memocom

Processing agreement

This Processor Agreement applies to all forms of processing of personal data that Memocom and its partners (hereinafter referred to as "Processor") performs for the benefit of a counterparty to whom it provides services, the client (hereafter referred to as "Processing Officer"). This processor agreement forms an integral part of the agreements between the Parties as agreed in the Agreement (hereinafter referred to as the "Agreement") between the two parties.

Article 1. Purposes of processing

1.1 The Processer undertakes to process on the instructions of Processing Contractor responsible personal data under the conditions of this Processor Agreement. Processing will only take place within the framework as agreed in the Agreement, plus those purposes that are reasonably related thereto or that are determined with further consent.
1.2 The personal data processed by the Processor in the context of the activities as referred to in the previous paragraph and the categories of the data subjects from whom they originate are included in Appendix 1.
1.3 The Processer will not process the personal data for any other purpose than as determined by the Processing Officer. Processing Manager will inform the Processer of the processing purposes in so far as these have not already been mentioned in this Processor Agreement.
1.4 The personal data to be processed by the Processing Officer remains the property of the Processing Officer and / or the relevant parties involved.

Article 2. Obligations of the Processor

2.1 With regard to the processing operations referred to in article 1, Processor shall ensure compliance with applicable laws and regulations, including in any case the laws and regulations relating to the protection of personal data, such as the General Data Protection Regulation.
2.2 The Processing Party will inform the Processing Officer, on his first request, of the measures it has taken with regard to its obligations under this Processor Agreement.
2.3 The obligations of the Processor arising from this Processor Agreement also apply to those who process personal data under the authority of the Processor, including but not limited to employees, in the broadest sense of the word.
2.4 The Processer shall immediately inform the Processing Officer if in his opinion an instruction by the Processing Officer is in conflict with the legislation referred to in paragraph 1.
2.5 The processor will, in so far as this is within its power, provide reasonable assistance to the Processing Officer for the performance of data protection effect assessments (PIAs). The time spent on this will be charged to Verwerkinger by the Processing Officer.

Article 3. Transfer of personal data

3.1 The processor may process the personal data in countries within the European Union. Transfers to countries outside the European Union are not permitted, unless Processing Officer gives permission for this.

Article 4. Distribution of responsibility

4.1 The authorized processing operations will be carried out by Verwerker employees within an automated environment.
4.2 The processor is solely responsible for the processing of the personal details under this Processor Agreement, in accordance with the instructions of the Processing Officer and under the explicit (final) responsibility of the Processing Officer. For the other processing of personal data, including in any case, but not limited to, the collection of the personal data by the Processing Officer, processing for purposes not reported by the Processing Officer to the Processor, processing by third parties and / or for other purposes, Processor expressly not responsible.
4.3 Processing Manager guarantees that the content, use and instructions for the processing of the personal data as referred to in this processor's agreement are not unlawful and do not infringe any right of third parties.

Article 5. Engaging third parties or subcontractors

5.1 The processor may use third parties in the context of this processor agreement and will supply a list of third parties (sub-processors) to the accountability manager on request.
5.2 The processor will in any case ensure that these third parties take on at least the same obligations in writing as agreed between the Process Manager and the Processor.
5.3 The processor guarantees correct compliance with the obligations arising from this Processing Agreement by these third parties and in the event of errors of these third parties is itself liable for all damage as if it itself committed the error (s).Deze Verwerkersovereenkomst is van toepassing op alle vormen van verwerking van persoonsgegevens die Memocom en haar partners (hierna genoemd als “Verwerker”), uitvoert ten behoeve van een wederpartij aan wie zij diensten levert, de opdrachtgever (hierna genoemd als “Verwerkingsverantwoordelijke”). Deze verwerkersovereenkomst maakt integraal onderdeel uit van de afspraken tussen Partijen zoals overeengekomen in de Overeenkomst (hierna genoemd als “Overeenkomst”) tussen beide partijen.

