

BICSMA´S

DATA PROCESSING AGREEMENT

**Table of Contents**

[**1 Definitions** 4](#_Toc5181818)

[**2 Formation, duration and termination of the Data Processing Agreement** 4](#_Toc5181819)

[**3 Processing of the Personal Data by Processor** 5](#_Toc5181820)

[**4 Third parties** 5](#_Toc5181821)

[**5 Data subject rights** 6](#_Toc5181822)

[**6 Return of the Personal Data and data retention** 7](#_Toc5181823)

[**7 Security and Personal Data Breaches** 7](#_Toc5181824)

[**8 Confidentiality** 8](#_Toc5181825)

[**9 Liability** 9](#_Toc5181826)

[**10 Audits** 10](#_Toc5181827)

[**11 General conditions** 10](#_Toc5181828)

[**Annexes:** 12](#_Toc5181829)

[**Annex 1: Processing of the Personal Data** 12](#_Toc5181830)

[**Annex 2: List of sub-processors** 12](#_Toc5181831)

[**Annex 3: Contact details to notify Controller of a Personal Data Breach or a security incident** 12](#_Toc5181832)

[**Annex 4: Appropriate technical and organisational measures** 13](#_Toc5181833)

*Note*

*This publication is educational material and does not constitute legal advice. For full information and guidance, please seek professional legal advice.*

This Agreement is made between

**Bicsma**, a private company with limited liability [enter other legal form if applicable], having its registered office and principal place of business in Breukelen, the Netherlands [place, country] at [address], [postal code], represented by [name of authorised representative(s)**]**, hereinafter referred to as “**Controller**”

and

**Company 2**, a private company with limited liability [enter other legal form if applicable], having its registered office and principal place of business in [place, country] at [address], [postal code], represented by [name of authorised representative(s)**]**, hereinafter referred to as “**Processor**”,

hereinafter collectively referred to as “the Parties”,

whereas:

1. The General Data Protection Regulation (hereinafter “the GDPR”) mandates Controller to use only Processors who provide sufficient guarantees to implement appropriate technical and organisational measures which meet the requirements of the GDPR, including for the security of processing and for the protection of the rights of the data subjects;
2. Processor provides services for Controller as specified in the Service Agreement [enter title of agreement] of [date] (hereinafter referred to as “the Underlying Agreement”);
3. Within the meaning of Article 4 paragraph 7 of the GDPR, Controlleris responsible for any Personal Data processing carried out on its behalf;
4. Within the meaning of Article 4 paragraph 8 of the GDPR and pursuant to the Underlying Agreement, Processor carries out Personal Data processing on Controller’s behalf;
5. Pursuant to Article 28 paragraph 3 of the GDPR, the Parties wish to lay down their rights and obligations regarding the processing of Personal Data by Processor on behalf of Controller in this Agreement, hereinafter: "Data Processing Agreement";
6. This Data Processing Agreement shall be regarded as a binding agreement on Processor with regard to Controller within the meaning of Article 28 paragraph 3 of the GDPR;
7. Controller provides that the Processor is authorised to process Personal Data on behalf of Controller;

hereby agree as follows:

**1 Definitions**

The terms used in this Data Processing Agreement shall be interpreted as follows and have the same meaning as in the GDPR:

1.1 Data Subject means the person to whom the Personal Data relates.

1.2 Data Processing Agreement means this Agreement including its Annexes.

1.3 Personal Data means any information relating to an identified or identifiable natural person.

1.4 Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed for the execution of the Underlying Agreement.

1.5 Processing means any operation or set of operations which is performed on Personal Data, including at least the collection, recording, arranging, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data.

1.7 GDPR means the General Data Protection Regulation.

1.8 Applicable Data Protection Laws mean any laws, by-laws, regulations, orders and requirements of any government entity or public authority that has jurisdiction over Processor or Controller, and any administrative or court decision in relation to the protection of Personal Data including, but not limited to, the GDPR.

