

TICKETCOUNTER DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") sets forth the parties' understandings regarding the processing of personal data under the Master Service Agreement and its terms. This DPA is an addendum to the Master Service Agreement and applies automatically when the conditions are met as specified in the Master Service Agreement or in an Order Form. The Master Service Agreement means the agreement that relates to the provision of ticket counter services (<https://www.ticketcounter.eu/ticketoplossingen>). The term of this DPA shall follow the term of the Master Service Agreement. Terms not defined herein shall have the meanings set forth in the Master Service Agreement.

This agreement is between **Ticketcounter B.V.**, a private limited company, with its registered office in The Hague, having its office at Van Nelleweg 1404, 3044 BC Rotterdam, registered under number 27279246 with the Chamber of Commerce, legally represented by Mr. S. B. Bakker, hereinafter referred to as 'Ticketcounter' or 'Processor' and the Customer of Ticketcounter (as further specified in the Master Service Agreement), hereinafter referred to as Controller. Processor and Controller will also be referred to separately hereinafter as "Party" or jointly as "Parties".

Whereas:

- A. In the performance of the Master Agreement, Controller makes personal data available to Processor. Processor shall process this personal data in the context of the said Master Agreement without Processor determining therein the purpose and means for such processing;
- B. The parties wish to regulate the processing of personal data by Processor through this Agreement, in accordance with the General Data Protection Regulation (hereinafter "GDPR").

PARTIES AGREE AS FOLLOWS:

ARTICLE 1 DEFINITIONS

Capitalized terms used in this Agreement shall have the meanings ascribed to them in this article.

- 1.1 Data Subject(s): the person(s) to whom a Personal Data relates.
- 1.2 Appendix: an appendix to the Agreement, which forms an integral part thereof.
- 1.3 Service Agreement: the Master Service Agreement between the parties relating to the services provided by Processor to Controller, which forms the basis of the Processing Agreement.
- 1.4 Data Processing Agreement: this agreement between Processor and Accountable Person including Appendices.
- 1.5 Personal Data: any data relating to a natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.
- 1.6 Controller: the party that determines the purpose of and means for Processing Personal Data.
- 1.7 Processing/Processing: any act or set of acts in relation to the Personal Data, including in any case the collection, recording, organization, storage, updating, modification, retrieval, consultation, use, provision by means of transmission, dissemination or any other form of making available, alignment, combination, blocking, erasure or destruction of data.
- 1.8 Any definition not mentioned shall have the meaning given in the General Data Protection Regulation (GDPR).

ARTICLE 2 SUBJECT OF THE AGREEMENT

- 2.1 Processor shall Process Personal Data on behalf of Controller under the terms of the Agreement. Appendix 1 to the Agreement describes the purposes of the Processing, the means of Processing, the type of Personal Data to be Processed and the duration of storage of the Personal Data. The Parties shall update Appendix 1 as necessary at any time during the term of the Agreement.
- 2.2 The Parties note that the Personal Data to be processed are potentially sensitive data within the meaning of the GDPR. Parties shall therefore observe the relevant legal requirements in the Processing thereof.

