

PROCESSOR CONTRACT

(UNILATERAL)

1. General

The following terms as used in this processor contract shall have the definitions provided here:

- 1.1 **General Terms and Conditions:** the Processor's General Terms and Conditions that apply in full to all contracts between the Processor and the Controller and which General Terms and Conditions shall constitute an integral part of this processor contract.
- 1.2 **Processor:** the limited liability companies of Visser & Visser (Accountants and Consultants), having their registered office and principal place of business at Bijdorp Oost 60 in Barendrecht, the Netherlands, and all entities affiliated with Visser & Visser Accountants and Consultants, including without limitation Accountants, Tax advisers, Payroll and Advice, Services, Consultancy & Interim.
- 1.3 **Data:** the personal data as described in Annex 1.
- 1.4 **Client:** the natural person or legal entity who or that has instructed the Processor to carry out Activities, also the 'Controller'.
- 1.5 **Contract:** any agreement between the Client and the Processor for the performance of Activities by the Processor for the Client, as stipulated in the order confirmation.
- 1.6 **Controller:** the Client who, as a natural person or legal entity, has instructed the Processor to carry out Activities.
- 1.7 **Activities:** all activities for which instructions have been given, or any other activities that the Processor performs. The above shall apply in the broadest sense possible and shall at least comprise the activities stipulated in the order confirmation.

2. Applicability of the processor contract

- 2.1 This processor contract applies to all data that is collected by the Processor for the Client for the purpose of the implementation of the contract with the Client and to all activities that result from the contract for the Processor and the data to be collected for such purpose.
- 2.2 The Controller shall be responsible for the processing of the data concerning certain categories of data subjects, as described in Annex 1.
- 2.3 When performing the contract, the Processor will process certain personal data for the Controller.
- 2.4 This is a processor contract within the meaning of article 28(3) of the General Data Protection Regulation (GDPR), in which the rights and obligations as regards the processing of the personal data have been laid down in writing, including as regards security. This processor contract is binding on the Processor in respect of the Controller.
- 2.5 Just like the Processor's General Terms and Conditions, this processor contract forms part of the Contract and of all future contracts between the parties.

3. Scope of the processor contract

- 3.1 By giving instructions for the performance of Activities, the Controller has instructed the Processor to process the data on behalf of the Controller in the manner described in Annex 1 in accordance with the provisions of this processor contract.
- 3.2 The Processor shall process the data exclusively in accordance with this processor contract, particularly the provisions of Annex 1. The Processor confirms that it will not process the data for any other purposes.

- 3.3 Control over the data will never vest with the Processor.
- 3.4 The Controller can give additional instructions in writing to the Processor due to modifications or changes to the applicable regulations on the protection of personal data.
- 3.5 The Processor shall process the data only in the European Economic Area.

4. Secrecy

- 4.1 The Processor and any persons employed by, or carrying out activities for, the Processor, to the extent that such persons have access to personal data, shall only process the data on instructions from the Controller, except for any statutory obligations to the contrary.
- 4.2 The Processor and any persons employed by, or carrying out activities for, the Processor, to the extent that such persons have access to personal data, shall be under the obligation to keep secret any personal data that comes to their knowledge, except if any legal requirement obliges them to communicate the information or if the need to communicate the information results from a task.

5. No further disclosure

- 5.1 The Processor will not share the data or disclose it to third parties, unless after the Processor has obtained the Controller's prior consent or instruction for this in writing, or is obliged to do so pursuant to mandatory regulations. If mandatory regulations oblige the Processor to share the data or disclose it to third parties, the Processor will inform the Controller accordingly in writing, except if this is not allowed.

6. Security measures

- 6.1 Taking into account the current state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of persons, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The security measures that have now been taken have been defined in Annex 2.
- 6.2 The Processor shall ensure that measures are taken that also aim to avoid any unnecessary collecting and further processing of personal data.
- 6.3 The data is stored and processed exclusively within the European Economic Area.

7. Supervision of compliance

- 7.1 The Processor shall give the Controller, at the latter's request and for the latter's account, information about the processing of the data by the Processor or by Sub-Processors. The Processor shall give the requested information as soon as possible, but no later than within five working days.
- 7.2 The Controller shall have the right - once a year and for its own account - to have an inspection carried out by an independent third party to be appointed by the Controller and the Processor jointly in order to verify that the Processor complies with the obligations pursuant to the GDPR and this processor contract. The Processor shall fully cooperate in this to the extent that this is reasonably required. The Processor shall have the right to charge its costs associated with the inspection to the Controller.
- 7.3 For the purpose of its obligation pursuant to paragraph 1 of this article, the Processor will - as a minimum - provide the Controller or a third party hired for this purpose by the Controller with:

- 7.3.1 all the relevant information and documents;
- 7.3.2 access to all relevant buildings, information systems and data.

7.4 The Controller and the Processor will consult with each other to discuss any risks and shortcomings as soon as possible upon the report having been finished. The Processor will implement measures, the costs of which will be borne by the Controller, in order to bring the risks and shortcomings found to a level that is acceptable for the Controller and/or remove them, unless the parties have agreed differently in writing.

8. Data leak

- 8.1 If an incident or data leak that concerns or may concern the data comes to the Processor's attention, the Processor will immediately inform the Controller accordingly, using the Controller's contact details that are known to the Processor, and the Processor will provide information about: the nature of the incident or the data leak, the data affected, the consequences for the data of the incident or data leak found or expected, and the measures that the Processor has implemented and will implement.
- 8.2 The Processor will support the Controller as regards reporting to data subjects and/or to authorities.

