Verwerkersovereenkomst

Verwerking van persoonsgegevens, artikel 28 AVG

De partijen zijn de leverancier en de klant die in het klantblad zijn genoemd; bij een bestelling via de website geldt de bestelling als klantblad, zoals artikel 1 van de algemene voorwaarden bepaalt. De klant is verwerkingsverantwoordelijke voor de persoonsgegevens in de dossiers die hij aanlevert. De leverancier verwerkt die gegevens uitsluitend namens de klant en voor de dienst uit het klantblad. Dit deel legt vast hoe dat gebeurt.

B1. Onderwerp, duur en doel

Doel	Uit de documentenset van een financieringsaanvraag een concept-memorandum samenstellen, met bronvermelding per gegeven en kengetallen volgens het rekenmodel uit artikel 2 van de algemene voorwaarden.
Aard van de verwerking	Ontvangen, lezen, ordenen, analyseren, vastleggen, beschikbaar stellen voor download en verwijderen.
Duur	Zolang de overeenkomst loopt, plus de bewaartermijnen uit B5.
Betrokkenen	Ondernemers en hun eventuele partners, bestuurders, aandeelhouders en andere personen die in de aangeleverde stukken voorkomen, en de medewerkers van de klant die inloggen.
Gegevens	Naam, adres en contactgegevens; functie en aandeelhoudersbelang; financiële gegevens uit jaarrekeningen, aangiften en privéstukken; gegevens uit het handelsregister. In aangiften inkomstenbelasting kan een burgerservicenummer voorkomen. De dienst heeft dat nummer niet nodig en gebruikt het nergens voor; de klant schermt het af vóór het uploaden. Zie B10. Inloggegevens van medewerkers van de klant.

B2. Instructies

De leverancier verwerkt de gegevens uitsluitend op schriftelijke instructie van de klant. Deze overeenkomst en het gebruik van de dienst gelden als die instructie. De leverancier gebruikt de gegevens niet voor eigen doeleinden en meldt het de klant wanneer een instructie naar zijn oordeel in strijd is met de AVG. Verwerkt de leverancier op grond van een wettelijke verplichting, dan meldt hij dat vooraf, tenzij die wet dat verbiedt.

B3. Geheimhouding en personeel

Iedereen die namens de leverancier toegang heeft tot de gegevens is tot geheimhouding verplicht. Toegang wordt alleen verleend voor zover nodig voor beheer, ondersteuning en storingsoplossing. De leverancier werkt als eenmanszaak; schakelt hij personeel of hulppersonen in, dan bindt hij hen aan dezelfde verplichtingen.

B4. Beveiliging

De maatregelen hieronder zijn de staat waarin de dienst wordt opgeleverd. Tot het moment waarop de leverancier schriftelijk bevestigt dat zij alle werken, worden er geen echte klantdossiers verwerkt, ook niet kosteloos of bij wijze van proef.

- Versleutelde verbinding tussen browser en server.
- Een persoonlijke login per medewerker. Bij een abonnement hoort daar tweestapsverificatie bij: een code uit een authenticator-app, bij iedere nieuwe sessie gevraagd. In de gratis proef logt een medewerker in met e-mailadres en wachtwoord; tweestapsverificatie is dan niet verplicht en kan wel zelf worden aangezet. Gedeelde inloggegevens zijn niet toegestaan.
- Sessies verlopen na dertig minuten zonder activiteit en in elk geval na acht uur; de beheerder kan alle sessies ineens intrekken, accounts blokkeren, en het aantal inlogpogingen is begrensd.
- Toegang uitsluitend tot de gegevens van de eigen vestiging, afgedwongen bij inloggen, het aanmaken en uitvoeren van een verwerkingsopdracht, de aanroep naar het taalmodel, opslaan, downloaden en registreren; bij iedere nieuwe versie van de dienst wordt automatisch met twee vestigingen getest dat die scheiding standhoudt.
- Een logboek van inloggen, gestarte dossiers en downloads per gebruiker, zonder documentinhoud. Geüploade bestanden worden verwijderd zodra de verwerking klaar is.
- Alle dossiergegevens worden versleuteld bewaard met een eigen sleutel per vestiging: de geüploade documenten, de gegevens van een lopende verwerking en het resultaat. Leesbare inhoud bestaat alleen kortstondig in het werkgeheugen en nooit op schijf; tijdelijke bestanden staan uitsluitend in het werkgeheugen en worden na de verwerking verwijderd; dat geldt ook voor het afschermen van gegevens, tekstherkenning en het opbouwen van het Word-document.
- De dienst draait op een virtuele server die de leverancier ook voor andere eigen toepassingen gebruikt. De dienst is daar afgeschermd: hij draait onder een eigen systeemgebruiker, de dossiergegevens staan op een eigen opslagvolume, de sleutels zijn alleen voor die gebruiker leesbaar en de dienst is niet rechtstreeks van buitenaf bereikbaar. De andere toepassingen draaien onder een andere gebruiker en kunnen de sleutels en dossiergegevens niet lezen.
- Die versleutelde gegevens en de hoofdsleutel staan op gescheiden opslag, zodat geen enkele kopie of momentopname allebei bevat. Dat beschermt tegen een gelekte kopie van de opslag, niet tegen iemand die toegang krijgt tot de draaiende server; de schijf als geheel is niet versleuteld.
- Van de accounts, de gegevens voor tweestapsverificatie, de gebruiksregistratie en het logboek staat een versleutelde reservekopie op een derde plek, zonder dossiergegevens en zonder de hoofdsleutel, met een eigen sleutel die de leverancier buiten de server bewaart. Zo blijven de termijnen uit B5 en onderzoek na een incident ook na uitval van de server mogelijk.

