Verwerkersovereenkomst

Audit Copilot
The Next Stapp B.V.

Onderwerp	Gegevens
Product	Audit Copilot (auditcopilot.nl), inclusief de Excel-invoegtoepassing
Verwerker	The Next Stapp B.V., Saelde 13, 5051 WL Goirle, Nederland (KvK 74720201)
Versie	1.0 – september 2026
Status	Ter ondertekening
Contact privacy	privacy@thenextstapp.nl

Deze verwerkersovereenkomst legt vast hoe The Next Stapp B.V. persoonsgegevens verwerkt in het kader van de levering van Audit Copilot, en voldoet aan de eisen van artikel 28 lid 3 van de Algemene Verordening Gegevensbescherming (AVG). Bijlage 1 beschrijft de concrete verwerkingen, Bijlage 2 de technische en organisatorische beveiligingsmaatregelen en Bijlage 3 de ingeschakelde subverwerkers.

Partijen

1. The Next Stapp B.V., statutair gevestigd te Goirle en kantoorhoudend aan Saelde 13, 5051 WL te Goirle, Nederland, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 74720201, rechtsgeldig vertegenwoordigd door de heer J.F. van der Heijden, algemeen directeur, hierna te noemen: **"Verwerker"**;

en

2. _____, statutair gevestigd en kantoorhoudend aan **_____**, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer _____, rechtsgeldig vertegenwoordigd door _____, hierna te noemen: **"Verwerkingsverantwoordelijke"**;

hierna gezamenlijk te noemen: **"Partijen"** en ieder afzonderlijk: **"Partij"**.

Overwegende dat

- Verwerker de webapplicatie Audit Copilot levert, waarmee accountantskantoren en auditteams financiële administraties geautomatiseerd inlezen, samenvoegen, analyseren en vastleggen ten behoeve van de controle- en samenstelpraktijk (de "**Dienst**");
- Verwerkingsverantwoordelijke de Dienst afneemt op grond van een tussen Partijen gesloten overeenkomst (de "**Hoofdovereenkomst**");
- Verwerker bij het leveren van de Dienst persoonsgegevens verwerkt die afkomstig zijn uit de administraties van Verwerkingsverantwoordelijke en van diens cliënten;
- Verwerkingsverantwoordelijke het doel en de middelen van die verwerking bepaalt en daarmee optreedt als verwerkingsverantwoordelijke, en Verwerker uitsluitend in opdracht van Verwerkingsverantwoordelijke handelt;
- Partijen op grond van artikel 28 lid 3 AVG de afspraken over die verwerking schriftelijk wensen vast te leggen;

komen Partijen het volgende overeen.

Artikel 1 – Onderwerp en begrippen

1.1 Deze Verwerkersovereenkomst is uitsluitend van toepassing op de verwerking van Persoonsgegevens in het kader van de Hoofdovereenkomst. Deze Verwerkersovereenkomst maakt onlosmakelijk deel uit van de Hoofdovereenkomst; alle bepalingen van de Hoofdovereenkomst zijn daarop van toepassing.

1.2 Begrippen als "verwerking", "persoonsgegevens", "betrokkene", "verwerkingsverantwoordelijke", "verwerker" en "inbreuk in verband met persoonsgegevens" hebben de betekenis die daaraan in de Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679, hierna: "**AVG**") is toegekend.

1.3 Verwerker verwerkt Persoonsgegevens ten behoeve van Verwerkingsverantwoordelijke, uitsluitend voor de doeleinden en op de wijze zoals nader uiteengezet in **Bijlage 1**.

1.4 Bij strijdigheid tussen deze Verwerkersovereenkomst en de Hoofdovereenkomst prevaleert deze Verwerkersovereenkomst, voor zover het de verwerking van Persoonsgegevens betreft.

Artikel 2 – Rolverdeling en instructies

2.1 Verwerker treedt op als verwerker in de zin van artikel 4 lid 8 AVG. Verwerkingsverantwoordelijke treedt op als verwerkingsverantwoordelijke in de zin van artikel 4 lid 7 AVG. Voor zover Verwerkingsverantwoordelijke de Dienst gebruikt ten behoeve van een cliënt die zelf verwerkingsverantwoordelijke is, staat Verwerkingsverantwoordelijke ervoor in dat hij bevoegd is deze Verwerkersovereenkomst mede namens die cliënt aan te gaan.

2.2 Partijen komen overeen dat deze Verwerkersovereenkomst en de Hoofdovereenkomst – inclusief de instructies die Verwerkingsverantwoordelijke geeft door middel van het inrichten en gebruiken van de Dienst, zoals het koppelen van een administratie, het uploaden van bestanden en het starten van een import of analyse – de volledige, gedocumenteerde instructies van Verwerkingsverantwoordelijke vormen.

