mollie

DATA PROCESSING AGREEMENT

This **DATA PROCESSING AGREEMENT** (hereinafter "**DPA**") including its appendices describes the Parties' obligations, including under applicable data protection laws, with respect to the processing of personal data (as defined below). The DPA is incorporated into the User Agreement.

This DPA is between Organisation (hereinafter "**Controller**")

and

Mollie B.V., a limited liability company (*besloten vennootschap)* having its registered seat in Amsterdam, at Keizersgracht 126, 1015 CW Amsterdam, the Netherlands and registered at the Dutch Chamber of Commerce under number 30204462, (hereinafter "**Mollie**" or "**Processor**")

and

Mollie UK Ltd., a limited liability company having its registered seat in London, 7 Pancras Square, London N1C 4AG, the United Kingdom and registered at the Companies House under number 14013554, (hereinafter "**Mollie**" or "**Processor**"),

each a "**Party**" and jointly "**Parties**".

Definitions

In this DPA, the following terms have the meaning as set forth below. Capitalised terms used but not defined herein shall have the meaning set forth in the Agreement.

Agreement	the agreement between Controller and Processor for the provision of services ("**User Agreement**").
Binding Corporate Rules	personal data protection policies which are adhered to by a controller or processor established in the territory of a Member State for transfers or a set of transfers of Personal Data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.
Controller	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the Processing of Personal Data.
Customer	Customers of Organisation who wish to pay for products and/or services provided by Organisation through Mollie's Payment Module.
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.
Data Processing Agreement	this agreement, including all attachments.
Supervisory Authority	an independent government body responsible for supervising compliance with the applicable laws relating to the Processing of Personal Data. In the Netherlands, this is the *Autoriteit Persoonsgegevens*.
Data Protection Impact Assessment	an assessment of the impact of the envisaged processing operations on the protection of Personal Data.
Data Protection Laws	all applicable legislation relating to data protection and privacy including, without limitation, the EU General Data Protection Regulation, all local laws and regulations which amend or replace any

	of them, together with any national implementing laws in any Member State of the European Economic Area (EEA), to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time.
Data Subject	the natural person to whom Personal Data relates (e.g. Customers).
GDPR	the General Data Protection Regulation (EU) 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.
Personal Data	any information relating to an identified or identifiable natural person; 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 the natural person.
Processing	any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. This list is not exhaustive. The terms "process", "processes" and "processed" will be construed accordingly.
Processor	a natural or legal person, public authority, agency or other body which Processes (Personal) Data on behalf of the Controller.
Organisation	the organisation that uses the Payment Module of Mollie for purposes including, but not limited to, the sale of products and/or services to Customers.
Standard Contractual Clauses	European Commission Standard Contractual Clauses for Data Processors (2010/87/EU) or Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (C/2021/3972).
Sub-processor	any third person, entity or company engaged by Processor to process Personal Data in the provision of the services under the Agreement.

SECTION A PURPOSE

Article A.1 Scope

Processor has agreed to provide services to Controller in accordance with the terms of the User Agreement. In providing services, Processor will Process Personal Data on behalf of Controller as identified in this DPA. Processor, as a financial institution, also processes Personal Data acting as a data controller.

Parties acknowledge and agree that to the extent Mollie processes Personal Data involved in payment transactions to: i) execute the User Agreement with Controller; ii) monitor, prevent and detect fraudulent payment transactions; iii) comply with legal or regulatory obligations applicable to the processing and retention of payment data to which Mollie is subject, including applicable anti- money laundering screening and compliance with know-your-customer obligations; and iv) improve Mollie's products and services, Mollie is acting as a data controller and has the sole and exclusive authority to determine the purposes and means of the processing of Personal Data it receives from or through (providing services to) Controller.

The processing activities, Personal Data and categories of Data Subjects for which Processor processes Personal Data on behalf of Controller are identified in Annex A.

SECTION B OBLIGATIONS

Article B.1 Controller Obligations

Controller is responsible for the Personal Data which Processor will Process and shall ensure compliance with all Data Protection Laws, including requirements pertaining to the transfer of the Personal Data under this DPA and the User Agreement. Controller warrants to have the right to Process the Personal Data and possesses the right to appoint Processor, to Process the data on behalf of Controller.

Controller agrees that, without limitation of Processor's obligations under this DPA, Controller is solely responsible for its use of the services, including (a) making appropriate use of the services to ensure a level of security appropriate to the risk in respect of the Personal Data; (b) securing the account authentication credentials, systems and devices Controller uses to access the services; (c) securing Controller's systems and devices that it uses with the services; and (d) maintaining its own backups of Personal Data.