De maatregelen zijn afgestemd op de aard van de gegevens en de stand van de techniek. Wijzigt de leverancier ze, dan blijft het beschermingsniveau ten minste gelijk.

B5. Bewaren en verwijderen

Geüploade documenten worden na de verwerking van de server van de leverancier verwijderd. Het resultaat van een dossier blijft **ten hoogste 24 uur** beschikbaar om te downloaden en wordt daarna automatisch verwijderd; de klant krijgt vóór die tijd een herinnering. Een langere termijn geldt alleen wanneer partijen dat schriftelijk afspreken.

Wat daarna bewaard blijft: de gebruiksregistratie (dossier-id en etiket, tijdstip, wie de verwerking startte, uitkomst) vierentwintig maanden, het logboek uit B4 twaalf maanden, de facturen zeven jaar zoals de wet verlangt, en de accounts met de gegevens voor tweestapsverificatie zolang die accounts bestaan. Een account en de bijbehorende gegevens voor tweestapsverificatie worden verwijderd zodra het wordt ingetrokken, en in elk geval bij het einde van de overeenkomst; de reservekopie uit B4 volgt dezelfde termijnen. Geen van deze gegevens bevat documentinhoud. Bij het einde van de verwerking kiest de klant of de leverancier de nog aanwezige gegevens aan hem teruggeeft of verwijdert; de leverancier voert die keuze binnen dertig dagen uit, ook voor bestaande kopieën, tenzij hij ze wettelijk moet bewaren. Dat laatste geldt alleen voor de facturen en de gegevens die daarvoor nodig zijn; die horen bij de eigen administratie van de leverancier en worden apart bewaard van de klantgegevens. Op verzoek bevestigt de leverancier teruggave of verwijdering schriftelijk.

B6. Subverwerkers

De klant geeft toestemming voor de subverwerkers die in de bijlage bij dit deel zijn opgenomen; die bijlage is de volledige en actuele lijst. Onder meer de volgende partijen worden ingeschakeld:

Anthropic	De taalmodellen die de documenten lezen en het concept schrijven, via de zakelijke interface. De geldende voorwaarden voor training en bewaring, het land van verwerking en het doorgiftemechanisme staan in de bijlage.
Hetzner	De server waarop de dienst draait, in het datacentrum in Helsinki, Finland.
Cloudflare	De beveiligde verbinding tussen de gebruiker en de server; het verkeer loopt langs het netwerk van deze partij.
Stripe	De abonnementsadministratie en de betalingen: bedrijfsnaam, adres, btw-nummer, e-mailadres en betaalgegevens (betaalkaart of bankrekening) van de klant. Geen dossiergegevens.

