Processing agreement
Countus Groep B.V.

Countus
Groep B.V.

1   General

Due to translation differences no rights can be derived from this English translation of the Processing Agreement. The original Dutch version of the Processing Agreement always takes precedence over this English translation.

In this processing agreement the following definitions apply:
1.   General Terms and Conditions: the General Terms and Conditions of the Processor, which apply in full to every agreement between the Processor and the Processing Controller and of which General Terms and Conditions this Processing Agreement forms an inseparable part.
2.   Processor: the private company Countus Groep B.V., with its registered office and with its principal place of business at Dokter Stolteweg 2, 8025 AV Zwolle and all entities affiliated with Countus Groep B.V.
3.   Data: the personal data as described in Appendix 1.
4.   Client: the natural person or legal entity who has given the Processor an order to perform Activities, as well as the Processing Controller.
5.   Agreement: any agreement between the Client and the Processor for the performance of Activities by the Processor on behalf of the Client, in accordance with the provisions in the order confirmation.
6.   Processing Controller: the Client who, as a natural person or legal entity, has given the Processor an order to perform Activities and whereby Data from the Client is processed.
7.   Activities: all activities stated in the order confirmation and where the Processing Controller processes personal data in accordance with the instructions of the Processor.

2   Applicability of the Processing Agreement

1.   This processing agreement applies to all data collected by the Processor for the Client in the context of carrying out of the Agreement with the Client, as well as to all Activities arising from the Agreement for the Processor and the data to be collected in that context.
2.   The Processing Controller is responsible for the processing of the Data regarding certain categories of data subjects, as described in Appendix 1.
3.   When carrying out the Agreement, the Processor shall only processes those personal data for the Processing Controller for the purposes indicated by the Processing Controller.
4.   This is a processing agreement within the meaning of Article 28 (3) of the Dutch AVG–regulation 'Algemene Verordening Gegevensbescherming', in which the rights and obligations with regard to the processing of personal data are regulated in writing, including with respect to security. This processing agreement is binding on the Processor with respect to the Processing Controller.
5.   Just like the General Terms and Conditions of the Processor, this processing agreement, forms part of the Agreement and all future agreements between the parties.

3 Processing agreement scope

1. By giving the order to perform Activities, the Processing Controller has instructed the Processor to process the Data on behalf of the Processing Controller in the manner described in Appendix 1 in accordance with the provisions of this processing agreement.
2. The Processor processes the Data exclusively in accordance with this processing agreement, in particular with what is contained in Appendix 1. The Processor confirms that it will not process the Data for other purposes.
3. Control over the Data never rests with the Processor.
4. The Processing Controller may provide additional written instructions to the Processor because of adjustments or changes in the applicable regulations in the field of personal data protection.
5. The Processor shall only process the Data in the European Economic Area.

4 Confidentiality

1. The Processor and the persons who are employed by the Processor or who perform work for it, insofar as these persons have access to personal data, only process the Data on instructions from the Processing Controller, save for divergent legal obligations.
2. The Processor and the persons who are employed by the Processor or who perform work for it, insofar as these persons have access to personal data, are obliged to maintain the confidentiality of the personal data of which they take note, except to the extent that any legal provision obliges them to notify or the need for notification arises from a task.

5 No further provision

1. The Processor will not share or provide the data to third parties, unless the Processor has obtained prior written permission or an order to that effect from the Processing Controller or is obliged to do so based on mandatory regulations. If the Processor is obliged to share the Data with or provide it to third parties on the basis of mandatory regulations, the Processor will inform the Processing Controller of this in writing, unless this is not permitted.

6 Security measures

1. Taking into account the state of the technology, the implementation costs, as well as the nature, the extent, the context and the processing objectives and the risks to the rights and freedoms of individuals that vary in likelihood and severity, the Processor shall take appropriate technical and organisational measures to ensure a level of security tailored to the risk. The security measures that have currently been taken are specified in Appendix 2.
2. The Processor shall ensure measures that are aimed amongst other things at preventing unnecessary collection and further processing of personal data.
3. The Data is stored and processed exclusively within the European Economic Area.

7 Compliance monitoring

1. The Processor will provide the Processing Controller at its request and at its expense with information about the Processing of the Data by the Processor or Sub-processors. The Processor will provide the requested information as quickly as possible, but within five working days at the latest.

2. Once a year and at its own expense, the Processing Controller has the right to have an independent third party jointly appointed by the Processing Controller and the Processor carry out an inspection to verify whether the Processor complies with the obligations under the the Dutch AVG-regulation 'Algemene Verordening Gegevensbescherming' and this processing agreement. The Processor will provide all reasonably necessary cooperation for this. The Processor has the right to charge its costs associated with the inspection to the Processing Controller.

3. To the Processing Controller or a third party engaged by the Processing Controller, the Processor will in every case, in the context of its obligation under paragraph 1 of this Article:

   3.1 provide all relevant information and documents;

   3.2 grant access to all relevant buildings, information systems and Data.

4. The Processing Controller and Processor will consult with each other as soon as possible after the report is completed to address any risks and shortcomings. The Processor will take measures at the expense of the Processing Controller to bring or eliminate the identified risks and shortcomings to a level acceptable to the Controller, unless the parties have agreed otherwise in writing.

5. The liability of the Processor arising from or relating to the Agreement and this Processing Agreement is governed by (the latest version of) the applicable General Terms and Conditions.