Article 6. Security

6.1 The processor will endeavor to take sufficient technical and organizational measures with regard to the processing of personal data, against loss or against any form of unlawful processing (such as unauthorized inspection, violation, modification or provision of the personal data).
6.2 The processor has in any case taken the measures referred to in the Security Protocol which is attached to this Processor Agreement as an appendix. The processor may unilaterally change the Security Protocol at any time. She will inform the Processing Officer of adjustments.
6.3 The processor does not guarantee that the security is effective under all circumstances. If an explicitly described security is missing in the Processor Agreement, Verwerker will endeavor to ensure that the security meets a level that, in view of the state of the art, the sensitivity of the personal data and the costs associated with securing security, is not unreasonable. is.
6.4 Processing Party only makes personal data available to Processer for processing, if it has ensured that the required security measures have been taken. Processing Manager is responsible for compliance with the measures agreed by the Parties.
6.5 Most hosting parties of processor work in accordance with ISO 27001 / ISO 27002 and ISO 9001, which are considered to comply with the security requirements in view of the state of the art.

Article 7. Reporting obligation 1.

7.1 The reprocessor is at all times responsible for reporting a vulnerability and / or data leak (which means: a breach of the security of personal data that leads to a chance of adverse consequences, or has adverse consequences, for the protection of personal data.) to the supervisor and / or parties involved. In order to enable Processing Officer to comply with this statutory obligation, Verwerker informs the Processing Officer of the vulnerability and / or the data leak within 48 hours after the leak has become known to him.
7.2 A report must always be made, but only if the event actually occurred.
7.3 The obligation to report in any case includes reporting the fact that a leak has occurred. In addition, the obligation to report includes:
• the nature of the personal data breach, where possible with reference to the categories of data subjects and personal data registers concerned and, approximately, the number of data subjects and personal data registers concerned;
• the name and contact details of the data protection officer or any other contact point where more information can be obtained;
• the likely impact of the personal data breach;
• the measures proposed or taken by the Processor to address the personal data breach, including, where appropriate, measures to mitigate any adverse effects.

Article 8. Handling requests from data subjects

8.1 In the event that a data subject submits a request for the execution of his / her legal rights to the Processor, the Processor will forward the request to the Processing Officer, and the Processing Officer will further process the request. The processor may inform the data subject of this.

Article 9. Confidentiality and confidentiality

9.1 In the context of confidentiality and confidentiality, reference is made to the General Terms and Conditions of Memocom Article 5 and 6.

Article 10. Audit

10.1 The Processer hereby gives the Processing Officer the right to have an audit carried out by an independent third party who is bound to confidentiality in order to check compliance with the provisions in this Processor Agreement or the Processor shall provide the Processing Officer with a third party notification, which can be used to that the Processor acts in accordance with the provisions of this Processor Agreement. The aforementioned in the opinion of the Processor. 10.2 This audit may take place once a year as well as with a concrete suspicion of abuse of personal data.
10.3 The processor shall cooperate with the audit and provide all relevant information reasonably relevant to the audit, including supporting data such as system logs, and employees as timely as possible.
10.4 The findings resulting from the audit carried out will be assessed by the Processor and may, at the discretion of the Processor and in the manner as the Processor itself determines, be implemented by the Processor.
10.5. The costs of the audit are borne by the Processing Officer.

Article 11. Liability

11.1 In the context of liability, reference is made to our General Terms and Conditions, with the following additional paragraphs:
11.2 The liability of the Processor for indirect damage is excluded. Indirect damage is understood to mean all damage that is not direct damage and therefore in any case, but not limited to, consequential loss, lost profit, missed savings, reduced goodwill, loss due to business stagnation, damage due to non-determination of marketing objectives, damage related to the use of data or data files prescribed by the Processing Officer, or loss, mutilation or destruction of data or data files.
11.3 The exclusions and limitations referred to in this article shall lapse if and insofar as the damage is the result of intent or willful recklessness on the part of the Processor management.

