

**Bijlage 1 Diensten, gegevens en doelen**

1. Contactgegevens klant

Zoals vermeld in de klantomgeving van de software.

2. Verwerkingsactiviteit (Diensten):

Het leveren van boekhoudsoftware, alsmede, indien nodig en overeengekomen, de implementatie daarvan.

3. Doel(en): [IN TE VULLEN DOOR KLANT]

Het voeren van een boekhouding

4. Persoonsgegevens:

- NAW-gegevens
- Geslacht / aanhef
- Email adres
- BSN
- BTW-ID
- BTW-nummer
- Geboortedatum
- Startdatum bedrijf
- IBAN van bedrijf
- LH-nummer
- RSIN
- KVK
- Bedrijfsactiviteit
- Taal
- Fiscaal partner (Geboortedatum, BSN)
- Kinderen
- Oude JR
- Oude BTW aangiften
- Jaaroverzicht banken
- Gegevens andere bedrijven die je bezit, maar geen klant zijn
- Jaaropgaven
- Lening overzichten en gerelateerde documenten
- Vermogensdocumenten
- Bonus
- Alimentatie
- Lijfrente
- AOV
- Ziektekosten

- Giften
- Studiekosten
- Dividend
- Overige inkomsten
- Banktransacties

5. Locatie(s) gegevens:

Locatie	Doorgifte?	Passende waarborgen?
Nederland	Nee	Nvt

6. Bewaartermijn:

Duur van de overeenkomst en 6 maanden erna.

## Bijlage 2 Maatregelen

### *Organisatorische maatregelen*

- Geheimhoudingsverklaring: Al onze medewerkers hebben contractuele geheimhoudingsclausules in hun arbeidsovereenkomst. Ze zullen nooit zonder goede reden informatie met derden delen. Hetzelfde geldt voor alle tijdelijke/externe medewerkers van eventuele payroll dienstverleners.
- Integriteit: Medewerkers krijgen alleen toegang tot persoonsgegevens op een "need-to-know"-basis, waardoor de gebruikersautorisatie wordt beperkt tot specifieke taken en/of applicaties. Bepaalde medewerkers hebben toegang tot algemene contactgegevens (zoals telefoonnummer en e-mailadres), maar andere informatie (zoals HR gegevens et cetera) zijn alleen toegankelijk voor directie en de HR. Zie ook het toegangsbeperking document in de Privacy map.
- Fysieke maatregelen voor toegangsbeveiliging en toegangscontrole: Onze kantoren zijn adequaat beveiligd en de toegang tot de panden is beperkt en alleen toegankelijk met een gewone en magnetische sleutel.
- Dataminimalisatie: we verzamelen niet meer gegevens dan nodig is. Waar mogelijk zullen wij te allen tijde controleren of de gevraagde gegevens daadwerkelijk nodig zijn of kunnen worden verminderd.
- Opslagbeperking en archivering: Wij bewaren persoonsgegevens zo lang als nodig is voor het doel waarvoor wij de gegevens gebruiken en/of zolang de wet ons verplicht om gegevens te bewaren. Hoe lang dat precies is, verschilt per doel en functie van de persoonsgegevens. We zullen stappen ondernemen om dit zoveel mogelijk te automatiseren. In ons verwerkingsregister hebben wij per verwerking de retentietermijn opgenomen.
- Evaluatie van de maatregelen: Om te bepalen of de uitgevoerde maatregelen voldoende effectief zijn, worden jaarlijks controles uitgevoerd. Dit doen we onder meer door interne audits van de maatregelen uit te voeren. Beveiligingszwakheden komen ook aan het licht door logging en monitoring.

### *Technische maatregelen*

- Toegangsbeperking: Alle gegevens worden beschermd door wachtwoordbeveiliging van de verschillende applicaties. Bij beëindiging van het dienstverband wordt toegang tot de verschillende applicaties en gegevens direct gedeactiveerd.
- Vertrouwelijkheid: Alle werknemerslaptops zijn beveiligd met een wachtwoord. Laptops zijn voorzien van encryptie.
- Wachtwoorden: Alle medewerkers hebben een unieke gebruikersnaam en wachtwoord voor hun eigen accounts en software.
- Software-updates: We controleren regelmatig op updates van de gebruikte software-afhankelijkheden. Updates voor de administratiesoftware worden getest en, als ze geen risico vormen voor de dagelijkse bedrijfsvoering, geïmplementeerd in de productieomgeving.
- CMS: Ons CMS (back-office van de boekhouders) is een gesloten omgeving waar alleen medewerkers toegang toe hebben. Dit betekent dat alleen gebruikers met een geldige

gebruikersnaam en tweevoudige verificatie kunnen inloggen. Deze inloggegevens worden opgeslagen in een beveiligde omgeving.

- **Correctheid:** Om de juistheid en actualiteit van de gegevens te garanderen, wordt er regelmatig een controle uitgevoerd op de juistheid van de gegevens.

## Bijlage 3 (Sub-)verwerkers

Naam	Omschrijving dienst	Locatie data	Buiten EER? JA / NEE	Passende waarborgen?	Verwerkers overeenkomst? JA / NEE
AWS	Hosting van mediabestanden (foto's en bonnen)	Duitsland	Nee	Nvt	Ja
Backseat Surfer BV *	IT beheer en ontwikkeling	Nederland	Nee	Nvt	Ja
Exact	Belasting aangifte en opstellen jaarrekeningen	Europa	Nee	Nvt	Ja
Gsuite	Directe communicatie klanten	Europa	Nee	Nvt	Ja
Hubspot	Onderhouden klantrelatie	Duitsland	Nee	Nvt	Ja
Logius	Verzorgd digitale koppeling met belastingdienst	Nederland	Nee	Nvt	Ja
Mailgun	Systeem e-mails naar klanten, E-mails vanuit facturen en offerte modules	Europa / US	Ja	Ja	Ja
Open AI	Scannen inkomsten uitgaven voor autocomplete	Europa / US	Ja	Ja	Ja
Ponto	Uitlezen banktransacties	Europa	Nee	Nvt	Ja
TransIP	Hosting applicatie en database	Nederland	Nee	Nvt	Ja
Visma Nmbrs	Salarisverwerking	Nederland	Nee	Nvt	Ja

\* Backseat Surfer BV is net als Dienstverlener een 100% dochter van KeesdeBoekhouder BV.

#### **Bijlage 4 Datalekken**

In geval van een datalek zal dit formulier (zo veel mogelijke) door Just ingevuld verstrekt worden aan de klant.

##### *Gegevens over het datalek*

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest:

- Exacte datum waarop de inbreuk was:
- Startdatum van de periode waarbinnen de inbreuk was:
- Einddatum van de periode waarbinnen de inbreuk was:
- Wanneer werd de inbreuk ontdekt?
- Hoe werd de inbreuk ontdekt?
- Om welk type persoonsgegevens gaat het?

##### *Vervolgacties naar aanleiding van het datalek*

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

##### *Technische beschermingsmaatregelen*

Waren de persoonsgegevens op het moment van het ontdekken van het datalek versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?

Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, op welke manier is dit dan gebeurd?