8 Data breach

1. As soon as possible after the Processor becomes aware of an incident or data breach that (among other things) relates or may relate to the Data, the Processor shall inform the Processing Controller of this via the contact details of the Processing Controller known to the Processor and the Processor will provide information about: the nature of the incident or data breach, the affected Data, the consequences of the incident or data breach established and expected on the Data and the measures that the Processor has taken and will take.

2. The Processor will support the Processing Controller with notifications to data subjects and/or authorities.

9 Inschakeling van subverwerkers

1. To the extent necessary, the Processing Controller hereby gives the Processor permission to use Sub-processors under the express condition that the Processor imposes on these Sub-processors at least the obligations that apply in this Processing Agreement between the Processing Controller and the Processor.

2. The Processor remains liable to the Processing Controller at all times for the processing of the Data by sub-processors engaged by it.

3. At the request of the Processing Controller, the Processor shall provide within four weeks an overview of the sub-processors engaged in the processing of the Processing Controller's Data.

4. The Processing Controller has the right to object to the use of a sub-processor within four weeks. The Processing Controller and the Processor will consult with each other if the Processing Controller objects to one of the sub-processors.

10 Obligations to cooperate and rights of the data subjects

1. The Processor will cooperate with the Processing Controller upon request in the event of a complaint, question or request from a data subject, or investigations or inspections by the Dutch Data Protection Authority.

2. The Processor will assist the Processing Controller at its request and at its expense in carrying out a data protection impact assessment.

3. If the Processor receives a request directly from a data subject for access, correction or deletion of his or her Data, the Processor will inform the Processing Controller within two working days of the receipt of the request. The Processor will carry out all instructions that the Processing Controller gives to the Processor in writing as a result of such a request from the data subject as quickly as possible. The Processor will take the necessary appropriate technical and organisational measures required to comply with such instructions from the Processing Controller.

4. If instructions from the Processing Controller to the Processor conflict with any legal provisions regarding data protection, the Processor shall report this to the Processing Controller.

11 Duration and termination

1. This processing agreement is valid as long as the Processor has an order from the Processing Controller to process Data in accordance with the instructions of the Processing Controller on the basis of the Agreement between the Processing Controller and the Processor.

2. If, after termination of the Agreement, the Processor must retain certain data and/or documents, computer disks or other data carriers on or in which Data is contained for a legal period of time on the basis of a legal retention obligation, the Processor will ensure the destruction of these data or documents, computer disks or other data carriers within 4 weeks after termination of the legal retention obligation.

3. Upon termination of the Agreement between the Processing Controller and the Processor, the Processing Controller may, within two months after termination of the Agreement, request the Processor to return all documents, computer disks and other data carriers on which or in which data are contained, to the Processing Controller, for the account of the Processing Controller. In the event of return, the Processor will provide the data in the form available to the Processor. To the extent that the Data is in a computer system or in another form as a result of which the Data cannot reasonably be provided to the Processing Controller, the Processor will provide the Processing Controller with an accessible, legible copy of the Data. After this period has expired, the Processor will proceed to permanently destroy the Data, unless the Processor is obliged to store Data on the basis of a legal obligation.

4. Without prejudice to the other provisions of this Article 12, the Processor will not process any Data after termination of the Agreement.

5. The method of destruction is determined in consultation with the Processing Controller. After destruction, the Processor will provide written confirmation thereof to the Processing Controller.

12 Nullity

1. If one or more provisions of this processing agreement are null or annulled, the remaining conditions remain fully applicable. If any provision of this processing agreement is not legally valid, the parties

shall mutually negotiate about the content of a new provision, which provision shall approximate the content of the original provision as closely as possible.

13 Governing law and choice of forum

1. Dutch law applies to this processing agreement.
2. All disputes in connection with the processing agreement or its implementation will be submitted to the competent court in the District of Overijssel.

Countus
Groep B.V.

Data

The Processing Controller allows the Processor to process the following Data by the Processor in the context of the order, including, but not limited to, personnel administration, payroll administration, provision of financial services:

1. Name (initials, first name and last name)
2. Telephone numbers (landline and mobile)
3. Email address
4. Date of birth/place of birth
5. Address/Place of residence
6. Details of proof of identity (in connection with the Money Laundering and Terrorist Financing (Prevention) Act, or Wwft)
7. Financial data, both business and private
8. BSN of the data subject
9. Data for incapacity for work notifications

Purposes

The activities for which the abovementioned Data may be processed, only if necessary, are in any case:

1. The activities, to be regarded as the primary service, in the context of which the Processing Controller has issued an order to the Processor;
2. Maintenance, including updates and releases of the system made available by the Processor or sub-processor to the Processing Controller;
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 are processed regarding the following categories of data subjects:

1. Employees of the Processing Controller, as well as interns, temporary workers, seconded workers and other persons of equivalent status;
2. Suppliers and customers of the Processing Controller;
3. Partner, children and other resident family members of the Processing Controller.

Countus
Groep B.V.

Security measures

The Processor has in any case taken the following security measures:

1. Logical access control by means of personal user ID and password;
2. This access control also determines which employees are granted access to which applications;
3. Encryption and secure transmission of personal data during electronic transfer to external parties;
4. Continuous attention is paid to privacy awareness;
5. Sub-processing agreements are/have been concluded with third parties;
6. Recovery procedures are tested irregularly;
7. Employment contracts have a confidentiality clause;
8. The security at data centre level is continuously monitored;
9. An implemented code of conduct is in force.