2.3 Verwerker verwerkt de Persoonsgegevens uitsluitend op basis van deze instructies en niet voor eigen doeleinden. Verwerker gebruikt de Persoonsgegevens niet voor het trainen of verbeteren van modellen voor kunstmatige intelligentie, noch voor profilering, verrijking of commerciële doeleinden.

2.4 Indien Verwerker op grond van Unierechtelijke of lidstaatrechtelijke bepalingen verplicht is tot een verwerking die verder gaat dan de instructies, stelt Verwerker Verwerkingsverantwoordelijke daarvan voorafgaand aan de verwerking in kennis, tenzij die wetgeving deze kennisgeving verbiedt om gewichtige redenen van algemeen belang.

2.5 Verwerker informeert Verwerkingsverantwoordelijke onverwijld indien een instructie naar zijn oordeel in strijd is met de AVG of met andere toepasselijke gegevensbeschermingswetgeving.

2.6 Verwerkingsverantwoordelijke is verantwoordelijk voor de rechtmatigheid van de verwerking en de grondslag daarvan, voor de juistheid en actualiteit van de aangeleverde Persoonsgegevens en voor het gebruik dat hij van de resultaten van de Dienst maakt. Verwerkingsverantwoordelijke bepaalt zelf welke administraties, bestanden en documenten hij aan de Dienst toevertrouwt en onthoudt zich van het aanleveren van Persoonsgegevens die redelijkerwijs niet nodig zijn voor het doel van de Dienst.

2.7 De Dienst is niet bestemd voor het structureel verwerken van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9 AVG of van het burgerservicenummer. Verwerkingsverantwoordelijke draagt er zorg voor dergelijke gegevens niet aan te leveren, behoudens voor zover dit onvermijdelijk voortvloeit uit de aard van de gecontroleerde administratie, zoals beschreven in Bijlage 1.

Artikel 3 – Geheimhouding

3.1 Onverminderd bestaande geheimhoudingsverplichtingen tussen Partijen houdt Verwerker de Persoonsgegevens strikt geheim en verstrekt deze niet aan derden, tenzij dit voortvloeit uit deze Verwerkersovereenkomst of uit een wettelijke verplichting.

3.2 Verwerker verleent uitsluitend toegang tot de Persoonsgegevens aan personen voor wie die toegang noodzakelijk is voor de uitvoering van de Dienst. Verwerker draagt er zorg voor dat deze personen zich tot geheimhouding hebben verbonden of door een passende wettelijke verplichting tot vertrouwelijkheid zijn gebonden.

3.3 Verwerker is zich ervan bewust dat de verwerkte gegevens mede vallen onder de geheimhoudingsplicht die op accountants rust, en behandelt deze gegevens met een daarop afgestemde zorgvuldigheid.

Artikel 4 – Beveiliging

4.1 Verwerker treft passende technische en organisatorische maatregelen als bedoeld in artikel 32 AVG om de Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen zijn beschreven in **Bijlage 2** en houden rekening met de stand van de techniek, de uitvoeringskosten en de aard, omvang, context en doeleinden van de verwerking, alsmede met de risico's voor de rechten en vrijheden van betrokkenen.

4.2 De maatregelen omvatten in ieder geval versleuteling van gegevens tijdens transport en in rust, versleutelde opslag van wachtwoorden, logische scheiding van de gegevens van verschillende klanten en administraties, toegang op basis van rollen en het beperken van toegang tot wat noodzakelijk is.

4.3 Partijen erkennen dat beveiliging een voortdurende inspanning vergt. Verwerker mag de maatregelen wijzigen of vervangen, mits het beschermingsniveau daardoor niet wezenlijk afneemt.

4.4 Verwerkingsverantwoordelijke is verantwoordelijk voor het zorgvuldig beheer van de aan zijn gebruikers verstrekte inloggegevens, voor het tijdig intrekken van toegang van vertrokken medewerkers en voor de beveiliging van de eigen apparatuur en netwerkomgeving.

Artikel 5 – Controle en audit

5.1 Verwerker stelt Verwerkingsverantwoordelijke op verzoek alle informatie ter beschikking die nodig is om de nakoming van de verplichtingen uit artikel 28 AVG aan te tonen.

5.2 Verwerkingsverantwoordelijke heeft het recht om ten hoogste eenmaal per kalenderjaar een audit te laten uitvoeren naar de naleving van deze Verwerkersovereenkomst, alsmede na een vastgestelde inbreuk in verband met persoonsgegevens die de gegevens van Verwerkingsverantwoordelijke raakt.