**2 Formation, duration and termination of the Data Processing Agreement**

2.1 This Data Processing Agreement shall enter into force on the day on which Parties sign the Underlying Agreement.

2.2 This Data Processing Agreement shall remain in force until the Underlying Agreement expires or is terminated. This Data Processing Agreement is terminated automatically on the day on which the Underlying Agreement expires or is terminated. None of the Parties may terminate this Data Processing Agreement prematurely.

2.3 This Data Processing Agreement may only be amended by Controller on the basis of amended laws and regulations and the instructions of the regulatory authorities. Deviations from this Data Processing Agreement are only binding if and insofar as expressly agreed to by the Parties in writing.

**3 Processing of the Personal Data by Processor**

3.1 Processor shall process, on behalf of Controller, the Personal Data described in Annex 1*.*

3.2 Processor shall process the Personal Data in a proper and careful manner and in accordance with the GDPR and other Applicable Data Protection Laws. If Processor considers that an instruction mentioned in this Data Processing Agreement, or given by Controller, infringes the Applicable Data Protection Laws, Processor shall immediately inform Controller of the alleged infringement.

3.3 Processor shall process the Personal Data described in Annex 1 only on behalf of Controller. Processor shall follow all instructions of Controller with regard to the Processing. If Processor is subject to legal obligations that conflict with the instructions of Controller or otherwise impact the Processing, Processor shall immediately notify Controller of such legal obligations. In any event, Controller shall be able to instruct Processor to change Processor's Processing practices, and processor shall immediately follow the instructions of Controller.

3.4 Processor shall only process the Personal Data to the extent necessary for performance of the Underlying Agreement, for performance of the instructions of Controller, for performance of this Data Processing Agreement, and for compliance with the Applicable Data Protection Laws.

3.5 Processor shall have no control over the purposes and means of the Processing of the Personal Data. Unless otherwise determined in this Data Processing Agreement, Processor shall not make any decisions regarding the use of the Personal Data, the access to the Personal Data by third parties, and the duration of the period for which the Personal Data are stored. Controller has exclusive authority over the Personal Data provided under this Data Processing Agreement.

3.6 Processor shall fully support the Data Protection Officer of Controller in the performance of its mandatory tasks as set out in Articles 38 and 39 of the GDPR. Processor shall ensure that the Data Protection Officer of Controller is informed of, and involved in, all issues which relate to the Processing of the Personal Data.

**4 Third parties**

4.1 Processor may not engage any third party as a sub-processor to process the Personal Data within or outside the European Union without the prior written consent of Controller. Controller hereby agrees to Processor’s use of the sub-processors listed in Annex 2.

Processor hereby undertakes to inform Controller of any intended changes concerning the Processing, including the engagement of a new sub-processor or the replacement of an existing sub-processor. Before engaging a new sub-processor or replacing an existing sub-processor, Processor shall give Controller written notice two months prior to that engagement and/or replacement. Processor shall ensure that all of the sub-processors are bound to the obligations arising from this Data Processing Agreement and the Applicable Data Protection Laws. Any agreement between Processor and its sub-processors shall contain the obligations imposed on Processor under this Data Processing Agreement, with special regard to obligations concerning the security of the Processing and the exercise of data subject rights.

Processor remains fully responsible for the Processing of the Personal Data in accordance with the Underlying Agreement, this Data Processing Agreement, the GDPR, and the Applicable Data Protection Laws. Processor shall vouch that all of the sub-processors engaged by Processor comply with the requirements set out in the Underlying Agreement, this Data Processing Agreement, the GDPR, and the applicable Data Protection Laws. In the event of infringement of Processor’s and sub-processor’s obligations under the Underlying Agreement, this Data Processing Agreement, the GDPR, and the Applicable Data Protection Laws, Processor shall remain fully liable to Controller and shall be held liable for the entire damage.

4.2 Processor shall not disclose the Personal Data to any third party, except upon the prior written request or authorisation of Controller.

4.3 If Processor is requested to provide information related to the Personal Data based on a legal obligation of Processor, Processor shall verify the identity of the requesting party and whether the request is truly based on valid legal obligation. Wherever possible, Processor shall inform Controller of such requests prior to the disclosure of the Personal Data.