ARTICLE 3 IMPLEMENTATION OF PROCESSING

- 3.1 Processor and Controller shall Process the Personal Data in a proper and careful manner, in accordance with applicable privacy laws and regulations.
- 3.2 The Controller shall not ask Processor to implement technical facilities or methodologies that may allow processing of data concerned to result in personal data being stored or processed outside the EU. Where possible, Processor will not store or process personal data outside the EU without the consent of the Controller. In this case, Processor will process the personal data based on the European Commission's Standard Contractual Clauses (SCC) (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en).
- 3.3 In the event that Controller wishes to implement facilities as under paragraph 3.2 above, Controller will submit a processor agreement in advance.
- 3.4 Controller determines the purpose and means of the Processing of Personal Data and is liable to Data Subject(s) for the Processing of Personal Data, without prejudice to Processor's obligations under the Service Agreement and the Agreement.
- 3.5 Subject to legal obligations, Processor shall process the Personal Data only to the extent necessary for the performance of its obligations under the Service Agreement. In any case, the processing will be carried out in accordance with the applicable privacy policy of Processor.
- 3.6 Processor shall not modify the Personal Data without an instruction to do so from Controller. Personal Data shall not be kept longer than necessary. This period is for the time being set at 14 months after the access ticket has expired, unless another period is agreed upon between the parties and/or unless the legal retention obligation (e.g. fiscal) for Processor is longer. Deviations from the aforementioned term must be in writing and signed by both parties in an addendum which forms an inseparable part of this processing agreement.
- 3.7 With the consent of the Data Subject, Controller may also process the personal data for its own use on its systems.
- 3.8 Controller is responsible for informing Data Subjects and ensuring that Data Subjects exercise their rights under applicable laws and regulations and for communicating with Data Subjects. Processor shall provide all cooperation to Controller, within the legal frameworks, to enable Controller to comply with its relevant obligations, including (i) allowing Data Subjects to access their Personal Data, (ii) removing or correcting Personal Data at the request of Data Subjects, and/or (iii) demonstrating that Personal Data has been removed or corrected following a request to do so by a Data Subject.
- 3.9 Processor is not entitled to transfer its obligations under the Agreement, in whole or in part, to (a) third party (parties) or to engage a third party (parties) in the Processing without the prior, explicit and written consent of the Controller. Processor will inform Controller in a timely manner of the desired transfer or engagement and the identity of the third party concerned. The Processor will make similar arrangements with the third party in respect of the Processing as those laid down in the Agreement.
- 3.10 Controller has noted and accepted that at the inception of the Agreement, Processor has a partnership with third parties as referred to in Article 3.9. Third parties include sub-processors who process personal data on behalf of Processor. These sub-processors are specified in Appendix 3.

ARTICLE 4 SECURITY

- 4.1 Processor shall take the technical and organizational security measures - which meet the applicable privacy laws and regulations, state of the art and cost of implementation measures - that are necessary to ensure the availability, integrity and confidentiality of the Personal Data and to secure them against loss or unlawful Processing. These measures are described in Appendix 2 and will comply with the applicable generally accepted security standards.
- 4.2 Processor shall always report any security incidents to Controller without delay. In the report, Processor shall state which incident has occurred, the possible consequences of the incident for the Personal Data concerned (or for access to it), and what measures have been or will be taken to end the incident and prevent it from occurring in the future. In accordance with the statutory

frameworks, the Controller will report the incident to the Personal Data Authority and/or the Controller and/or another authority, if applicable.

- 4.3 In the event that the incident may have consequences for the Data Subject(s), the Processor will, where necessary, also cooperate in informing the Data Subject(s) adequately about the security incident.

ARTICLE 5 CONFIDENTIALITY

- 5.1 Processor shall keep the Personal Data confidential. If this is not contractually agreed with persons employed by or working for the Processor, as well as Processor itself, Processor shall impose a confidentiality obligation on those persons with respect to the Personal Data of which they may become aware.
- 5.2 Processor shall not disclose the Personal Data in any way or make them available to third parties, unless a legal requirement obliges Processor to provide the Personal Data.

ARTICLE 6 AUDITS

- 6.1 Processor shall at all times allow Controller to have Processor's compliance with the obligations set forth in this Agreement audited by independent auditors without using and accessing, to the extent reasonably possible, Processor's confidential data. Processor shall provide Controller with all data and information reasonably required by Controller to conduct the audit. If the audit reveals that Processor is not in full compliance with its obligations, Processor shall immediately terminate (remediate) the deficiencies demonstrated by the audit at its own expense.

ARTICLE 7 CHANGES

- 7.1 In the event of changes in the work to be carried out by the Processor and/or the Controller under the Service Agreement that may affect the Processing, the parties will always consult with each other about the changes to the Agreement that may be necessary, which expressly include changes to the technical and organizational measures referred to in Article 4 of the Agreement.