Article B.2 Processor Obligations

Processor undertakes to:

(a) process the Personal Data only in accordance with documented instructions from Controller and shall take necessary steps to ensure that any natural person acting under its authority who has access to Personal Data does not Process the Personal Data except upon instructions from Controller;
(b) promptly inform Controller if any of the instructions regarding the Processing of Personal Data provided to Processor by Controller, breach any applicable Data Protection Laws or the provisions set out in this DPA;
(c) implement appropriate technical and organisational procedures to protect Personal Data, considering 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; and
(d) without undue delay inform Controller if it receives a complaint or request relating to either Party's obligations under Data Protection Laws relevant to this DPA, including any compensation claim from a Data Subject or any notice, investigation or other action from a Supervisory Authority and provide Controller with full details of such investigation, complaint or request unless not permitted by law or by request of the Supervisory Authority.

SECTION C TRANSFERS AND SUB-PROCESSORS

Article C.1 Transfer of Personal Data

Where Personal Data relating to an EU Data Subject is transferred outside of the EEA, it shall be processed by an entity: (i) located in a third country or territory recognised by the EU Commission as having an adequate level of protection; or (ii) that is subject to EU Standard Contractual Clauses and/or UK International Data Transfer Agreement or UK SCC's Addendum; or (iii) that has other legally recognised appropriate safeguards in place, such as the Binding Corporate Rules, which guarantee the same level of protection and safeguards as this DPA.

Article C.2 Sub-processors

Controller hereby consents to Processor's use of Sub-processors specified in Annex B. This list may be updated by Processor from time to time in accordance with this DPA.

Processor will provide Controller the possibility to object to each new Sub-processor that will be involved solely for the scope of the data processing activities as identified in Annex A.

Prior to engaging a new Sub-processor, Processor shall notify Controller thereof and provide Controller at least ten (10) calendar days to object, except where Processor reasonably believes engaging a new Sub-processor on an expedited basis is necessary to protect the confidentiality, integrity or availability of the Personal Data or avoid material disruption to the services provided. In that case, Processor will give such notice as soon as reasonably practicable. If, within five (5) calendar days after such notice, Controller notifies Processor in writing that Controller objects to Processor's appointment of a new Sub-processor based on reasonable data protection concerns, the parties will discuss such concerns in good faith and whether they can be resolved. Objections to new Sub-processors shall be submitted to privacy@mollie.com.

Controller acknowledges that Sub-processors are essential to provide the services and that objecting to the use of a Sub-processor may prevent Processor from offering the services to Controller. If the parties are not able to mutually agree to a resolution of such concerns, Controller, as its sole and exclusive remedy, may terminate the DPA for convenience.

All Sub-processors who process Personal Data in the provision of services to Controller shall comply with the obligations set out in this DPA. Processor shall, prior to disclosure of Personal Data to any Sub-processor, carry out adequate due diligence to ensure that the Sub-processor is capable of providing the level of protection for Controller

Personal Data required by this DPA and enter into an agreement with that Sub-processor under which the Sub-processor agrees to comply with the obligations equivalent to those set out in this DPA.

SECTION D SECURITY

Article D.1 Security measures

Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(i) the pseudonymisation and encryption of Personal Data;
(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing. In assessing the appropriate

level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

Article D.2 Data Breach notification

Processor shall notify Controller without undue delay of any accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to Personal Data after discovery, insofar the Data Breach is only related to the processing of Personal Data by Processor in its capacity as a processor. If and where the Data Breach concerns Personal Data for which Processor is deemed Controller as described in Processor's Privacy Statement, Processor reserves the right to treat the Data Breach as a controller.

A delay in giving a Data Breach notice requested by law enforcement and/or in light of Processor's legitimate needs to investigate or remediate the matter before providing notice shall not constitute an undue delay. Such notices will describe, to the extent possible, details of the Data Breach, including steps taken to mitigate the potential risks. Without prejudice to Processor's obligations under this Section D.1, Controller is solely responsible for complying with Data Breach notification laws applicable to Controller and fulfilling any third party notification obligations related to any Data Breaches. Processor's notification of or response to a Data Breach under this Section D.1. will not be construed as an acknowledgement by Processor of any fault or liability with respect to the Data Breach.

Any costs incurred in resolving the Data Breach and in implementation of measures necessary to prevent such a Data Breach in the future will be borne by the Party who incurs the costs.