5.3 Een audit wordt uitgevoerd door een onafhankelijke, aan geheimhouding gebonden deskundige, na een aankondiging van ten minste dertig (30) dagen, tijdens kantooruren en op zodanige wijze dat de bedrijfsvoering van Verwerker zo min mogelijk wordt verstoord. De audit strekt zich niet uit tot gegevens van andere klanten van Verwerker.

5.4 De kosten van de audit komen voor rekening van Verwerkingsverantwoordelijke, tenzij uit de audit blijkt dat Verwerker in belangrijke mate tekortschiet in de nakoming van deze Verwerkersovereenkomst. In dat laatste geval draagt Verwerker de redelijke kosten en voert hij de noodzakelijke verbeteringen zonder onnodige vertraging door.

5.5 Verwerker mag aan de auditverplichting voldoen door het overleggen van een actuele, door een onafhankelijke deskundige opgestelde assurancerapportage of certificering die de relevante beheersmaatregelen dekt, alsmede door de van zijn subverwerkers verkregen rapportages.

Artikel 6 – Doorgifte buiten de Europese Economische Ruimte

6.1 De Persoonsgegevens worden opgeslagen binnen de Europese Unie. De productieomgeving van de Dienst is ondergebracht bij Microsoft Azure in de regio Zweden (Sweden Central); back-ups en uitwijkvoorzieningen bevinden zich in de daaraan gekoppelde Azure-regio binnen de Europese Unie.

6.2 Verwerker geeft geen Persoonsgegevens door aan een land buiten de Europese Economische Ruimte of aan een internationale organisatie, tenzij daarvoor een geldig overdrachtsmechanisme als bedoeld in hoofdstuk V AVG geldt – zoals een adequaatheidsbesluit of door de Europese Commissie vastgestelde modelcontractbepalingen – en de noodzakelijke aanvullende maatregelen zijn getroffen.

6.3 In afwijking van het bepaalde in lid 1 vindt de geautomatiseerde analyse van documenten en werkbladen plaats bij Anthropic, gevestigd in de Verenigde Staten. Daarbij worden de betrokken documenten en de daaruit afgeleide tekst naar die dienst verzonden. Deze doorgifte berust op de door de Europese Commissie vastgestelde modelcontractbepalingen, aangevuld met de in Bijlage 2 beschreven maatregelen. De aangeboden gegevens worden niet gebruikt voor het trainen van modellen. Bijlage 3 vermeldt per subverwerker de regio en de grondslag voor doorgifte.

6.4 Enkele in Bijlage 3 genoemde subverwerkers maken deel uit van een concern dat buiten de Europese Economische Ruimte is gevestigd. Voor zover de verwerking en opslag van de Persoonsgegevens bij deze subverwerkers blijkens Bijlage 3 binnen de Europese Unie plaatsvindt, zijn voor eventuele toegang vanuit een derde land modelcontractbepalingen overeengekomen.

Artikel 7 – Inbreuken in verband met persoonsgegevens (datalekken)

7.1 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging, en in beginsel binnen achtenveertig (48) uur nadat hij daarvan kennis heeft genomen, over iedere inbreuk in verband met persoonsgegevens die de Persoonsgegevens van Verwerkingsverantwoordelijke raakt.

7.2 Onder een inbreuk in verband met persoonsgegevens wordt verstaan: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde

verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens.

7.3 De melding bevat ten minste, voor zover bekend: de aard van de inbreuk, de betrokken categorieën en het aantal betrokkenen en gegevens, de waarschijnlijke gevolgen, de reeds getroffen en voorgenomen maatregelen, en de contactgegevens voor nadere informatie. Ontbrekende informatie wordt zo spoedig mogelijk nagezonden.

7.4 Verwerkingsverantwoordelijke beoordeelt zelf of de inbreuk moet worden gemeld bij de Autoriteit Persoonsgegevens en aan betrokkenen. Verwerker doet dergelijke meldingen niet uit eigen beweging namens Verwerkingsverantwoordelijke, maar verleent daarbij alle redelijkerwijs benodigde medewerking.

7.5 Verwerker documenteert iedere inbreuk, treft onverwijld maatregelen om de gevolgen te beperken en herhaling te voorkomen, en informeert Verwerkingsverantwoordelijke over de afhandeling.

7.6 Ontvangt Verwerker een klacht of verzoek van een betrokkene, een toezichthouder of een andere derde dat betrekking heeft op de Persoonsgegevens, dan handelt hij deze niet zelfstandig af, maar stuurt hij deze onverwijld door aan Verwerkingsverantwoordelijke.

Artikel 8 – Bijstand aan Verwerkingsverantwoordelijke

8.1 Rekening houdend met de aard van de verwerking verleent Verwerker Verwerkingsverantwoordelijke passende bijstand bij het vervullen van diens plicht om verzoeken van betrokkenen te beantwoorden die betrekking hebben op de uitoefening van hun rechten uit hoofdstuk III AVG, waaronder het recht op inzage, rectificatie, wissing, beperking, overdraagbaarheid en bezwaar.

