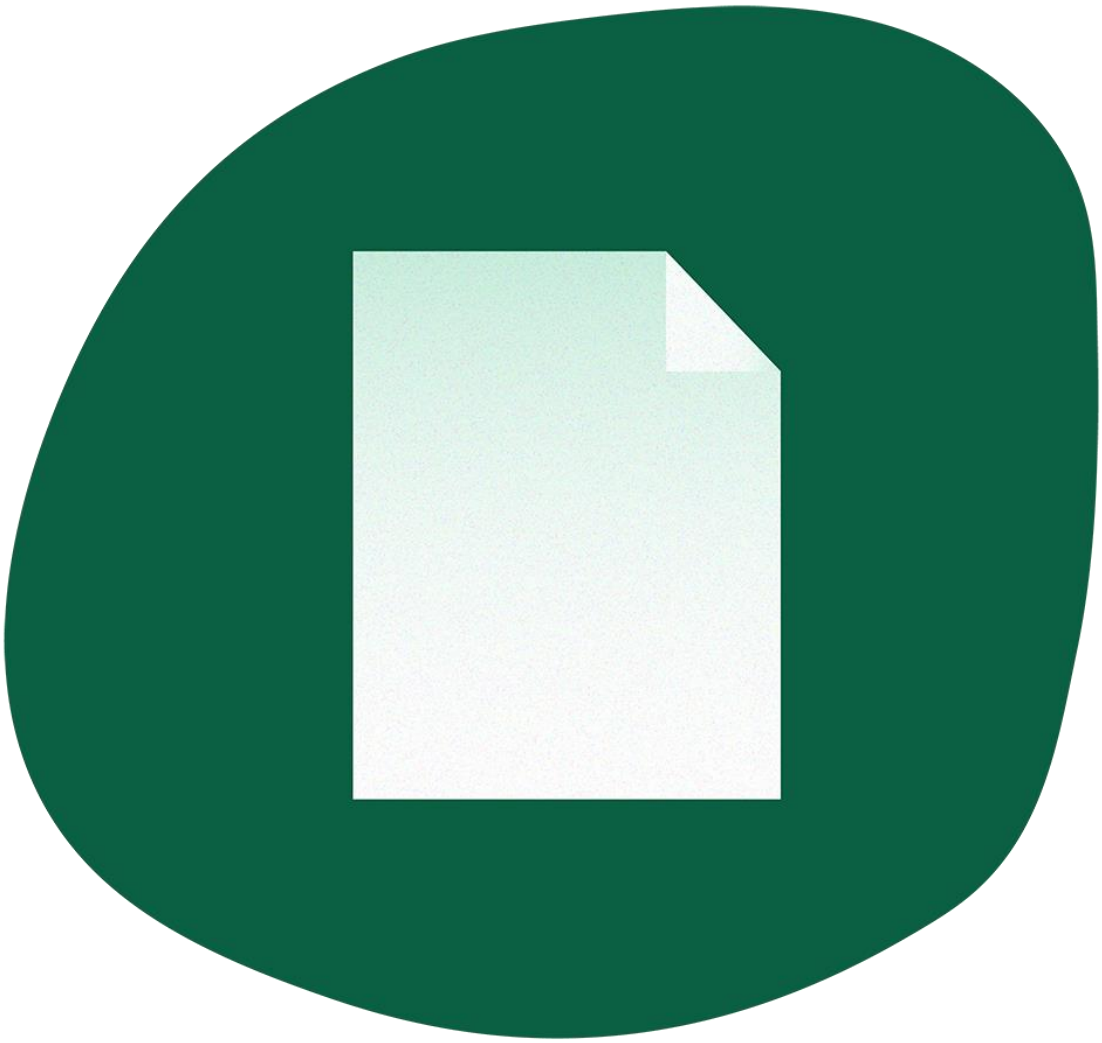
Data Processing Agreement



Queue·it

Table of Contents

1 Data Processing Agreement 1

2 AGREED TERMS 1
2.2 Purpose of Processing 3
2.3 Security and Confidentiality of Data 3
2.4 Liability 5
2.5 Surviving Obligations 4
2.6 Termination 5

