

Processor Agreement



**LARGE ENOUGH FOR FLEXIBILITY AND
SMALL ENOUGH FOR CUSTOMER
INTIMACY**

Contents

1. Introduction	3
2. Processing of Personal Data	3
3. Securing Personal Data	4
4. Use of Sub-processors	4
5. Data breach	4
6. Liability	4
7. Return of Personal Data and retention period	5

Annex 1: Security measures overview

Annex 2: Definitions

1. Introduction

The GDPR sets rules for the protection of Personal Data across the EU and affects every service provider that uses Personal Data in any way.

1. As Xibis processes Personal Data in the context of development, testing and management, Xibis is required, under the GDPR-guidelines, to enter into a Processing Agreement with its customers, hereinafter referred to as "Client".
2. This Processor Agreement takes effect from the moment of signature, start of the project and/or a start date specified in the order confirmation and is part of all legally valid Agreements and/or (oral) arrangements between Xibis en Client.
3. The Processor Agreement ends automatically when the processing of personal data ends. The Processor Agreement cannot be terminated separately.
4. Upon termination of this Processor Agreement, ongoing obligations for Xibis, such as the notification of Data breaches involving the Client's Personal Data, and the duty of confidentiality will continue.

2. Processing of Personal Data

1. Xibis will only process Personal Data in accordance with the GDPR requirements directly applicable to Xibis' products and services.
2. Xibis only processes the Personal Data within the scope of the services to be provided under the Agreement and in accordance with the written instructions of the Client.
3. Xibis abides by the law and processes data in a proper, careful and transparent manner.
4. Client is the Data Controller and has and maintains full control over Client's Personal Data.
5. Xibis shall not process Client's Personal Data in any other way, unless Client gives its prior consent or instruction to do so.
6. The maximum Personal Data that parties expect to process concerns the name and address details lawfully provided by Client and any other data Client wishes to enter in the software. In addition, in the context of testing, developing software and analysing problems, Xibis uses back-ups and data dumps.
7. Client declares to act in accordance with the GDPR and comply with its obligations under applicable law.
8. Client guarantees the lawfulness of the use, processing, archiving, purpose of use and exchange of Client's Personal Data and/or any other use resulting from the implementation of this Processor Agreement.
9. Xibis will fully cooperate so that Client can comply with its legal obligations if a Data Subject exercises his or her rights under applicable regulations regarding the processing of Personal Data. The obligations of the GDPR include being able to comply with the following rights of the Data Subject: the right of inspection, right to rectification, right to erasure of data, right to restriction of processing and right to notification of actions carried out as a result of the aforementioned rights.
10. Without prior written consent of Client, Xibis may not process, transfer, modify, change, supplement or disclose any Personal Data to any other person or organisation.
11. As soon as Xibis receives a request to that effect, as referred to in paragraph 9, from a Data Subject, Xibis will immediately inform Client. Client will inform Xibis whether Xibis, on behalf of Client, can respond to the request and, if so, in what manner.
12. Without prejudice to its obligations under the Agreement, Xibis shall, in such case, immediately correct or otherwise adjust the Personal Data in accordance with Client's instructions.
13. If Xibis engages other organizations with the consent of the Client, they must, as a minimum, comply with the requirements set out in this Processor Agreement.

3. Securing Personal Data

1. Xibis ensures that Personal Data are adequately secured. To prevent loss and unlawful processing, Xibis takes appropriate technical and organizational measures.
2. These measures are appropriate to the risk of the processing, classified as normal. An overview of these measures and the policy on them is included in Appendix 1.
3. Xibis will ensure that for staff members or sub-processors who have access to the Personal Data of Client, access is strictly limited to only those relevant Personal Data required to perform the work.
4. All the above mentioned persons will be notified by Xibis of:
 - a. The confidential nature of the Personal Data and be made aware of Xibis' obligations under this Processor Agreement with respect to the Personal Data
 - b. Their responsibilities
 - c. Confidentiality obligations or professional or legal obligations of confidentiality
5. If Xibis or the Client finds that a change in the security measures to be taken is necessary, consultations will be held about the change thereof.

4. Use of Sub-processors

1. Client acknowledges and accepts that Xibis may appoint sub-processors in relation to its products and services for the processing of Personal Data.
2. If a sub-processor is deployed to perform the work specified in the Agreements and/or (oral) agreements with Client, this will be coordinated with Client in advance.
3. Xibis will ensure, by contract or other legal document, that any sub-processor is subject to obligations in relation to the processing of Personal Data which will be no less protective than the obligations to which Xibis is subject under this Processor Agreement.
4. If the sub-processor fails to comply with its data protection obligations, Xibis remains fully liable to the Client for compliance with the sub-processor's obligations.