8.2 Verwerker verleent deze bijstand door middel van de functionaliteit die de Dienst biedt en, waar die functionaliteit ontoereikend is, door redelijke ondersteuning op verzoek. Verwerkingsverantwoordelijke beschikt zelf over de mogelijkheid gegevens in te zien, te corrigeren en de gegevens van een administratie te laten verwijderen.

8.3 Verwerker verleent tevens redelijke bijstand bij het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) en bij een voorafgaande raadpleging van de toezichthouder, voor zover deze betrekking hebben op de verwerkingen die onder deze Verwerkersovereenkomst vallen.

8.4 Verwerker mag voor bijstand die de gebruikelijke ondersteuning aanzienlijk te boven gaat een redelijke vergoeding in rekening brengen, mits hij dit vooraf kenbaar maakt.

Artikel 9 – Subverwerkers

9.1 Verwerkingsverantwoordelijke verleent Verwerker hierbij algemene schriftelijke toestemming om subverwerkers in te schakelen bij de uitvoering van de Dienst. De op het moment van ondertekening ingeschakelde subverwerkers zijn opgenomen in **Bijlage 3**.

9.2 Verwerker informeert Verwerkingsverantwoordelijke over de voorgenomen toevoeging of vervanging van een subverwerker ten minste dertig (30) dagen voordat die wijziging ingaat. Verwerkingsverantwoordelijke kan binnen die termijn op redelijke, met de gegevensbescherming verband houdende gronden schriftelijk bezwaar maken.

9.3 Komen Partijen na een tijdig bezwaar niet binnen een redelijke termijn tot een oplossing, dan is Verwerkingsverantwoordelijke gerechtigd de Hoofdovereenkomst op te zeggen voor het onderdeel waarop de betreffende verwerking betrekking heeft, zonder daarbij schadeplichtig te worden.

9.4 Verwerker legt iedere subverwerker bij overeenkomst verplichtingen op die ten minste gelijkwaardig zijn aan de verplichtingen uit deze Verwerkersovereenkomst. Verwerker blijft jegens Verwerkingsverantwoordelijke volledig aansprakelijk voor het nakomen van die verplichtingen door de subverwerker.

9.5 Een actueel overzicht van subverwerkers is op verzoek beschikbaar via privacy@thenextstapp.nl.

Artikel 10 – Bewaren, teruggave en verwijdering

10.1 Verwerker bewaart de Persoonsgegevens niet langer dan noodzakelijk is voor de uitvoering van de Dienst of dan wettelijk is voorgeschreven. De bewaartermijnen zijn nader beschreven in Bijlage 1.

10.2 Op eerste verzoek van Verwerkingsverantwoordelijke, en in ieder geval bij het einde van de Hoofdovereenkomst, verwijdert Verwerker naar keuze van Verwerkingsverantwoordelijke alle Persoonsgegevens of geeft hij deze in een gangbaar, gestructureerd formaat terug.

10.3 Verwerker verwijdert de Persoonsgegevens binnen dertig (30) dagen na het einde van de Hoofdovereenkomst, dan wel binnen dertig (30) dagen na een daartoe strekkend verzoek, tenzij Unierechtelijke of lidstaatrechtelijke bepalingen hem verplichten de gegevens langer te bewaren. In dat laatste geval informeert Verwerker Verwerkingsverantwoordelijke over de grondslag en de duur daarvan.

10.4 Reguliere back-ups worden volgens het geldende back-upschema overschreven en vervolgens vernietigd. Gedurende die periode blijven de gegevens uitsluitend beschikbaar voor herstel na een calamiteit en worden zij niet voor andere doeleinden gebruikt.

10.5 Verwerker bevestigt de verwijdering op verzoek schriftelijk.

Artikel 11 – Aansprakelijkheid

11.1 De in de Hoofdovereenkomst opgenomen bepalingen inzake aansprakelijkheid en vrijwaring zijn onverkort van toepassing op deze Verwerkersovereenkomst, behoudens voor zover dwingend recht zich daartegen verzet.

11.2 Iedere Partij is aansprakelijk voor de schade die het gevolg is van haar eigen tekortkoming in de nakoming van deze Verwerkersovereenkomst of van een aan haar toe te rekenen schending van de AVG.

11.3 Verwerkingsverantwoordelijke vrijwaart Verwerker voor aanspraken van derden die voortvloeien uit het feit dat de door Verwerkingsverantwoordelijke gegeven instructies of aangeleverde gegevens in strijd zijn met toepasselijke wetgeving.