**5 Data subject rights**

5.1 Processor shall take every effort to enable Controller to fulfil its obligation to facilitate the exercise of data subject rights under the GDPR and other Applicable Data Protection Laws. Such data subject rights include, in particular, the right of access, the right to rectification, the right to erasure, the right to restriction of Processing, the right to data portability, the right to object to the Processing, and the right not to be subject to automated decision-making including profiling. Processor shall provide Controller with all the information Controller may need to be able to respond to data subject requests as required by the GDPR or the Applicable Data Protection Laws.

5.2 Processor hereby confirms that it possesses the necessary means to assist Controller in complying with data subject rights and data subject requests. Processor hereby confirms that it will take all reasonable measures to ensure that Controller is able to comply with all requests submitted by Data Subjects in relation to the Processing of their Personal Data and their rights under Articles 12-22 of the GDPR.

5.3 Processor shall notify Controller immediately of any request received from a Data Subject in relation to their Personal Data under Processing. Following receipt of the notification, Controller may instruct Processor to inform the Data Subject concerned that all requests in relation to the Processing shall be submitted to Controller, or request Processor to respond to the request. Where Controller requests Processor to respond to the request, and/or where Processor can reasonably conclude that responding to the request is part of the obligations of Processor under the Applicable Data Protection Laws, Processor shall consult with Controller before responding to the request. Processor may not react to any request submitted by a Data Subject without the prior written consent of Controller.

5.4 Upon request of Controller, Processor shall provide Controller with information about the Processing performed for the purposes of the Underlying Agreement. The information provided by Processor shall enable Controller to respond to any request or complaint received from a Data Subject relating to the Processing of the Personal Data by Processor.

**6 Return of the Personal Data and data retention**

6.1 Upon termination or expiry of this Data Processing Agreement, all the Personal Data shall be deleted or returned to Controller in the manner set out in the Underlying Agreement. (If the Underlying Agreement does not contain relevant requirements, they should be included in this clause).

6.2 Upon termination or expiry of this Data Processing Agreement, Processor shall aid Controller to transfer the Processing Activities to the subsequent Processor as set out in the Underlying Agreement. (If the Underlying Agreement does not contain relevant requirements, they should be included in this clause).

6.3 Unless the Applicable Data Protection Laws require Processor to retain the Personal Data for a determined time period, Processor may only retain the Personal Data for the maximum retention period set out in Annex 1. When that retention period terminates, Processor shall erase all the Personal Data, unless:

6.3.1 Controller has explicitly requested Processor to retain certain categories of the Personal Data for a longer period, or Controller has explicitly requested Processor to provide the Personal Data to Controller; and/or

6.3.2 Processor has experienced a security incident and needs to process the Personal Data to investigate that incident.

6.4 Where Clause 6.3.1 applies, Processor shall retain the Personal Data for the requested time period and/or provide the requested data to Controller on a suitable data carrier.

6.5 Where Clause 6.3.2 applies, Processor shall inform Controller of the incident and provide the data to Controller on a suitable data carrier.

**7 Security and Personal Data Breaches**

7.1 Processor shall notify Controller of any Personal Data Breach without undue delay and within forty-eight (48) hours after becoming aware of the Personal Data Breach. Processor shall use the contact details included in Annex 3 to inform the Controller about the following aspects of the Personal Data Breach:

1. the nature of the breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. the name and contact details of the data protection officer or other contact point where more information can be obtained;
3. the likely consequences of the breach;
4. the measures taken or proposed to be taken to contain the breach and to mitigate its possible adverse effects on data subjects.

Unless otherwise agreed in writing, Controller shall notify the Personal Data Breach to the competent supervisory authority (or authorities). Where required, Controller shall also inform the Data Subject(s) concerned of the Personal Data Breach. Processor shall provide all assistance to Controller in order to ensure that Controller is able to comply with its Personal Data Breach notification obligation. In particular, at the request of Controller, Processor shall provide Controller with (i) all the (additional) information and (ii) all the documents necessary for Controller to comply with the relevant provisions of the GDPR and the Applicable Data Protection Laws.