5. Data breach

1. In accordance with the GDPR requirements, Client, as the Data Controller, is responsible for reporting any Data Breach to the Authority for the Protection of Personal Data (AP). Xibis will, therefore, not make any reports to the AP itself.
2. If an incident occurs, Xibis will inform Client without delay with a target deadline of 12 hours but no later than 72 hours after the discovery of the Data breach with the information specified in Article 33 (3) of the GDPR, so that Client can fulfil its obligations as responsible party.
3. The assessment of whether there is a Data breach lies with the Client. Client takes the lead in this and assesses whether a Data breach must be reported. Xibis will provide all requested cooperation in this respect.
4. If Client makes a (preliminary) notification to the AP and/or the Data Subject(s) regarding a Data breach at Xibis, without having previously discussed this with Xibis, Client will be liable for any damages and costs incurred by Xibis.
5. For the determination of a Data breach, Xibis uses the GDPR and the Compulsory Data Breach Notification Policy as guidelines

6. Liability

1. Xibis is liable to Client for the damage caused by the processing Personal Data when, in the processing, the obligations specifically addressed to Xibis included in this Processor Agreement have not been complied with and/or Xibis acts in violation of the GDPR Regulation. In the context

of this article, Xibis means Xibis, its employees and/or third parties engaged by it, including sub-processors.

2. In connection with this article, Xibis indemnifies Client for all damages, fines, claims of third parties (including Data Subjects) and expenses of Client. This also applies if there has been a breach of Client's lawful instructions.

7. Return of Personal Data and retention period

1. This Processor Agreement forms part of Agreements and/or (oral) agreements between Parties and enters into force for an indefinite period of time at the time the Agreements and/or (oral) agreements are concluded.
2. In the context of the ongoing nature of the relationship between Parties, Personal Data will, with the consent of Client, be retained after termination of the Agreements and/or (oral) arrangements for as long as necessary within the relationship between Parties.
3. Should Client wish to have the data removed, a written request to that effect may be submitted to Xibis. Xibis undertakes to comply with this immediately and in any case within ninety calendar days after the request.
4. Xibis contact details: info@xibis.nl or 0183-640028.

ANNEX 1

Overview with security measures

Below is an overview of the security standards included in this Processor Agreement. In order to determine what constitutes appropriate security measures, an assessment has been carried out based on the risks of the processing, including the following points:

- The type of Personal Data being processed (normal, special or sensitive) and any associated (risk) classification that Xibis itself has given to the data
- The number of Data Subjects whose data is processed
- The purpose for which data is processed
- The duration and manner in which data should be retained

A distinction is made between organizational security requirements, such as preventing the theft of a laptop containing Personal Data from the car, and technical security requirements, such as a comprehensive IT environment secured against viruses and where encryption of data is applied.

Technical security measures

- ✓ Up-to-date virus scan
- ✓ Unique login code and password (changed regularly)
- ✓ No unsecured external hard disks
- ✓ No unsecured back-ups made

Organizational security measures

- ✓ Clean desk policy
- ✓ Do not leave laptop unattended
- ✓ Never leave a laptop in the car
- ✓ Properly destroy old documents
- ✓ Careful use of USB sticks

ANNEX 2

Definitions

The terms used for this purpose following from the General Data Protection Regulation (GDPR) and have the following meanings:

- **Agreement:** The initial Agreement from which this Processor Agreement results
- **Data Subject:** Identified or identifiable natural person to whom the processed Personal Data relates
- **Data breach:** A security breach that accidentally or unlawfully results in the destruction, loss, alteration or unauthorized disclosure of, or unauthorized access to, transmitted, stored or otherwise processed data
- **Data Controller:** A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing Personal Data
- **GDPR:** General Data Protection Regulation. Regulation (EU)2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data and repealing Directive 95/46/EG
- **Parties:** Joint designation of Xibis and Client
- **Personal Data:** Any information about an identified or identifiable natural person that Xibis processes in the context of the performance of its obligations under the Agreement
- **Processor Agreement:** This Agreement including its annexes
- **Processing:** Any operation or set of operations involving Personal Data, including the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of data
- **Sub-processor:** Any third party appointed by Xibis to process data