9. Sub-processors

- 9.1 If the Processor has received previous (general) consent to outsource its obligations to third parties, the Processor will inform the Controller about its intention to engage a sub-processor. The Processor will grant the Controller a period of 7 working days within which to object to the sub-processor being engaged. The Processor will not engage the sub-processor until after the 7-day period has expired without the Controller having objected, or if the Controller has indicated that it does not object to the sub-processor being engaged.
- 9.2 If the Processor does not have prior consent to outsource its obligations to third parties, the Processor will ask prior consent for engaging the sub-processor.
- 9.3 The Processor will ensure that the sub-processor is subject to this processor contract or to a sub-processor contract that contains the same obligations as this processor contract.

10. Data subjects' cooperation obligations and rights

- 10.1 At its request, the Processor will cooperate with the Controller in the event of a complaint, question or request of a data subject, or in the event of studies or inspections by the Dutch data protection authority (Autoriteit Persoonsgegevens).
- 10.2 The Processor will assist the Controller at its request and for its account when the latter carries out a data protection impact assessment.
- 10.3 If the Processor receives a request for access, correction or removal of a data subject's data directly from such data subject, the Processor will inform the Controller of the fact that such request has been received within two working days. The Processor will carry out all the instructions given to the Processor by the Controller in writing as a consequence of such request from the data subject. The Processor will implement the

necessary appropriate technical and organisational measures that are needed to comply with such instructions from the Controller.

- 10.4 If instructions from the Controller to the Processor conflict with any statutory provisions regarding data protection, the Processor will report this to the Controller.

11. Term and termination

- 11.1 This processor contract shall be valid for as long as the Processor is tasked with processing data for the Controller pursuant to the contract between the Controller and the Processor. This processor contract will apply to the relationship between the Processor and the Controller for as long as the Processor carries out Activities on behalf of the Controller.
- 11.2 If, upon the termination of the contract, the Processor has to keep certain data and/or documents, computer disks or other data carriers with data on or in them, for a statutory period pursuant to a statutory obligation to keep such items, the Processor will ensure that this data or these documents, computer disks or other data carriers are destroyed within 4 weeks of the statutory obligation to keep them having expired.
- 11.3 If the contract between the Controller and the Processor has ended, the Controller can request the Processor within two months of the contract ending that all documents, computer disks and other data carriers with data in or on them be returned to the Controller, for the Controller's account. If such items are returned, the Processor will provide the data in the form in which it is present at the Processor's. To the extent that the data is located in a computer system or has any other form which prevents the reasonable provision of the data in such form to the Controller, the Processor will provide the Controller with an accessible, legible copy of the data. Upon this term having elapsed, the Processor will permanently destroy the data, unless any statutory obligation requires the Processor to store data.
- 11.4 Without prejudice to the other stipulations of this article 12, the Processor will not keep or use any data upon the contract having ended.
- 11.5 How to destroy the data will be established in conjunction with the Controller. When the data has been destroyed, the Processor will confirm this in writing to the Controller.
- 11.6 Without prejudice to the other stipulations of this article 12, the Processor will not keep or use any data upon the contract having ended.

12. Invalidity

- 12.1 If one or several provisions in this processor contract are null and void or are nullified, this will be without prejudice to the other provisions. If any provision in this processor contract is legally ineffective, the parties will negotiate about the content of a new provision that is as close a representation of the content of the original provision as possible.

13. Applicable law and competent court

- 13.1 This processor contract is governed by Dutch law.
- 13.2 Any disputes in connection with the processor contract or its performance shall be adjudicated by the competent court in Rotterdam, the Netherlands.

ANNEX 1 DATA, PURPOSES AND CATEGORIES OF DATA SUBJECTS

DATA

The Controller will have the Processor process the following data for the purpose of the assignment, which data may include, without limitation, personnel records, wage records, financial reports:

- (1) Name (initials, last name)
- (2) Telephone number
- (3) Email address
- (4) Date of birth
- (5) Residence
- (6) Details of ID (in connection with the Dutch Money Laundering and Terrorist Financing (Prevention) Act (Wwft in Dutch))
- (7) Financial details, both business and private
- (8) Name and address details and the citizen's service number (Dutch BSN) of the Controller's personnel

PURPOSES

The activities for which the processing of the above data is allowed - only if necessary - shall as a minimum include:

- (1) the activities, to be considered as primary service provision, tasked to the Processor by the Controller;
- (2) the maintenance, including updates and releases of the system made available to the Controller by the Processor or the sub-processor;
- (3) the data and technical management, also by a sub-processor;
- (4) the hosting, also by a sub-processor.

CATEGORIES OF DATA SUBJECTS

The data that is processed concerns the following categories of data subjects:

- (1) Customers
- (2) Employees of customers
- (3) Possible customers

<p style="text-align: center;">ANNEX 2 SECURITY MEASURES</p>
--

SECURITY MEASURES

The Processor has at least taken the following security measures:

- Back-up and recovery procedures
- Security of network connections (both managed internally and externally)
- Authorities have been assigned to a limited number of people, based on their positions, who are responsible for implementing the processing (including periodic checks thereof)
- Encryption of personal data during electronic transfer (system-to-system links) to external parties
- Security policy
- Code of conduct
- Confidentiality clauses in employment contracts
- Intruder alarm
- Logical access control by means of passwords and/or personal access codes
- Sub-processor contracts with third parties
- Safe method to store data files within the office network