KEES DE BOEKHOUDER

FOUNDERS

Appendix 1 Services, data and purposes

1. Client contact information

As stated in the client environment of the software.

2. Processing Activity (Services):

The provision of accounting software and, if necessary and agreed, the implementation thereof.

3. Object(s): [TO BE FILLED OUT BY THE CLIENT]

Keeping accounts

4. Personal Data:

- Name and address details
- Gender/salutation
- E-mail address
- Citizen service number
- VAT identification number
- VAT number
- Date of birth
- Starting date of the company
- IBAN of the company
- Withholding tax number
- Legal Entities and Partnerships Identification Number (RSIN)
- Ch. of Comm.
- Business activity
- Language
- Tax partner (Date of birth, citizen service number)
- Children
- Old financial statements
- Old VAT returns
- Annual bank statements
- Data of other companies you own but which are not clients
- Annual income statements
- Loan statements and related documents
- Documents relating to capital
- Bonus
- Spousal maintenance
- Annuity contract
- Invalidity insurance
- Medical expenses

- Gifts
- Study costs
- Dividends
- Other income
- Bank transactions

5. Location(s) details:

Location	Transfers?	Appropriate safeguards?
The Netherlands	No	N/A

6. Retention period:

Duration of the agreement and 6 months thereafter.

KEES DE BOEKHOUDER FOUNDERS

Appendix 2 Measures

Organisational measures

- Confidentiality Statement: All our employee contracts of employment include a confidentiality clause. They will never share any information with third parties without good reason. The same applies to all temporary/external employees working for any payroll service providers.
- Integrity : The employees will only have access to personal data on a "need-to-know" basis, as a result of which the user authorisation is limited to specific tasks and/or applications. Some employees will have access to general contact details (such as the telephone number and e-mail address) but other information (such as HR data etc.) will only be accessible to the management board and HR. See also the access restriction document in the Privacy folder.
- Physical measures for access security and access control : Our offices are adequately secured and the access to the building is limited and access is only possible by means of a key or magnetic key.
- Data minimisation: we do not collect more data than is necessary. In so far as possible, we will always check whether the data requested is actually required or whether the collection of data may be prevented.
- Storage limitation and archiving: We retain personal data for as long as this is necessary for the purpose for which we use your data and/or for as long as the law requires us to retain the data. How long this is, exactly, differs for each purpose and function of the personal data. We will take steps to automate this as much as possible. We have included the retention period per type of processing in our processing register.
- Evaluation of the measures: In order to determine whether the measures implemented are sufficiently effective, annual audits are performed. We do this, among other things, by performing internal audits of the measures. Security weaknesses are also revealed by logging and monitoring.

Technical measures

- Access restriction: All data are protected by password protection of the various applications. On termination of the employment access to the various applications and data is deactivated immediately.
- Confidentiality : All employee laptops are password-protected. Laptops are encrypted.
- Passwords: All employees have a unique user name and password for their own accounts and software.
- Software updates: We regularly check for updates of the software-dependencies used. Updates for the administration software are tested and, if they do not pose a risk to day-to-day business operations, they will be implemented in the production environment.
- CMS: Our CMS (accounting back office) is a closed environment that is accessible to employees only. This means that only users with a valid username and password can log into CMS. These login details are stored in a secure environment.
- Correctness: in order to guarantee the accuracy and up-to-date nature of the data, regular checks are carried out to make sure that the data are correct.

Appendix 3 (Sub)processors

Name	Description of services	Location data	Outside of EEA? YES / NO	Appropriate safeguards?	Processors Agreement? YES/ NO
AWS	Hosting of media files (photos and tickets)	Germany		N/A	Yes
Backseat Surfer BV *	IT management and development	Netherlands	No	N/A	Yes
Exact	Tax return and drawing up annual financial statements	Europe	No	N/A	Yes
Gsuite	Direct communication with clients	Europe	No	N/A	Yes
Hubspot	Maintaining the client relationship	Germany	No	N/A	Yes
Logius	Handles digital link with Tax and Customs Administration	Netherlands		N/A	Yes
Mailgun	System e-mail to clients, E-mails from invoices and quotation modules	Europe / US	Yes	Yes	Yes
Open AI	Scanning revenue and expenses for autocomplete	Europe / US	Yes	Yes	Yes
Ponto	Retrieve bank transactions	Europe	No	N/A	Yes
TransIP	Hosting application and database	Netherlands	No	N/A	Yes
Visma Nmbrs	Payroll processing	Netherlands	No	N/A	Yes

* Backseat Surfer BV is, as is Service Provider, a 100% subsidiary of KeesdeBoekhouder BV.

Appendix 4 Data Breaches

If a data breach is discovered, this form, that has been filled in by Just (to the extent possible), will be provided to the client.

Information about the data breach

Summarise the incident in which a personal data security breach occurred:

- Exact date on which the breach occurred:
- Starting date of the period in which the breach occurred:
- End date of the period in which the breach took occurred:
- When was the breach discovered?
- How was the breach discovered?
- What type of personal data is involved?

Follow-up actions in response to the data breach

What technical and organisational measures has your organisation taken to address the breach and prevent further breaches?

Technical protective measures

Were the personal data encrypted, hashed or otherwise unintelligible or inaccessible to unauthorised persons at the time the data breach was discovered?

If the personal data were rendered wholly or partially unintelligible or inaccessible, how was this done?