7.2 Processor shall implement at least the technical and organisational security measures described in the Underlying Agreement and the policies listed in Annex 4. The technical and organisational security measures of Processor shall ensure an adequate level of data protection, considering the nature of the Processing, the risks inherent in the Processing, the state of the art, and the costs associated with the implementation and execution of the measures.

7.3 Processor shall submit regular reports to Controller in order to assess the continued effectiveness of the technical and organisational security measures taken by Processor. In addition, Processor shall demonstrate compliance with recognised information security and/or service management standards, such as ISO / IEC 27001: 2013 and ISO/IEC 27002 or equivalent. Processor shall demonstrate compliance with such standards by valid certifications or equivalent evidence. Processor shall have a fully implemented, fitting and explicit security policy for the Processing of Personal Data. At Controller 's request, Processor shall provide to Controller a copy of that security policy.

7.4 Controller is entitled to propose Processor to take additional security measures. Where the additional security measures proposed by Controller lead to a change of the Underlying Agreement or any other agreement between Controller or Processor, the Parties shall agree in good faith to implement the proposed changes.

**8 Confidentiality**

8.1 Processor shall keep the Personal Data confidential. Processor shall not disclose Personal Data in any way to any employee or any third party without the prior written consent of Controller, except where:

(i) the Personal Data need to be disclosed to a competent public authority to comply with a legal obligation, or

(ii) the Personal Data are required for audit purposes, or

(iii) the Personal Data are required by authorised staff members of Processor in order to execute the Processing activities that Processor and Controller have agreed upon.

8.2 Processor shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data. Processor shall ensure that all personnel engaged in the Processing have received appropriate training on their responsibilities, and are subject to obligations of confidentiality. Processor shall ensure that confidentiality obligations in respect of the Personal Data remain binding on all members of the personnel after the termination of employment, regardless of the cause of such termination.

8.3 Processor shall take commercially reasonable steps to ensure the reliability of any personnel engaged in the Processing of the Personal Data.

8.4 Processors shall ensure that access to Personal Data is limited to those personnel who require such access to perform the tasks of Processor under the Underlying Agreement.

8.5 In addition, Processor is obliged to:

a) make timely changes to the authorisations granted in the event that there is a change in the position of the personnel/third party, and/or in the event that the personnel/third party leaves Processor;

b) periodically review the authorisations granted and all authorisation changes;

c) register the authorisations granted in such a manner that any individual abuse of the Personal Data can be detected and ceased at an early stage.

**9 Liability**

9.1 Any failure to fulfil the obligations of Processor entitles Controller to request Processor to rectify the mistake at Processor’s own cost and risk.

9.2 Processor shall be held liable for any damage suffered by Controller as a result of (i) an infringement of the obligations of Processor under this Data Processing Agreement, and / or (ii) the acts or omissions of third parties engaged by Processor.

9.3 Processor shall maintain an indemnity insurance that provides protection against the liabilities set out in Section 9 of this Data Processing Agreement. At the request of Controller, Processor shall give Controller unconditional access to the insurance policy and the pertaining premium payment receipts.

9.4 Processor shall forfeit to Controller an immediately due and payable penalty of € 25,000 twenty-five thousand euros) for each and any violation of this Data Processing Agreement. Processor shall forfeit to Controller a penalty of € 500, - (five hundred euros) for each day that the violation continues, without prejudice to Controller's right to claim full compensation for the damage suffered.

9.5 Controller represents and warrants that it has obtained the Data Subject’s express consent and/or has another lawful basis to process the Personal Data. Controller represents and warrants that the content of the Personal Data is not unlawful and does not infringe any rights of third parties. Controller indemnifies Processor from and against all claims and actions made by third parties in respect of the Processing of Personal Data without express consent and/or lawful basis under this Data Processing Agreement.

