Data Processing Agreement

Holvi Payment Services Ltd
Published: 1 October 2022
Version: 2.0

1. Scope

1.1. This Data Processing Agreement ('DPA') is part of Holvi's Terms of Service between the Customer and Holvi Payment Services Ltd ('Holvi'), or any other agreement governing the Customer's use of Holvi's services when Holvi processes Personal Data on behalf of the Customer. The DPA is agreed in order to meet the requirements of the General Data Protection Regulation ('GDPR') and to protect the Data Subject's rights between the Customer ('Data Controller') and Holvi ('Data Processor').

1.2. The DPA has been designed to ensure the parties' compliance with Article 28 (3) of GDPR.

1.3. The DPA sets out the rights and obligations of the Data Controller and the Data Processor when processing Personal Data on behalf of the Data Controller, and is in force as long as the Customer continues to use these services.

1.4. In the context of providing the agreed services, the Data Processor will process Personal Data on behalf of the Data Controller in accordance with the DPA.

1.5. The DPA shall take priority over any similar provisions contained in other agreements between the parties.

1.6. The DPA does not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to GDPR or other legislation.

2. Definitions

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 of personal data.

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

Data Subject: A natural person about whom a controller holds personal data and who can be identified, directly or indirectly, by reference to that personal data.

Data Transfer: An intentional sending of personal data to another party or making the data accessible by it, where neither sender nor recipient is a data subject.

EU: European Union.

EEA: European Economic Area.

General Data Protection Regulation: Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of

personal data and on the free movement of such data and repealing Directive 95/46/EC ('GDPR').

Member State: A state that is a member of the European Union.

Personal Data: Any information relating to an identified or identifiable natural person ('Data Subject').

Personal Data Breach: 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.

Sub-Processor: A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, is authorised to process personal data.

Supervisory Authority: An independent public authority which is established by a Member State.

Terms of Service: The terms of service by Holvi Payment Services Ltd.

3. Rights and obligations of the Data Controller

3.1. The Data Controller is responsible for ensuring that the processing of Personal Data complies with GDPR according to Article 24 of GDPR and with the applicable EU, EEA or Member State data protection law and the DPA.

3.2. The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of Personal Data.

3.3. The Data Controller shall be responsible, among other things, for ensuring that the processing of Personal Data, which the Data Processor is instructed to perform, has a legal basis.

4. Basis for processing and processing according to instructions

4.1. The Data Processor will always process Personal Data (including Customers' Data) in accordance with GDPR, the applicable EU, EEA or Member State data protection law, and the agreements between Holvi and the Customer.

4.2. The Data Processor shall process Personal Data only according to the instructions from the Data Controller, unless required to do so by the EU, EEA or Member State law to which the Data Processor is subject. Subsequent instructions can also be given by the Data Controller throughout the duration of the processing of Personal Data, but such instructions must always be documented and kept in writing, including electronically, in connection with the DPA.

4.3. The Data Processor shall immediately inform the Data Controller if instructions given by the Data Controller, in the opinion of the Data Processor, contravene GDPR or the applicable EU, EEA or Member State data protection law.

5. Categories of Personal Data processed

5.1. The Personal Data that the Data Processor processes on behalf of the Data Controller includes the information that the Customer transfers to Holvi and Holvi collects on behalf of the Customer (including Customers' Data). Data types may be further specified in the respective service descriptions.

5.2. The purpose of the Data Processor's processing of Personal Data on behalf of the Data Controller is to enable the Data Controller to make appropriate use of the services provided as described in the agreement entered into by the Data Processor as supplier and the Data Controller as Customer.

5.3. The processing of Personal Data which the Data Processor does on behalf of the Controller is to make Holvi's services and related value-added services available for the Data Subjects of the Controller.

5.4. Processing includes the following category of Data Subject: Customer's customers who use the Holvi value-added services. Typically, these Data Subjects will engage with the Customer via Holvi's value-added services (e.g. Web Shop).

5.5. To develop the product in accordance with users' needs and ensure safe and non-abusive usage, the technical performance and security of the product, and to bill customers correctly based on their usage, the Data Processor needs to track certain usage information about users' navigation in the product. As the Data Processor determines the scope and purpose of this usage information, it is the Data Processor who will be the Data Controller for this information. The individual user will be the Data Subject. The processing of this information will be governed by Holvi's Privacy Policy and the user will retain all their rights under GDPR.