ARTICLE 8 TERM AND TERMINATION

- 8.1 This Agreement shall apply for as long as Processor processes the Personal Data in connection with the Service Agreement.
- 8.2 If and when this Agreement ends, Processor shall return the documents, computer disks and other data carriers containing the Personal Data to Controller. To the extent that the Personal Data is contained in a computer system and/or in any other form as a result of which it cannot reasonably be returned, Processor shall completely remove the Personal Data from it insofar as this is technically possible and provide a copy of the Personal Data to Controller. This is in line with the provisions in Art. 3.6 and Art. 3.7.
- 8.3 After termination of this Agreement, the provisions which by their nature are intended to remain in force afterwards, including the obligation of secrecy, will remain in full force.

ARTICLE 9 LIABILITY AND INDEMNIFICATION

- 9.1 Any claims arising out of, or related to, this Processing Agreement shall be subject to the terms and conditions of the (i) General Terms and Conditions B2B of Processor and (ii) Processor's Master Service Agreement with Controller.

ARTICLE 10 APPLICABLE LAW AND DISPUTE RESOLUTION

- 10.1 This Agreement shall be governed by Dutch law, to the extent that mandatory provisions do not oppose this. There is both a Dutch and an English version of this Agreement. In the event of contradictions in the interpretation of the versions, the Dutch text will always be decisive and binding between the Parties.
- 10.2 Disputes arising from or related to this Agreement will be exclusively settled by the competent court in Rotterdam.

CUSTOMER	TICKETCOUNTER
Date:	Date:
Name:	Naam:
Title:	Title:
Signature:	Signature:

CONCEPT

APPENDIX 1 DESCRIPTION OF THE PROCESSING OF PERSONAL DATA

1. PERSONAL DATA TO BE PROCESSED:

Name, address, phone number, email address, contract information, bank information and ticket information of Controller and/or employees.

2. PURPOSE(S) FOR PROCESSING:

Manage and support software applications that support Controller's business process.

3. DESCRIPTION OF PROCESSING(S) AND MEANS

Processor will Process the aforementioned Personal Data in connection with the activities it undertakes to perform the Service Agreement. Processor will do so through the following means:

- Online ticketing application
- Hosted on Microsoft Azure Cloud platform (on EU territory)

4. STORAGE TERM

Processor will retain the Personal Data for the following duration:
Fourteen months after the purchased admission ticket has expired.

APPENDIX 2 TECHNICAL AND ORGANIZATIONAL MEASURES

This Appendix describes the technical and organizational measures to secure the Processing of Personal Data in more detail.

1. Standards related to information security

The Ticketcounter platform was set up in the Microsoft Azure Cloud in cooperation with Microsoft. Microsoft Azure Cloud meets the security requirements that the state of the art currently allows and meets the standards set by ISO27001. This provides the highest level of protection against unauthorized physical access to the platform in the data center.

This includes the following additional measures:

- **Anonymizing / Deleting Personal Data:**
Environments used for testing do not contain personal data. These environments are anonymized. In addition, there is a process to look up, provide insight and delete individuals who request access and/or deletion from the system.
Also, there is an automated process to delete personal data that is x days old the every night system.
- **Keyvault:**
Passwords, keys and other sensitive settings are stored in a keyvault. The various applications have access to this vault. So there is no access data in, for example, GIT (version control program).
- **Pen testing and security audit**
We have our system security tested by varying external parties. The latest test is from December 2019
- **Reports with personal data not accessible via email**
No reports containing personal data will be emailed.
- **Responsible disclosure**
A public responsible disclosure policy is available. This describes a safe procedure for outsiders to report potential problems. These reports come directly to our support team, so they can be responded to 7 days a week.
- **Development & management**
The group that can do technical support and management on production is kept as small as possible. Developers only have access to the test and acceptance environment by default.
- **Sales channels with limited viewing rights**
It is possible to indicate in a sales channel that personal data is not viewable by employees. In this way, orders remain anonymous.
- **Releases**
Releasing new software version goes through a build server and deployment scripts.
This way there is tracking and tracing of who did a release and what happened. There is no need to log in to the servers to do updates.
Coupled with the tracking and tracing in GIT (version control program), it is always possible to find out who added what code. In addition, it is recorded who did the code review before the code went to test.
- **Code reviews and Unit test**
New code can only be merged to test after it has been checked by another developer via a code review. This extra touch of quality prevents errors.
After each pull request, the available unit test are automatically run to test both the happy flow and the error handling.
- **PAAS**
We use the PAAS solutions of Microsoft Azure as much as possible. This means that we do not manage virtual machines with software updates. This allows us to keep up with security updates faster and the chance of incorrect configurations is much smaller.