Artikel 12 – Duur, wijziging en slotbepalingen

12.1 Deze Verwerkersovereenkomst treedt in werking op de datum van ondertekening door beide Partijen en geldt voor de duur van de Hoofdovereenkomst. Zij eindigt van rechtswege zodra de Hoofdovereenkomst eindigt en Verwerker geen Persoonsgegevens meer voor Verwerkingsverantwoordelijke verwerkt.

12.2 Beëindiging van deze Verwerkersovereenkomst laat onverlet de bepalingen die naar hun aard bestemd zijn om ook daarna voort te duren, waaronder de artikelen 3, 7, 10 en 11.

12.3 Wijzigingen van deze Verwerkersovereenkomst zijn slechts geldig indien deze schriftelijk door beide Partijen zijn overeengekomen. Indien wetgeving, rechtspraak of een aanwijzing van een toezichthouder daartoe noopt, treden Partijen in overleg over de noodzakelijke aanpassing.

12.4 Is een bepaling van deze Verwerkersovereenkomst nietig of vernietigbaar, dan blijven de overige bepalingen onverkort van kracht. Partijen vervangen de betreffende bepaling door een geldige bepaling die de strekking daarvan zo veel mogelijk benadert.

12.5 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing. Geschillen worden voorgelegd aan de bevoegde rechter in het arrondissement Zeeland-West-Brabant, tenzij de Hoofdovereenkomst een andere forumkeuze bevat.

Aldus overeengekomen en in tweevoud ondertekend

The Next Stapp B.V. (Verwerker)	**Verwerkingsverantwoordelijke**
Naam: J.F. van der Heijden	Naam:
Functie: Algemeen directeur	Functie:
Plaats:	Plaats:
Datum:	Datum:
Handtekening:	Handtekening:

Bijlage 1 – Omvang, aard en doel van de verwerking

Deze bijlage beschrijft de verwerkingen die Verwerker in het kader van Audit Copilot uitvoert, zoals bedoeld in artikel 28 lid 3 AVG.

1. Onderwerp en aard van de verwerking

Audit Copilot is een meergebruikers-SaaS-oplossing waarmee accountants en auditteams de financiële administraties van hun cliënten geautomatiseerd inlezen, normaliseren, analyseren en vastleggen. De verwerking bestaat uit het overnemen van gegevens uit boekhoudpakketten en aangeleverde bestanden, het opslaan daarvan in een centraal gegevensmodel, het uitvoeren van analyses en controles, het koppelen van banktransacties aan grootboekposten en het beschikbaar stellen van de resultaten in de webapplicatie en de Excel-invoegtoepassing.

2. Doeleinden van de verwerking

- het geautomatiseerd inlezen en samenvoegen van financiële administraties ten behoeve van de controle- of samenstelopdracht van Verwerkingsverantwoordelijke;
- het uitvoeren van cijferanalyses, aansluitingscontroles en steekproeven op de ingelezen administratie;
- het afletteren van bankmutaties tegen grootboekposten en het vastleggen van de gevonden koppelingen;
- het herkennen en ontsluiten van de inhoud van aangeleverde documenten, zoals facturen en jaarrekeningen, ten behoeve van de controlewerkzaamheden;
- het uitvoeren van integriteits- en compliancecontroles op betrokken rechtspersonen en functionarissen, waaronder de verificatie of een bankrekeningnummer bij een opgegeven tenaamstelling hoort;
- het beheren van gebruikersaccounts, autorisaties en toegang tot de Dienst;
- het vastleggen van gebruik en verwerkingsstappen ten behoeve van beveiliging, foutopsporing en de controleerbaarheid van het dossier.

3. Categorieën betrokkenen

Categorie	Toelichting
Gebruikers van de Dienst	Medewerkers van Verwerkingsverantwoordelijke en van diens cliënten die op de Dienst inloggen.
Debiteuren en crediteuren	Klanten en leveranciers van de gecontroleerde entiteit, waaronder eenmanszaken en natuurlijke personen, en hun contactpersonen.
Tegenpartijen bij banktransacties	Personen en organisaties die voorkomen in de ingelezen bankafschriften.
Medewerkers van de gecontroleerde entiteit	Personen die boekingen hebben ingevoerd of geaccordeerd, en personen die voorkomen in loonstaatgegevens.
Bestuurders, functionarissen en uiteindelijk belanghebbenden	Natuurlijke personen die als functionaris van een rechtspersoon in het handelsregister of in de jaarrekening voorkomen.
Overige personen in vrije tekstvelden	Personen die incidenteel voorkomen in omschrijvingen van boekingen of in aangeleverde documenten.