5.6. Both parties acknowledge that Holvi will be the Data Controller for other processing activities as described in Holvi's Privacy Policy and Terms of Service, including, but not limited to, transmission of communication, fault and error detection and handling, security, developing the service, provision of customer support, billing, user activation and engagement, marketing and sales activities of Holvi.

5.7. Personal Data that the Data Processor processes for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Security and confidentiality

6.1. Article 32 of GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

6.2. The Data Controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

a. Pseudonymisation and encryption of Personal Data

b. The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services

c. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident

d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

6.3. According to Article 32 of GDPR, the Data Processor shall also – independently from the Data Controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Data Controller shall provide the Data Processor with all information necessary to identify and evaluate such risks.

6.4. The Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to Article 32 of GDPR by, among other things, providing the Data Controller with information on the technical and organisational measures already implemented by the Data Processor pursuant to Article 32 of GDPR and any other information required by the Data Controller, taking into account the information available to the Processor and the Controller being unable to carry out those measures without the Processor's assistance.

6.5. The Data Processor shall only grant access to the Personal Data being processed on behalf of the Data Controller to persons under the Data Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis.

6.6. The Processor's employees are committed to confidentiality when processing the Controller's data, and the Processor has taken appropriate technical and organisational measures to ensure the security of processing.

6.7. The Data Processor shall, in any event and at a minimum, design the service and the routines of the Data Processor to have a high level of security and prevent any breaches. Testing is integrated in the development process, and a system for continuous deployment with automated tests running before deployment is in place.

7. Use of sub-processors

7.1. To provide Holvi's services and other value-added services for the Data Controller, the Data Controller accepts that the Data Processor may engage sub-processors. On commencement of the DPA, the Data Controller authorises the engagement of the following sub-processors, the list of which can be found here.

7.2. The Data Processor has the Data Controller's general authorisation for the engagement of sub-processors. The Data Processor shall inform in writing the Data Controller of any intended changes concerning the addition or replacement of sub-processors at least two (2) months in advance, thereby giving the Data Controller the opportunity to object to such changes and terminate the DPA with the Data Processor prior to the engagement of the concerned sub-processor(s), provided that the Controller has substantial and documented reasons for such objection.

7.3. Where the Data Processor engages a sub-processor for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in the DPA shall be imposed on that sub-processor by way of a contract or other legal act under EU, EEA or Member

State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the DPA and GDPR.

7.4. A copy of such a sub-processor agreement clause and subsequent amendments shall – at the Data Controller's request – be submitted to the Data Controller, thereby giving the Data Controller the opportunity to ensure that the same data protection obligations as set out in the DPA are imposed on the sub-processor. Provisions on business related issues that do not affect the legal data protection content of the sub-processor agreement, do not require submission to the Data Controller.

7.5. If the sub-processor does not fulfil their data protection obligations, the Data Processor shall remain liable to the Data Controller in regards to the fulfilment of the obligations of the sub-processor. This does not affect the rights of the Data Subjects under GDPR – in particular those foreseen in Articles 79 and 82 of GDPR – against the Data Controller and the Data Processor, including the sub-processor.

8. Co-operation

8.1. Taking into account the nature of the processing, the Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Data Controller's obligations to respond to requests for exercising the Data Subject's rights laid down in Chapter 3 of GDPR.

8.2. This entails that the Data Processor shall, insofar as this is possible, assist the Data Controller in the Data Controller's compliance with:

a. The right to be informed when collecting Personal Data from the Data Subject
b. The right to be informed when Personal Data have not been obtained from the Data Subject
c. The right of access by the Data Subject
d. The right to rectification
e. The right to erasure ('the right to be forgotten')
f. The right to restriction of processing
g. Notification obligation regarding rectification or erasure of Personal Data or restriction of processing
h. The right to data portability
i. The right to object
j. The right not to be subject to a decision based solely on automated processing, including profiling

8.3. In addition to the Data Processor's obligation to assist the Data Controller pursuant to Clause 6.4, the Data Processor shall, taking into account the nature of the processing and the information available to the Data Processor, assist the Data Controller in ensuring compliance with:

a. The Data Controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Personal Data Breach to the competent Supervisory Authority, the Finnish Data Protection Authority, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons

b. The Data Controller's obligation to without undue delay communicate the Personal Data

Breach to the Data Subject, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons

c. The Data Controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data (a data protection impact assessment)

d. The Data Controller's obligation to consult the competent Supervisory Authority, the Finnish Data Protection Authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk

9. Deletion and return of the data

9.1. On termination of the provision of Personal Data Processing Services, the Data Processor shall delete all Personal Data processed on behalf of the Data Controller, unless otherwise required by law.