2. Access control to company premises.

Ticketcounter is located in the gated office of the van Nellefabriek. Unauthorized access to Ticketcounter's office is prevented by security guards and cameras (24 hours a day, 7 days a week) and an access card system.

3. Access control to systems.

- Ticketcounter employees have access to systems that process personally identifiable information as necessary for the job the employee is performing;
- Access control is used in all environments, databases and applications;
- A single account is provided to each end user so that it is always traceable and provable who performed specific actions. It is not contractually permitted to share accounts.

4. Access control to personal data.

- Ticketcounter Employees will only be authorized for access that corresponds to the position.
- Ticketcounter has a clear procedure for termination of employee or third party accesses due to termination of the employment relationship or contract.
- Personal data is stored in databases.
- Access to personal data is always protected by a username and password.
- Ticketcounter uses secure connections in its systems through the industry standard SSL (Secure Sockets Layer).

5. Office Automation

All Ticketcounter employees receive a laptop from Ticketcounter. Our standard configuration includes the following security measures:

- Push updates
- Security updates are forced to the laptop. If these updates are not installed within the set timeframe, access to the ticket counter network will be lost
- Bitlocker encryption
- All disks are encrypted via bitlocker. Should the laptop be stolen, no access to the data on the laptop is possible.
- Windows is provided with an additional Microsoft E3 license with the security center, compliance center and defender antivirus to provide protection against viruses and ransomware.
- Depending on the function, roles and rights are assigned. This limits access to data to what the employee's job requires.
- Lastpass Enterprise Vault
- Passwords and other sensitive data are stored in the Lastpass vault. Through groups, it is possible to share data.
- File shares are only accessible with trusted computers.
- -factor authentication to access the laptop and domain.

6. Input control

- Ticketcounter maintains log files of all system operations related to Personal Data that fall under Ticketcounter's managerial responsibility.
- The Ticketcounter platform provides event logging so that any breach of security can be identified. The log files are protected against unauthorized access.

7. Ticketcounter Employees

- Confidentiality has been agreed upon in writing with all Ticketcounter employees as a permanent part of the employment contract.

8. Measures of availability.

- Computers and laptops of Ticketcounter are protected by anti-malware solutions that are kept up to date by a specialized party.
- Use of the Azure Cloud ensures a high level of availability of the platform.

N.B. The measures described in this appendix do not guarantee or ensure that any form of unauthorized access, use or unwanted loss of personal data will be prevented.

CONCEPT

APPENDIX 3 SUB-PROCESSORS

The Processor shall ensure that all persons to whom it grants access to this list of sub-processors pursuant to this Processing Agreement are bound by confidentiality and shall ensure that these confidentiality obligations are complied with. Sharing this list with third parties is not permitted, unless required by law.

Sub-Processor	Provided Services	DPA
Microsoft Azure	Cloud based storage services	yes
Microsoft 365	Email; Microsoft Dynamics; Microsoft Office	yes
Twilio (SendGrid – US partij)	Confirmation emails	yes, signed SCC's available

CONFIDENTIAL