**10 Audits**

10.1 Controller is entitled to perform audits on the security measures implemented by Processor and Processor’s adherence to the confidentiality obligations set out in Section 8 of this Data Processing Agreement. Such audits may be carried out by an expert of Controller or by a third party sworn to secrecy. Unless a supervisory authority requires otherwise, the number of audits by Controller shall be limited to a single audit over a one-year (12-month) period. Where there is a valid reason, Controller shall have the right to perform additional audits. At the request of Controller, Processor shall ensure that Controller is able to test Processor’s compliance with the requirements set out in this Data Processing Agreement and the Underlying Agreement. Controller shall bear any costs relating to the audits, unless the audit results show that Processor has failed to meet its obligations under this Data Processing Agreement. In that event, Processor shall bear all costs of the audit.

10.2 Processor shall once a year provide to Controller an auditor’s opinion report drawn up by an independent external expert. The report shall contain the auditor’s opinion on Processor’s compliance and, where appropriate, relevant improvement recommendations to enhance Processor’s compliance.

10.3 Processor shall make all reasonable efforts to provide assistance to the auditor in assessing Processor’s compliance. Processor shall also ensure that any third parties engaged in the Processing by Processor provide the same assistance to the auditor.

10.4 The performance of audits shall not lead to any delay in the activities to be performed by Processor under the Underlying Agreement and / or this Data Processing Agreement.

10.5 Processor shall implement all the improvement recommendations included in the auditor’s opinion. Controller may set a time limit for Processor to implement the recommended improvements. Processor shall submit to Controller a report on implementing the improvements.

**11 General conditions**

11.1 The Parties agree that those obligations of Processor that are intended to survive the termination/expiry of the Underlying Agreement and this Data Processing Agreement, will persist after the termination/expiry of the Underlying Agreement and this Data Processing Agreement. The obligations referred to herein include, but are not limited to: (i) the transfer of the Personal Data, (ii) the identification of unauthorised Processing, (iii) the confidentiality obligations of the personnel of Processor and the confidentiality obligations of the third parties engaged in the Processing by Processor.

11.2 Deviations from this Data Processing Agreement are only binding if and insofar as expressly agreed between the Parties in writing.

11.3 The provisions of the Underlying Agreement, including its annexes, apply to this Data Processing Agreement. If there is conflict between one or more provisions of the Underlying Agreement and one or more provisions of this Data Processing Agreement, the provision(s) of this Data Processing Agreement shall prevail. The general terms and conditions of Processor shall not apply to the Processing of the Personal Data and this Data Processing Agreement, and are hereby expressly rejected by Controller.

Thus agreed and signed in duplicate,

Place, [date]

Controller Processor

on its behalf, on its behalf,

[[name signature)] [name signature)]

**Annexes:**

1. Processing of the Personal Data
2. List of sub-processors
3. Contact details to notify Controller of a Personal Data Breach or a security incident
4. Appropriate technical and organisational measures

**Annex 1: Processing of the Personal Data**

1. Name / Description of the processing;

Give a description of the processing

1. Nature and purpose of the processing of the Personal Data;

Describe the nature and purpose of the processing

1. Categories of the data subjects and Personal Data covered in the Data Processing Agreement

*Describe categories of the data subjects and the Personal Data concerned*

1. The duration of the processing:

*How long will the Personal Data be processed?*

**Annex 2: List of sub-processors**

**Add names of sub-processors to be approved by Controller**

**Annex 3: Contact details to notify Controller of a Personal Data Breach or a security incident**

First contact person:

Fill in contact information

Second contact person:

Fill in contact information

**Annex 4: Appropriate technical and organisational measures**

Remove or add bullets to list the technical and organizational measures you would like to make mandatory for Processor. Naturally, the measures should be determined in relation to the nature of the processing and the Personal Data concerned.

• Information security policy (which explicitly addresses data protection measures and has been made known to all employees and relevant external parties);

• Unambiguous allocation of responsibilities with regard to information security at all organisational levels, including Board and executive level;

• Security awareness;

• Physical security and security of equipment;

• Access security;

• Logging and monitoring;

• Compliant processing and safeguards in all application systems;

• Appropriate management of technical vulnerabilities;

• Incident management;

• Data breach and security incident procedure;

• Continuity management;

• Data protection and the confidentiality of personal data;

• Confidentiality agreements