9.2. On termination of the provision of Personal Data Processing Services, the Data Processor shall be under obligation to return all the Personal Data to the Data Controller and delete existing copies (if applicable) unless EU, EEA or Member State law requires storage of the Personal Data.

9.3. The Customer acknowledges and accepts that Holvi processes some of the data also in the capacity of a Data Controller, and such data is retained by Holvi in accordance with Holvi's Privacy Policy.

10. Transfer of data

10.1. Any transfer of Personal Data to third countries or international organisations by the Data Processor shall only occur on the basis of documented instructions from the Data Controller and must always take place in compliance with Chapter 5 of GDPR.

10.2. In case transfers to third countries or international organisations, which the Data Processor has not been instructed to perform by the Data Controller, are required under EU, EEA or Member State law to which the Data Processor is subject, the Data Processor shall inform the Data Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

10.3. The DPA shall not be confused with standard data protection clauses within the meaning of Article 46 (2) (c) and (d) of GDPR, and the DPA cannot be relied upon by the parties as a transfer tool under Chapter 5 of GDPR.

11. Notification of Personal Data breach

11.1. In case of any Personal Data breach, the Data Processor shall, without undue delay after having become aware of it, notify the Data Controller of the Personal Data breach.

11.2. The Data Processor shall notify the Data Controller without undue delay upon becoming aware of and confirming the Personal Data breach, but no later than 72 hours, where feasible, in order to enable the Data Controller to comply with its obligation to notify the Personal Data breach to the competent Supervisory Authority pursuant to Article 33 of GDPR.

11.3. In accordance with Clause 8.3 a) of this DPA, the Data Processor shall assist the Data Controller in notifying the Personal Data Breach to the competent Supervisory Authority, meaning that the Data Processor is required to assist in obtaining the information listed below which, pursuant to Article 33 (3) of GDPR, shall be stated in the Data Controller's notification to the competent Supervisory Authority:

a. The nature of the Personal Data including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned

b. The likely consequences of the Personal Data breach

c. The measures taken or proposed to be taken by the Controller to address the Personal Data breach including, where appropriate, measures to mitigate its possible adverse effects

12. Audit and inspection

12.1. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of GDPR and the DPA and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

12.2. The Data Processor and the Controller shall cover their own costs with regard to any audit. If the Controller requests the use of an external auditor, the Controller shall cover the costs of use of such an auditor and any costs related to or incurred by such an audit.

13. Amendments

13.1. The Data Processor may amend this DPA and any supplemental documentation at any time when deemed necessary. The amendments shall be notified to the Data Controller electronically. The amendments enter into force on the date set out in the notice, however, at the earliest two (2) months from the date of the notification.

13.2. Where an amendment to the DPA or any supplemental documentation is required by law the amendment may be made without prior notice to the Data Controller and shall be effective immediately.

13.3. If any provision or provisions of this DPA are held to be invalid, illegal, or unenforceable the Data Processor will not rely on that part and make adequate changes as soon as reasonably practical to fully comply. The corresponding term(s) will be amended accordingly.

14. Other provisions

14.1. For the sake of clarity, what is agreed on limitations of liability, communication and governing law and venue on the Terms of Service apply also to this DPA accordingly.

14.2. The parties may agree on other clauses concerning the provision of the Personal Data Processing Service specifying e.g. liability, as long as they do not contradict directly or indirectly the DPA or prejudice the fundamental rights or freedoms of the Data Subject and the protection afforded by

GDPR. These are to be made separately and in writing.

14.3. The DPA shall apply for the duration of the provision of Personal Data Processing Services, and cannot be terminated unless another DPA governing the provision of Personal Data Processing Services has been agreed upon between the parties.