3 Appendix 6
3.1 Appendix 1 - Data Processing Terms 6

1 Data Processing Agreement

1.1 This Agreement is made between

1.1.1 Queue-it ApS a company incorporated and registered in Denmark with the company number DK 33052901 whose registered office is at Skelbækgade 4, 1., 1717 Copenhagen V, Denmark (the "Supplier", "Data Processor") and

1.1.2 The legal entity that entered into an agreement with Queue-it ApS, (the "Customer", "Data Controller").

1.2 Background

1.2.1 The Customer requires certain licenses to use the Supplier's products to provide services to corporate internet facing websites.

1.2.2 The Supplier is a skilled and experienced provider of internet website crash prevention and online virtual queuing and has agreed to license such software and services to the Customer.

1.2.3 This agreement (the "Agreement") is an appendix to the terms to license the software and services to the Customer.

1.3 Interpretation

1.3.1 Where this Agreement uses the terms defined in Regulation (EU) 2016/679 including the Commission Implementation Decision of 10th July 2023 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

1.3.2 This Agreement shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 including the Commission Implementation Decision of 10th July 2023 or Regulation (EU) 2018/1725 respectively.

1.3.3 This Agreement shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 including the Commission Implementation Decision of 10th July 2023 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

1.4 Hierarchy

1.4.1 In the event of a contradiction between this Agreement and the provisions of related agreements between the parties existing at the time when this Agreement is agreed or entered into thereafter, this Agreement shall prevail.

2 Agreed terms

The parties agree as follows:

2.1 Definitions and application

2.1.1 In this Agreement the following terms have the meaning set out below:

"Data" means any personal data passed from Customer to the Data Processor including the information listed in Appendix 1 – Data Processing Terms of this Agreement and is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Data Security Incident" a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Data transmitted, stored or otherwise processed.

"Data Subject" means an individual to whom the Data (or relevant part of the Data) relates.

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law'.

"Data Processor" means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

"Data Protection Legislation" shall mean all applicable laws relating to data protection, the processing of personal data and privacy, including: The Danish Data Protection Act 2018. The General Data Protection Regulation (EU) 2016/679 from 25th May 2018 including the Commission Implementation Decision of 10th July 2023; the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and any legislation that, in respect of the United Kingdom, replaces such legislation as a consequence of the United Kingdom leaving the European Union; the California Consumer Privacy Act, CCPA (Assembly Bill No. 375); and any other applicable legislation and regulations in any other country and any modification or re-enactment of such legislation or regulations from time to time.

"Commission Implementation Decision of 10th July 2023" shall mean the Commission Implementation Decision of 10th July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

2.1.2 This Agreement shall apply to all Data supplied by Customer to the Data Processor from the date of this Agreement until either party terminates this Agreement pursuant to Clause 2.6 below.

2.2 Purpose of Processing

2.2.1 The Data Processor shall process the Data it receives from the Customer solely for the purposes of the processing operations as set out in the following and for no other purpose except with the express written consent of the Customer. The purpose of processing the Data is to offload end-users of the Customer to a virtual waiting room e.g. if number of end-users exceeding the Customer's website capacity.

2.3 Security and Confidentiality of Data

2.3.1 The Data Processor shall carry out the Processing in compliance with the Data Protection Legislation.

2.3.2 The Data Processor shall implement (and assist the Customer to implement) technical and organizational measures to safeguard the Data from unauthorized or unlawful Processing or accidental loss, destruction, or damage and confirms that it has implemented appropriate technical and organizational measures to prevent unauthorized or unlawful Processing, accidental loss, destruction, damage or disclosure of the Data.