De leverancier legt elke subverwerker bij overeenkomst dezelfde verplichtingen inzake gegevensbescherming op als in dit deel zijn opgenomen, waaronder in elk geval geheimhouding, passende beveiliging en medewerking aan de rechten van betrokkenen, en blijft jegens de klant volledig verantwoordelijk voor het nakomen daarvan. De technische uitvoering verschilt per partij: de maatregelen die hieronder in de bijlage per subverwerker staan, zijn de maatregelen die met die partij zijn overeengekomen. De maatregelen uit B4 en de bewaartermijn uit B5 gelden voor de dienst van de leverancier zelf; een subverwerker hanteert de termijnen en maatregelen van zijn eigen dienst, die per partij in de bijlage staan. Wil de leverancier een subverwerker toevoegen of vervangen, dan meldt hij dat ten minste dertig dagen vooraf; maakt de klant binnen die termijn schriftelijk bezwaar op redelijke gronden, dan mag hij de overeenkomst per die datum beëindigen zonder kosten.

Per subverwerker staan het land van verwerking en, bij verwerking buiten de Europese Economische Ruimte, het toegepaste doorgiftemechanisme uit hoofdstuk V AVG in de bijlage bij dit deel. De leverancier houdt die bijlage actueel en verstrekt op verzoek inzage in de onderliggende waarborg.

B7. Rechten van betrokkenen

Wendt een betrokkene zich rechtstreeks tot de leverancier, dan verwijst de leverancier hem door naar de klant en informeert hij de klant. De leverancier helpt de klant binnen redelijke termijn bij verzoeken om inzage, correctie, verwijdering, beperking of overdracht, voor zover de klant dat niet zelf in de dienst kan doen. Daarnaast helpt de leverancier de klant, met de informatie waarover hij beschikt, bij het beveiligen van de verwerking, het melden en afhandelen van datalekken, het uitvoeren van een gegevensbeschermingseffectbeoordeling en een eventuele voorafgaande raadpleging van de toezichthouder.

B8. Datalekken

De leverancier meldt een inbreuk in verband met persoonsgegevens zonder onredelijke vertraging aan de klant, en in elk geval binnen achtenveertig uur nadat hij daarvan kennis heeft gekregen, met wat bekend is over de aard, de betrokken gegevens en personen, de gevolgen en de genomen maatregelen. Hij helpt de klant bij diens melding aan de Autoriteit Persoonsgegevens en aan betrokkenen. De klant beslist zelf of hij meldt; de leverancier meldt niet namens de klant.

B9. Controle

De leverancier geeft op verzoek de informatie die nodig is om naleving van dit deel aan te tonen, en werkt mee aan controles door de klant of een door de klant gemachtigde. Een reguliere controle vindt ten hoogste eens per jaar plaats en wordt ten minste twee weken vooraf gemeld; bij een datalek, een gerede aanwijzing van niet-naleving of een wettelijke verplichting van de klant kan een controle ook tussentijds en op kortere termijn plaatsvinden. De kosten draagt de klant, tenzij de controle een wezenlijke tekortkoming aantoont.

B10. Burgerservicenummer en bijzondere gegevens

De dienst heeft geen burgerservicenummer nodig en gebruikt het nergens voor. Komt het nummer toch in een aangeleverd document voor, dan wordt het wel degelijk ontvangen en doorgestuurd, en dus verwerkt; die verwerking berust uitsluitend op de aanlevering door de klant. Het nummer kan wel voorkomen in aangiften die de klant aanlevert. Zolang de leverancier geen controle heeft die het nummer in zowel digitale documenten als scans aantoonbaar onderschept, blijft het afschermen vóór het uploaden een taak van de klant. Die controle draait wanneer zij er is volledig op de eigen server van de leverancier; er komt geen extra partij aan te pas. Zodra zij beschikbaar is, meldt de leverancier dat en wordt deze bepaling aangepast.

Hetzelfde geldt voor andere gevoelige gegevens die in aangiften en privéstukken kunnen staan, zoals gegevens over gezondheid, zorgkosten of lidmaatschappen. De dienst heeft die niet nodig; de klant verwijdert of schermt ze af vóór het uploaden. Constateert de leverancier dat zulke gegevens toch zijn meegestuurd, dan meldt hij dat aan de klant, verwerkt hij het betreffende document niet verder en verwijdert hij het.

B11. Aansprakelijkheid en rangorde

Op dit deel is de aansprakelijkheidsregeling uit het klantblad van toepassing, of, als het klantblad die niet bevat, die uit artikel 7 van de algemene voorwaarden, voor zover de AVG dat toelaat. Wijken het klantblad of de algemene voorwaarden af van dit deel waar het de verwerking van persoonsgegevens betreft, dan gaat dit deel voor.