4. Categorieën persoonsgegevens

Categorie	Gegevens
Accountgegevens	Voor-, tussen- en achternaam, e-mailadres, een onomkeerbare wachtwoordhash, toegewezen rol en toegangsbereik, instellingen en voorkeuren, aanmaak- en gebruiksmomenten van het account, acceptatie van de privacyverklaring en tokens voor wachtwoordherstel.
Relatiegegevens	Naam en handelsnaam, adresgegevens, telefoonnummer, e-mailadres, IBAN, btw-identificatienummer, KvK-nummer, kredietlimiet en betalingsgedrag van debiteuren en crediteuren.
Financiële transactiegegevens	Grootboekmutaties met omschrijving, factuurnummers en referenties, openstaande posten, en de code en naam van de medewerker die de boeking heeft ingevoerd.
Bankgegevens	Rekeningnummer, tenaamstelling en IBAN/BIC van de tegenpartij, transactiereferenties en de vrije omschrijving bij de mutatie.
Loongegevens	Uit de verzamelloonstaat: personeelsnummer, naam, geboortedatum, geslacht, functie, loonbedragen en ingehouden premies en heffingen.
Gegevens uit documenten	De inhoud van geüploade documenten zoals facturen, bankafschriften, contracten en jaarrekeningen, inclusief de daarin voorkomende persoonsgegevens.
Compliancegegevens	Naam, functie en geboortedatum van functionarissen van rechtspersonen, alsmede de uitkomsten van uitgevoerde screenings.
Koppelingsgegevens	Toegangs- en vernieuwingstokens en accountaanduidingen voor gekoppelde administratiesystemen.
Loggegevens	Tijdstip, gebruikersaanduiding en aard van uitgevoerde import-, analyse- en verwijderacties.

Bijzondere categorieën van persoonsgegevens worden niet doelbewust verwerkt. De Dienst kan wel loongegevens en geboortedata bevatten, voor zover deze deel uitmaken van de door Verwerkingsverantwoordelijke aangeleverde administratie. Verwerkingsverantwoordelijke bepaalt welke gegevens hij aanlevert.

5. Herkomst van de gegevens

Bron	Wijze van ontsluiten
Exact Online	Koppeling via de API van de leverancier, geautoriseerd door de gebruiker.
AFAS Profit	Koppeling via de API van de leverancier met een door de cliënt verstrekt toegangstoken.
Microsoft Dynamics 365 Business Central	Koppeling via de API van de leverancier, geautoriseerd via Microsoft Entra ID.
XML Auditfile Financieel (XAF)	Door de gebruiker aangeleverd bestand.
Bankafschriften (CAMT.053)	Door de gebruiker aangeleverd bestand.
Documenten	Door de gebruiker geüploade bestanden of documenten uit de gekoppelde documentopslag van Verwerkingsverantwoordelijke.
Openbare registers	Gegevens over rechtspersonen en functionarissen uit het handelsregister en uit openbare bronnen.

6. Bewaartermijnen

De gegevens van een administratie blijven beschikbaar zolang de betreffende opdracht in de Dienst actief is en Verwerkingsverantwoordelijke daarover wil beschikken. Verwerkingsverantwoordelijke kan de gegevens van een administratie op elk moment laten verwijderen; de Dienst voorziet in een gecontroleerde verwijderprocedure die zowel de opgeslagen gegevens als de bijbehorende documenten verwijdert. Na beëindiging van de Hoofdovereenkomst worden alle gegevens verwijderd overeenkomstig artikel 10. Back-ups worden volgens het geldende back-upschema bewaard en daarna overschreven. Loggegevens die nodig zijn voor beveiliging en

verantwoording worden niet langer bewaard dan daarvoor noodzakelijk is.

7. Plaats van verwerking

De Dienst draait op het Microsoft Azure-platform in de regio Zweden (Sweden Central). Opslag van gegevens en back-ups vindt plaats binnen de Europese Unie. Voor de geautomatiseerde analyse worden documenten aangeboden aan een AI-dienst die zich buiten de Europese Economische Ruimte kan bevinden; artikel 6 en Bijlage 3 beschrijven welke dat is en op welke grondslag die doorgifte berust. Voor de overige ingeschakelde subverwerkers geldt de in Bijlage 3 vermelde verwerkingsregio.

8. Contactgegevens

Voor alle aangelegenheden die deze Verwerkersovereenkomst betreffen, waaronder meldingen van een inbreuk in verband met persoonsgegevens, is Verwerker bereikbaar via **privacy@thenextstapp.nl**. Verwerker heeft geen functionaris voor gegevensbescherming aangesteld, omdat daartoe geen wettelijke verplichting bestaat; de privacycoördinator van Verwerker is op bovenstaand adres het vaste aanspreekpunt.

Bijlage 2 – Technische en organisatorische maatregelen

Verwerker treft ten minste de hieronder beschreven maatregelen als bedoeld in artikel 32 AVG. De indeling volgt de gebruikelijke categorieën van beheersmaatregelen.