2.3.3 The Data Processor shall ensure that each of its employees, agents or subcontractors are made aware of its obligations with regard to the security and protection of the Data and shall require that they:

a) enter into binding obligations with the Data Processor in order to maintain an appropriate obligation of confidentiality and the levels of security and protection provided for in this Agreement.

b) Process the Data solely on instructions from Customer; and

c) Is appropriately reliable, qualified and trained in relation to their Processing of Data.

2.3.4 The Data Processor shall not divulge the Data whether directly or indirectly to any person, firm, or company without the written consent of Customer, except to those of its employees who are engaged in the Processing of the Data and are subject to the binding obligations referred in 2.3.3

2.3.5 In the event that the Data Processor subcontracts any part of the Processing to a third party in accordance with 2.3.4 the Data Processor shall ensure that a written contract on the same terms as this Agreement is entered into by the subcontractor and that any subcontractor provides the Data Processor with a

plan of the technical and organizational means it has adopted to prevent unauthorized or unlawful Processing or accidental loss or destruction of the Data. The Data Processor will remain responsible for all acts and omissions of sub-contractor as if they were its own.

2.3.6 The Data Processor will Process the Data only on behalf of Customer and in compliance with Customer's documented instructions and this Agreement or any other written agreement between the parties and if the Data Processor cannot provide such compliance for whatever reason the Data Processor will inform Customer promptly of its inability to comply, in which case Customer shall be entitled to suspend the Processing of the Data and/or terminate this Agreement and the contract to which this Agreement is appended if compliance with this Agreement is not restored within a reasonable time and in any event within one month following suspension.

2.3.7 The Data Processor may not, in any circumstances, transfer any of the Personal Data to any country or territory outside of the European Economic Area without the Customer's prior written consent, which may be withheld at its absolute discretion.

https://queue-it.com/data-processing-agreement-sub-processors/ contains a list of sub processors to the Data Processor. The list will be updated on an ongoing basis via the Suppliers web site and the Customer will be notified prior to the change.

2.3.8 The Data Processor shall notify the Customer without undue delay (and in any event no later than 24 hours) after becoming aware of a reasonably suspected, "near miss" or actual Data Security Incident. Where, and in so far as, it is not possible to provide all the relevant information at the same time, the information may be provided in phases without undue further delay, but the Data Processor may not delay notification on the basis that an investigation is incomplete or ongoing.

2.3.9 The Data Processor shall (if applicable) promptly notify the Customer of and assist the Customer in relation to:

a) Any request for disclosure of the Data by a law enforcement authority unless otherwise prohibited from so notifying;

b) Documenting, reporting or taking measures to address or mitigate any Data Security Incident;

c) Any request received seeking to exercise a Data Subject's rights under the Data Protection Legislation;

d) Conducting privacy impact assessments of any Processing operations and consulting with any applicable supervisory authority or appropriate persons accordingly.

2.3.10 An authorized and individual Data Protection Manager from the Supplier will via the email address privacy@queue-it.com respond to enquiries from either a Data Subject or Customer relating to the Processing of the Data and will deal

promptly and properly with any such enquiries and in any event within the time frames stipulated by the Data Protection Legislation.

2.3.11 The Data Processor will make available to the Customer all information necessary to demonstrate compliance with the obligations set out in this Agreement and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer.

2.3.12 The Data Processor will comply with all reasonable instructions from the Customer to rectify, delete and update any Data or files and will confirm to the Customer within a reasonable time that this has been done.

2.3.13 The Data Processor will comply with the rights of Data Subjects and allow the rights of access, correction, blocking, suppression or deletion as reasonably requested in writing by the Customer.

2.3.14 The Data Processor will not, and will procure that any subcontractors will not, make or permit any announcement in respect of the Data Security Incident to any person without the Customer's prior written consent, which may be given, withheld or made subject to conditions at the Customer's sole discretion.

2.4 Liability

2.4.1 The Data Processor will, to the extent to which it is liable, indemnify the Customer for any loss or damage of whatsoever nature suffered or incurred by the Customer or for any liability of the Customer to any other person for any loss or damage of whatsoever nature suffered or incurred by that person.