Article 12. Duration and termination

12.1 This Processor Agreement is concluded by signing the Parties of the Agreement and starts on the date of the last signature.
12.2 This Processor Agreement has been entered into for the duration as stipulated in the Agreement between the Parties and in the absence thereof at least for the duration of the cooperation.
12.3 As soon as the Processor Agreement has been terminated, for whatever reason and in whatever way, then, at the choice of the Processing Party, the Processor will return all personal data that are present to it in the original or copy form to the Processing Officer and / or this personal data and any remove and / or destroy copies thereof. The aforementioned with the exception of the personal data of which the Processor must keep these in order to fulfill the statutory (storage) obligations.
12.4 The Processor is entitled to revise this Processing Agreement from time to time. It will notify the Processing Controller changes at least three months in advance. The contracting party may cancel at the end of these three months if they can not accept the changes. Otherwise, the changes are deemed to have been approved by the Processing Officer.

Article 13. Applicable law and dispute resolution

13.1 The Processor Agreement and its implementation are governed by Dutch law.
13.2 All disputes that may arise between the Parties in connection with the Processor Agreement shall be submitted to the competent court for the district in which the Processor is established.

Article 14. Other provisions

14.1 This AVG Processor Agreement is drawn up on the basis of the DHPA (Dutch Hosting Provider Association) Processor Agreement and is an addendum to current agreements.
14.2 In the event of conflicts between different documents or their annexes, the following order of priority applies:

- the agreement;
- the processor agreement;
- the terms and conditions;
- any additional conditions.

Appendix 1: Specification of personal data and data subjects

The Processor does not check on customer environments or in copies made thereof which (personal) data are processed. For this reason, the Processor assumes by default that they are processors of the category of standard personal data (such as name, address, etc.) and have implemented the standard control measures for this. If the Processing Officer includes the category of special personal data (such as citizen service number, race / ethnic origin, health data, belief / belief, "deviant" nature, political preference / opinion, sexual orientation / behavior, trade union membership, legal data, genetic / biometric data) processed by the Processor and specifying specific control measures, this must be reported specifically to the Processor by the controller. The Processing Officer must submit the category of special personal data with any specific control measures and the name of Data Protection Officer (FG) in a "Register of personal data" that meets the requirements set in the General Data Protection Regulation (AVG). The Processing Manager is also responsible for keeping the supplied 'Register personal details' up-to-date. If the Processor receives no "register of personal details" with (optional) additional control measures from the Processing Officer, it can be assumed that no or standard personal data is processed and the standard control measures are sufficient for the purpose of the Agreement. The Packaging Manager guarantees that the categories of data subjects described in this Appendix 1 are complete and correct, and indemnifies the Processor against any defects and claims that result from an incorrect representation by the Processing Officer.

Appendix 2: Security protocol (standard control measures)

The purpose of the security protocol is to inform about the organizational, technical and ISO 27001 measures taken by Memocom or its partners and to ensure the security of personal data. The measures are described in general terms, as a specific description of the measures can be a major risk for the protection of the measures.

Organizational measures:

Some organizational measures taken by the Processor and / or its hosting party are:

- work according to ISO 27001 - Information management system;
- awareness of employees;
- training of employees;
- knowledge and competence of employees;
- procedures and instructions.

Technical measures:

Some technical measures taken by the Processor are:

- physical security of rooms;
- digital security of systems and applications;
- hardware and software measures;
- update measures;
- virus scans;
- firewalls;
- logging measures;
- password management;
- authorization;
- encryption;
- etc.

ISO 27001 measures:

In the ISO 27001 methodology used by most partners or sub-processors of Memocom, a number of control measures have been included, consisting of main components, subdivided into sub-components. The main parts consist of:

- information security policy;
- organizing information security;
- safe staff;
- management of assets;
- access security;
- cryptography;
- physical protection of the environment;
- security of business operations;
- communication security;
- maintenance of systems;
- supplier relationship;
- management of information security incidents;
- information security aspects of business continuity management;
- compliance.

The main subsections and subsections are described in more detail in ISO 27001 and ISO 27002. Should the Processing Officer require additional specific control measures, please refer to Appendix 1 Specification of personal data and data subjects