitend gebruikt worden om producten en dienstverlening te verbeteren. AFAS

zal de verzamelde gebruikersstatistieken **nooit** gebruiken voor commerciële doeleinden of aanbieden aan derde partijen.

Geheimhoudingsplicht

AFAS is zich bewust dat de informatie die de klant met AFAS deelt en opslaat binnen AFAS Online, een geheim en bedrijfsgevoelig karakter heeft. Alle AFAS medewerkers zullen gedurende hun dienstverband en daarna, zoals in hun arbeidsovereenkomst met geheimhoudingsclausule is opgenomen, op verantwoorde wijze met de informatie van de klant omgaan.

Medewerkers met toegang tot klantgegevens
Systeembeheerders van AFAS Online hebben volledige toegang tot de klantgegevens voor:

- het plaatsen van een nieuwe versie;
- het doorvoeren van patches en hotfixes;
- het maken van een back-up;
- het verplaatsen van een gegevens binnen het AFAS Online domein.

Consultants, Supportmedewerkers en andere AFAS medewerkers hebben alleen toegang tot de klantgegevens indien zij toestemming daarvoor hebben ontvangen van de klant en voor zolang zij toestemming hebben van de klant. De klant is via de eigen autorisatietool binnen de applicatie daar zelf verantwoordelijk voor.

Beveiliging

AFAS neemt blijvend passende technische en organisatorische maatregelen om de persoonsgegevens van de klant te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. AFAS is daarvoor ISO27001 gecertificeerd. Deze maatregelen worden aangemerkt als een passend beveiligingsniveau in de zin van de AVG. Meer informatie hierover is te vinden op de speciale AFAS Online pagina in de klantportal. De klant is gerechtigd om in overleg met AFAS tijdens de looptijd van de overeenkomst door een onafhankelijke deskundige de naleving hiervan te controleren, bijvoorbeeld door middel van het uitvoeren van een audit. De klant zal alle kosten in verband met deze controle dragen.

AFAS is aansprakelijk voor schade in het kader van persoonsgegevens door handelen of nalaten van de subverwerker waarbij de aansprakelijkheidsbeperking uit het hoofdstuk Aansprakelijkheid geldt. De toepasselijke aansprakelijkheidsbeperking geldt niet indien er bij de subverwerker sprake is van grove nalatigheid of opzettelijk wangedrag. AFAS is ook niet aansprakelijk in geval van overmacht (zoals gedefinieerd in het hoofdstuk Aansprakelijkheid) bij haarzelf of aan de kant van de subverwerker.

Indien de Autoriteit Persoonsgegevens aan de verwerkersverantwoordelijke een bindende aanwijzing zal geven dient de klant AFAS direct op de hoogte stellen van deze bindende aanwijzing. AFAS zal er alles aan doen wat in redelijkheid van haar verwacht kan worden om de naleving mogelijk te maken. Als AFAS niet doet wat in redelijkheid van haar gevraagd kan worden waardoor er een boete volgt, of als de Autoriteit Persoonsgegevens direct een boete oplegt omdat sprake is van opzet of ernstige verwijtbare nalatigheid aan de kant van AFAS, dan geldt de toepasselijke aansprakelijkheidsbeperking als hiervoor genoemd in het hoofdstuk Aansprakelijkheid niet.

Subverwerkers

AFAS verwerkt de klantdata in datacenters van LeaseWeb Netherlands B.V. en deze is hiermee subverwerker. De datacenters waar AFAS gebruik van maakt bevinden zich uitsluitend in Nederland (Schiphol Rijk en Haarlem) en vallen onder Nederlandse wet- en regelgeving en voldoen aan de strenge Nederlandse en Europese wetgeving met betrekking tot logische en fysieke toegangsbeveiliging en continuïteit. De datacenters zijn minimaal ISO 27001 gecertificeerd. De (persoons)gegevens worden door AFAS en subverwerker uitsluitend verwerkt binnen de Europese Economische ruimte.

AFAS zal geen nieuwe subverwerkers gegevens laten verwerken zonder de klant daarover tijdig te informeren. De klant kan bezwaar maken bij AFAS tegen de subverwerker. AFAS zal deze bezwaren op directieniveau afhandelen. Mocht AFAS toch gegevens willen laten verwerken door de nieuwe subverwerker, heeft de klant de mogelijkheid om de overeenkomst te beëindigen.

Privacyrechten

AFAS heeft geen zeggenschap over de persoonsgegevens die door de klant beschikbaar worden gesteld. Zonder noodzaak, gezien de aard van de door de klant verstrekte opdracht, expliciete toestemming van de klant of wettelijke verplichting zal AFAS de

gegevens niet aan derden verstrekken of voor andere doeleinden verwerken, dan voor de overeengekomen doeleinden. De klant garandeert dat de persoonsgegevens verwerkt mogen worden op basis van een in de AVG genoemde grondslag.