Bijlage · Subverwerkers

Land van verwerking en grondslag voor doorgifte

Deze bijlage hoort bij B6 en wordt door de leverancier actueel gehouden. Bij een wijziging meldt hij dat ten minste dertig dagen vooraf, zoals in B6 is bepaald.

Overzicht

Hetzner	**Rol:** de server waarop de dienst draait en waarop de versleutelde dossiergegevens staan. **Entiteit en land:** Hetzner Online GmbH, Duitsland; de server staat in het datacentrum in Helsinki, Finland. **Doorgifte:** geen. Zowel de leverancier als het datacentrum bevinden zich binnen de Europese Economische Ruimte.
Anthropic	**Rol:** het taalmodel dat de documenten leest en het concept schrijft, via de zakelijke programmeerkoppeling. **Land:** verkeer kan worden gerouteerd naar landen in de Verenigde Staten, Europa, Azië en Australië; opslag vindt plaats in de Verenigde Staten. **Doorgifte:** de verwerkersovereenkomst van Anthropic met daarin de standaardcontractbepalingen van de Europese Commissie maakt deel uit van de zakelijke voorwaarden. **Training:** "Anthropic may not train models on Customer Content from Services" (zakelijke voorwaarden, onderdeel B). **Bewaring:** invoer en uitvoer worden binnen 30 dagen na ontvangst verwijderd. Wordt materiaal gemarkeerd wegens vermoedelijke schending van het gebruiksbeleid, dan tot 2 jaar, en classificatiescores tot 7 jaar. **Let op bij bestanden:** de functie voor het uploaden van bestanden valt buiten een eventuele afspraak over nulretentie; bestanden blijven daar staan tot ze uitdrukkelijk worden verwijderd of vervallen. PDF-bestanden die rechtstreeks in het bericht worden meegestuurd vallen er wel onder. De leverancier verwijdert geüploade bestanden direct na verwerking.
Cloudflare	**Rol:** de beveiligde verbinding tussen gebruiker en server; het verkeer loopt langs het netwerk van deze partij. Verwerkt geen dossiergegevens in rust. **Entiteit en land:** Cloudflare, Inc., Verenigde Staten, met een wereldwijd netwerk. **Rol volgens de overeenkomst:** verwerker of subverwerker. **Doorgifte:** de standaardcontractbepalingen van de Europese Commissie, aangevuld met het gegevensbeschermingskader tussen de Europese Unie en de Verenigde Staten waar die certificering geldt.

Overzicht, vervolg

Stripe	**Rol:** abonnementsadministratie en betalingen: bedrijfsnaam, adres, btw-nummer, e-mailadres en betaalgegevens (betaalkaart of bankrekening) van de klant. Geen dossiergegevens. **Entiteit:** Stripe Payments Europe, Limited (Ierland) voor klanten buiten Noord- en Zuid-Amerika. **Rolverdeling:** voor het uitvoeren van de betaaldienst treedt Stripe op als verwerker; voor eigen doeleinden zoals fraudebestrijding en naleving van financiële regelgeving bepaalt Stripe zelf doel en middelen en is zij verwerkingsverantwoordelijke. Dat tweede deel valt niet onder deze verwerkersovereenkomst. **Doorgifte:** via het addendum gegevensoverdracht van Stripe, met standaardcontractbepalingen en, waar van toepassing, het gegevensbeschermingskader tussen de Europese Unie en de Verenigde Staten.
E-mailvoorziening	**Rol:** correspondentie, meldingen en herinneringen aan gebruikers; contactgegevens en berichten zonder dossierinhoud. Blijft ook bestaan wanneer er geen berichtendienst wordt gebruikt. **Aanbieder:** de e-mailvoorziening bij het adres arn@quicknet.nl, geleverd door VodafoneZiggo, Nederland. **Doorgifte:** geen; verwerking binnen de Europese Economische Ruimte.
Opslag van de reservekopie	**Rol:** versleutelde reservekopie van accounts, gegevens voor tweestapsverificatie, gebruiksregistratie en logboek; geen dossiergegevens. **Waar:** de versleutelde kopie wordt dagelijks op de server gemaakt en daarna bewaard op apparatuur van de leverancier zelf in Nederland: een versleutelde werkcomputer en een versleutelde externe schijf. Alleen de leverancier heeft de sleutel om haar te openen. Er is hiervoor geen externe partij ingeschakeld. **Doorgifte:** geen.