1. Fysieke toegangsbeveiliging

De Dienst wordt volledig gehost in datacenters van Microsoft Azure. Verwerker heeft geen eigen serverruimte en beheert geen fysieke infrastructuur. De fysieke beveiliging van de datacenters, waaronder toegangscontrole, cameratoezicht, brandbeveiliging en klimaatbeheersing, wordt door Microsoft verzorgd en is onderworpen aan onafhankelijke certificering. Werkplekken van medewerkers van Verwerker zijn voorzien van schijfversleuteling en automatische vergrendeling.

2. Toegangsbeveiliging van systemen

Gebruikers loggen in met een persoonlijk account. Wachtwoorden worden niet in leesbare vorm opgeslagen, maar met een algoritme voor wachtwoordafleiding (PBKDF2-HMAC-SHA256, 100.000 iteraties, met een unieke willekeurige salt per gebruiker) versleuteld vastgelegd; de vergelijking gebeurt in constante tijd. Herstelverzoeken verlopen via een eenmalig, in versleutelde vorm opgeslagen en in de tijd beperkt token. Bij aanmelden met gebruikersnaam en wachtwoord geldt tweestapsverificatie: de aanmelding wordt bevestigd met een eenmalige, in de tijd beperkte verificatiecode die per e-mail wordt verzonden. Verwerkingsverantwoordelijke kan de Dienst koppelen aan de eigen Microsoft Entra ID-omgeving, zodat inloggen verloopt via het eigen identiteitsbeheer, inclusief meervoudige verificatie en centraal gebruikersbeheer. Toegang tot de beheeromgeving van de Dienst verloopt uitsluitend via beheerde identiteiten en meervoudige verificatie; er worden geen gedeelde beheeraccounts gebruikt.

3. Toegangsbeveiliging van gegevens

Autorisatie berust op een rollenmodel dat onderscheid maakt tussen beheerders, medewerkers van een accountantskantoor en gebruikers van een cliënt. Aan iedere rol is een afgebakend bereik van klanten, opdrachten en administraties verbonden, dat bij het benaderen van de Dienst wordt toegepast. Medewerkers van Verwerker krijgen uitsluitend toegang tot productiegegevens wanneer dat noodzakelijk is voor beheer of ondersteuning, op basis van het beginsel van minimale rechten.

4. Beheersing van verstrekking en transport

Al het verkeer met de Dienst verloopt uitsluitend over een versleutelde verbinding; onversleutelde verzoeken worden doorgeleid naar de beveiligde variant en de browser wordt door middel van een strikte transportbeveiligingsinstructie verplicht tot het gebruik daarvan. Verbindingen met de database en met externe koppelingen zijn eveneens versleuteld. Gegevens worden versleuteld opgeslagen. Toegangs- en vernieuwingstokens van gekoppelde administratiesystemen worden afgeschermd opgeslagen.

5. Invoer- en wijzigingscontrole

Import-, analyse-, afletter- en verwijderacties worden vastgelegd in logtabellen met vermelding van het tijdstip en de handelende gebruiker, zodat achteraf is vast te stellen wie welke bewerking heeft uitgevoerd. Verwerkingen die over meerdere stappen lopen zijn beveiligd met een exclusieve claim per administratie, waardoor gelijktijdige, conflicterende bewerkingen worden voorkomen en gegevens niet kunnen worden overschreven door een verlopen proces.

6. Opdracht- en leveranciersbeheer

Verwerker verwerkt uitsluitend op basis van de instructies van Verwerkingsverantwoordelijke. Met iedere subverwerker is een verwerkersovereenkomst gesloten met ten minste gelijkwaardige verplichtingen. Medewerkers en ingeschakelde derden zijn contractueel tot geheimhouding gebonden en worden geïnstrueerd over de omgang met vertrouwelijke gegevens. Wijzigingen aan de Dienst worden via een beheerde ontwikkelstraat doorgevoerd, met versiebeheer, gescheiden acceptatie- en productieomgevingen en geautomatiseerde uitrol; ontwikkelaars beschikken niet over vaste, permanente productiereferenties.

7. Beschikbaarheid en herstel

De databank wordt continu geback-upt, met de mogelijkheid tot herstel naar een willekeurig tijdstip binnen de korte-termijnbewaarperiode, aangevuld met langetermijnback-ups op week-, maand- en jaarbasis. Back-upopslag is zone-redundant en bestandsopslag wordt geografisch gerepliceerd naar een tweede EU-regio. Er is een uitgewerkt uitwijkscenario met een bijbehorend draaiboek, waarmee de omgeving in een andere regio binnen de Europese Unie kan worden opgebouwd. Het functioneren van de Dienst wordt gemonitord; storingen en mislukte verwerkingen leiden tot een automatische melding aan de beheerder.