AFAS zal wel, indien een verzoek gedaan wordt door de Stichting Autoriteit Financiële Markten, De Europese Centrale Bank of De Nederlandsche Bank N.V. op grond van de uitvoering van hun taak uit hoofde van de Wft, of op grond van andere wet- en regelgeving, alle mogelijke informatie beschikbaar stellen aan de betreffende organisatie. Tevens verplicht AFAS de subverwerker, zoals hierboven benoemd, eveneens te voldoen aan een dergelijk verzoek van deze toezichthouders.

Betrokkenen
De klant is verantwoordelijk voor de ingevoerde gegevens van de betrokkenen en daarbij voor het informeren en bijstaan van de rechten van de betrokkenen. AFAS zal nooit op verzoeken van betrokkenen ingaan en altijd verwijzen naar de verantwoordelijke. AFAS zal, voor zover dat binnen de applicatie mogelijk is, haar medewerking verlenen aan de klant zodat deze kan voldoen aan zijn wettelijke verplichtingen in het geval dat een betrokkene haar rechten uitoefent op grond van de AVG of andere toepasselijke regelgeving betreffende de verwerking van persoonsgegevens.

Meldplicht datalekken

De AVG vereist dat eventuele datalekken gemeld worden aan de Autoriteit Persoonsgegevens door de verwerkingsverantwoordelijke van de data. AFAS zal daarom zelf geen meldingen doen bij de Autoriteit Persoonsgegevens. Uiteraard zal AFAS de klant juist, tijdig en volledig informeren over relevante incidenten, zodat de klant als verwerkingsverantwoordelijke aan zijn wettelijke verplichtingen kan voldoen. De Beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens geven hierover meer informatie.

Indien de klant een (voorlopige) melding verricht bij de Autoriteit Persoonsgegevens en/of de betrokkene(n) over een datalek **bij AFAS**, zonder dat de klant dit vooraf heeft besproken met AFAS, dan is de klant aansprakelijk voor door AFAS geleden schade en kosten. De klant is daarnaast verplicht een dergelijke melding direct in te trekken.

Bepaling datalek
Voor het bepalen van een datalek, gebruikt AFAS de AVG en de Beleidsregels meldplicht datalekken als leidraad.

Melding aan de klant
Indien blijkt dat bij AFAS sprake is van een beveiligingsincident of datalek zal AFAS de klant daarover zo spoedig mogelijk informeren nadat AFAS bekend is geworden met het datalek. Om dit te realiseren zorgt AFAS ervoor dat al haar medewerkers in staat zijn en blijven om een datalek te constateren en verwacht AFAS van haar opdrachtnemers dat zij AFAS in staat stelt om hier aan te kunnen voldoen. Voor de duidelijkheid: als er een datalek is bij een leverancier van AFAS, dan meldt AFAS dit uiteraard ook. AFAS is het contactpunt voor de klant. De klant hoeft geen contact op te nemen met de leveranciers van AFAS.

Informeren klant (contactpersoon instellen)
In eerste instantie zal AFAS de contactpersoon van het abonnement informeren over een datalek. Mocht deze contactpersoon niet (meer) de juiste zijn, dan kan dat aangepast worden via de klantportal op de pagina 'persoonlijke gegevens'. Kies voor 'aanpassen' en vink het veld 'Meldplicht Datalekken' aan.

Informatie verstrekken
AFAS probeert de klant direct alle informatie te verstrekken die de klant nodig heeft om een eventuele melding bij de Autoriteit Persoonsgegevens en/of de betrokkene(n) te verrichten.

Termijn van informeren
De AVG geeft aan dat er ‘onverwijld’ gemeld moet worden. Dit is volgens de Autoriteit Persoonsgegevens zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na ontdekking ervan door de verantwoordelijke. Indien er een beveiligingsincident optreed zal AFAS de klant zo snel mogelijk, maar uiterlijk binnen 48 uur na het ontdekken door AFAS ervan, informeren. De klant zal zelf de beoordeling moeten maken of het beveiligingsincident valt onder de term ‘datalek’ en of er melding aan de Autoriteit Persoonsgegevens gedaan zal moeten worden. De klant heeft hiervoor 72 uur, nadat de klant hiervan op de hoogte is gesteld, de tijd.

Voortgang en maatregelen
AFAS zal de klant op de hoogte houden over de voortgang en de maatregelen die getroffen worden. AFAS maakt hierover afspraken met de primaire contactpersoon bij de initiële melding. In ieder geval houdt AFAS de klant op de hoogte in geval van een wijziging van de situatie, het bekend worden van nadere informatie en over de maatregelen die getroffen worden.

AFAS registreert alle security incidenten en handelt deze volgens een vaste procedure (workflow) af. De registratie en afhandeling van security incidenten wordt getoetst met een audit in het kader van de ISO27001 certificering.

Gegevens verwijderen

AFAS zal, na afloop van de overeenkomst, alle klant gegevens verwijderen zoals beschreven staat bij ‘Beëindiging van de overeenkomst’. Mocht de klant eerder de gegevens verwijderd willen hebben, dan kan daarvoor een verzoek worden ingediend. AFAS verplicht zich daar gehoor aan te geven.