2.5 Surviving Obligations

2.5.1 The parties agree that at the termination of the services the Data Processor on request of the Customer shall securely destroy all Personal Data and certify to the Customer that it has been done so (in each case as requested by the Customer).

2.5.2 In the event that legislation imposed upon the Data Processor prevents it from destroying whole or part of the Personal Data in accordance with clause 2.5.1 the Data Processor warrants that it shall guarantee the confidentiality and security of the Personal Data and shall hold the Data only for the purposes mandated by legislation and in accordance with this Agreement.

2.5.3 The Data Processor warrants that upon request of Customer and/or of the Information Commissioner it shall submit its Data Processing facilities for audit of the above-mentioned measures.

2.6 Termination

2.6.1 Subject to clause 2.6.5 below this Agreement will terminate when the Customers agreement with the Supplier terminates.

2.6.2 The Customer shall be entitled to terminate this Agreement and the contract to which this Agreement is appended insofar as it concerns processing of personal data in accordance with this Agreement if:

a) the Data Processor is in substantial or persistent breach of this Agreement or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, or

b) the Data Processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to this Agreement or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

2.6.3 The Data Processor shall be entitled to terminate this Agreement and the contract to which this Agreement is appended insofar as it concerns processing of personal data under this Agreement where, after having informed the Customers that its instructions infringe applicable legal requirements, the Customer insists on compliance with the instructions.

2.6.4 Following termination of this Agreement, the Data Processor shall, at the choice of the Customer, delete all personal data processed on behalf of the Customer and certify to the Customer that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with this Agreement.

2.6.5 Notwithstanding termination, the provisions of clause 2.3 shall survive the termination of this Agreement and shall continue in full force and effect until the Data Processor has complied in full with the provisions of clauses 2.5.1 and 2.5.2 above.

3 Appendix

3.1 Appendix 1 - Data Processing Terms

3.1.1 Background:

a) These Data Processing Terms set out contractual provisions to ensure the protection and security of data passed from the Customer to the Data Processor for processing.

b) The Data Protection Legislation place certain obligations upon a Data Controller to ensure that any data processor it engages provides sufficient guarantees to ensure that the processing of the data carried out on its behalf is secure and legal.

c) These Data Processing Terms exists to ensure that there are sufficient security guarantees in place and that the processing complies with the Data Protection Legislation.

3.1.2 The personal data related to actual and/or potential customers / end-users of Customer passing through the Data Processors systems.

a) IP-address and userAgent from the end-user's device / browser is the categories of personal data being processed. The IP address is only used for logging purposes, preventing unauthorized access, malicious code distribution, stopping 'denial of service' attacks and the systems build-in feature that prevent malicious activity from single IP addresses (bots etc.). IP-address and userAgent will be deleted after 12 months.

b) Email address of end-user if the Data Processor's optional Identity feature is used by the Customer and such emails is processed by the Data Processor on behalf of the Customer. Email addresses will be deleted after 3 months.

c) Email address of end-user if the Data Processor's optional Notification feature is used by the Customer. Email address of end-user will only be handed over to the Customer if consent is given from end-user. Email addresses will be deleted after 3 months.

3.1.3 The Data will be processed in connection with the processing operations during the term of this Agreement or such shorter period where the processing is no longer authorized, and in respect of any post-termination processing activities permitted by the Customer from time to time.

3.1.4 the Data Processor will not store sensitive personal data (cf. Article 9 of the General Data Protection Regulation):

a) Racial or ethnic origin

b) Political opinions

c) Religious beliefs

d) Philosophical beliefs

e) Trade union membership

f) Data concerning health including abuse of medicine, narcotics, alcohol etc.

g) Data concerning sex life or sexual orientation

3.1.5 the Data Processor will not store Data on purely private matters of individuals (cf. section 8 of the Danish Personal Data Act, as of 25 May 2018, cf. Articles 6 and 9 of the General Data Protection Regulation):

a) Criminal offences

b) Significant social problems

c) Other purely private matters, which are not mentioned above.