8. Scheiding van gegevens

De Dienst is meergebruikers opgezet. Iedere klant, opdracht en administratie heeft een eigen aanduiding die in vrijwel iedere gegevenstabel is opgenomen en die bij elke bevraging en bewerking wordt meegegeven. Daardoor zijn de gegevens van verschillende klanten logisch van elkaar gescheiden. Acceptatie- en productieomgevingen zijn volledig van elkaar gescheiden; voor test- en ontwikkeldoeleinden worden geen productiegegevens gebruikt.

9. Geheimhouding en bewustwording

Alle personen die namens Verwerker toegang hebben tot Persoonsgegevens zijn gebonden aan een geheimhoudingsverplichting die ook na beëindiging van de samenwerking voortduurt. Verwerker besteedt structureel aandacht aan bewustwording op het gebied van informatiebeveiliging en gegevensbescherming.

10. Beveiliging van de ontwikkelketen

Afhankelijkheden van derden worden automatisch bewaakt op bekende kwetsbaarheden en tijdig bijgewerkt. Geheimen, sleutels en verbindingsgegevens van de productieomgeving worden centraal in een sleutelkluis en in het beveiligde geheimenbeheer van de ontwikkelomgeving bewaard. De uitrol naar de productieomgeving verloopt via kortlevende, op federatie gebaseerde autorisatie in plaats van vaste wachtwoorden.

Bijlage 3 – Overzicht van subverwerkers

Verwerker maakt bij het leveren van de Dienst gebruik van de onderstaande subverwerkers. Dit overzicht is actueel op de in de voettekst vermelde versiedatum; de meest actuele versie is opvraagbaar via privacy@thenextstapp.nl.

Subverwerker	Dienst en doel	Gegevens	Regio en doorgifte
Microsoft (Azure)	Hosting van de applicatie, databank, bestandsopslag, wachtrijen, sleutelbeheer en monitoring.	Alle in Bijlage 1 genoemde gegevens.	EU – Zweden (Sweden Central), met uitwijk in een gekoppelde EU-regio.
Anthropic	Geautomatiseerde analyse van documenten en werkbladen ter ondersteuning van de controle; de aangeleverde documenten worden ongewijzigd aangeboden.	Documentinhoud en werkbladen, inclusief de daarin voorkomende persoonsgegevens.	Verenigde Staten – modelcontractbepalingen; geen gebruik voor modeltraining.
Microsoft (Azure OpenAI)	Alternatieve aanbieder voor dezelfde analyse, inzetbaar in plaats van Anthropic.	Tekst uit aangeleverde documenten en werkbladen, waaronder namen van functionarissen.	EU
Microsoft (Azure AI Document Intelligence)	Herkennen en structureren van de inhoud van geüploade documenten, zoals facturen.	Documentinhoud, waaronder namen, adressen en bedragen.	EU
Microsoft (Microsoft 365 / Graph)	Verzenden van transactionele berichten en, indien gekoppeld, het benaderen van de documentopslag van Verwerkingsverantwoordelijke.	E-mailadres en naam van gebruikers; opgehaalde documenten.	EU
Microsoft (Entra ID)	Identiteitsverificatie voor gekoppelde aanmelding en voor koppelingen met administratiesystemen.	Aanmeldgegevens en accountaanduiding.	EU
Google (Vertex AI)	Ondersteuning bij online integriteits- en achtergrondonderzoek op basis van openbare bronnen.	Namen van rechtspersonen en functionarissen die worden onderzocht.	EU – Nederland (europe-west4)
SurePay B.V.	Controle of een bankrekeningnummer bij de opgegeven tenaamstelling hoort.	IBAN en tenaamstelling van de tegenpartij.	Nederland
Company.info B.V.	Raadplegen van handelsregister- en concernstructuurgegevens voor compliancecontroles.	Namen en functiegegevens van rechtspersonen en functionarissen.	Nederland

Toelichting: Microsoft, Google en Anthropic maken deel uit van een concern dat buiten de Europese Economische Ruimte is gevestigd. Bij Microsoft en Google vinden verwerking en opslag binnen de Europese Unie plaats; bij Anthropic vindt de verwerking in de Verenigde Staten plaats. Voor doorgifte naar en toegang vanuit een derde land gelden de door de Europese Commissie vastgestelde modelcontractbepalingen en aanvullende waarborgen. De aan Anthropic, Azure OpenAI en Vertex AI aangeboden gegevens worden niet gebruikt voor het trainen van modellen. Softwarecomponenten die uitsluitend binnen de omgeving van Verwerker draaien en waarbij geen gegevens naar de leverancier worden verzonden, zijn geen subverwerker en staan daarom niet in dit overzicht.