SECTION E AUDIT

Article E.1 Right to Audit

Controller shall have the right to request, upon reasonable notice, audit reports from Processor pertaining to the Processing of Personal Data within the scope of the services provided under this DPA.

Audit reports, as referenced in this clause, shall include but not be limited to, reports related to the security, confidentiality, and data protection measures implemented by Processor in connection with the Processing of Personal Data. These reports may also cover compliance with relevant Data Protection Laws.

Requests for audit reports shall be made in writing and sent to privacy@mollie.com, specifying the scope and purpose of the request. Processor shall acknowledge the receipt of such requests in a timely manner.

The receipt of audit reports shall be subject to professional duty of confidentiality. Controller may use the audit reports only for the purposes of meeting Controller's regulatory audit requirements and confirming that Processor's Processing of Personal Data complies with this DPA. The audit reports shall not be shared externally.

SECTION F DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATIONS

Article F.1 Assistance

Processor shall assist Controller with undertaking an assessment of the impact of Processing Personal Data (article 35 GDPR) and with any consultations with a Supervisory Authority (article 36 GDPR), if and to the extent an assessment or consultation is required to be carried out under Data Protection Laws and where Processor is allowed and/or required to cooperate.

SECTION G DATA SUBJECT RIGHTS

Article G.1 Assistance

If Processor receives a request from a Data Subject in relation to Controller Personal Data, Processor will advise the Data Subject to submit their request to Controller and/or forward the request to Controller, and Controller will be responsible for responding to any such request.

Upon Controller's request and at Controller's expense, Processor will provide Controller with such assistance as it may reasonably require to comply with obligations under Data Protection Laws to respond to requests from data subjects to exercise their rights under Data Protection Laws (e.g. rights of data access, rectification, erasure, restriction, portability and objection) in cases where Controller cannot reasonably fulfil such requests independently via its access to Processor's products and services.

SECTION H MISCELLANEOUS

Article H.1 Confidentiality

Processor shall keep confidential all Personal Data and shall ensure that all employees, agents, officers and contractors having access to or being involved with the Processing of Personal Data are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential and is informed of and complies with the obligations of this DPA.

Article H.2 Liability

Any and all liability arising out of this DPA will be governed by the relevant provisions of the User Agreement, including limitations of liability.

Notwithstanding the provisions of the User Agreement, each Party shall only be liable to the other Party for any damages it causes the other Party by any breach of this DPA. These damages shall be clearly demonstrated. Processor will only be liable for the damage caused by the processing where it has not complied with obligations of Data Protection Laws specifically directed to data processors or where it has acted outside of or contrary to Controller's lawful instructions as described in this DPA. In that context, Processor will only be liable if Controller proves that Processor is responsible for the event giving rise to the damage.

Controller shall be solely liable to the Data Subject, and the Data Subject shall be entitled to receive compensation, for any material or non-material damages Controller or Processor (or its Sub-processor(s)) causes the Data Subject by breaching this DPA.

Article H.3 Term and Termination

The term of this DPA shall coincide with the commencement of the User Agreement and/or use of the specific product or service as included in Annex A.

This DPA shall terminate automatically together with termination of the User Agreement and/or use of the specific product or service as included in Annex A, whichever is terminated first.

Upon termination of this DPA, Processor shall, upon Controller's request, return the Personal Data to Controller or to a Processor nominated by Controller, or delete the Personal Data, unless Processor is required to retain a copy in accordance with any law of the European Union or any member state of the European Union.

SECTION I FINAL PROVISIONS

Article I.1 Entire Agreement

This DPA constitutes a part of the User Agreement. All rights and obligations stemming from the User Agreement are also applicable to this DPA. Annex A constitutes an integral part of this DPA.

Article I.2 Amendment by Agreement only

No variation of this DPA shall be valid unless it is in writing and signed by authorised representatives of each Party.

Article I.3 Severability

Each of the provisions in this DPA are distinct and severable, and if any provision, or part of a provision is held unenforceable, illegal or void in whole or in part by any court, regulatory authority or other competent authority, it shall to that extent be deemed not to be part of this DPA and the enforceability, legality and validity of the remainder of this DPA will not be affected. Parties agree to attempt to substitute for any invalid or unenforceable provision a valid or enforceable provision which achieves to the greatest extent possible the same effect as would

have been achieved by the invalid or unenforceable provision. Except for amendments implemented by this DPA, the User Agreement remains unchanged and in full force and effect.

Article I.4 Right of Assignment
Parties may only transfer this DPA in line with the User Agreement (clause 8.9).

Article I.5 Governing Law
This DPA shall be governed by and interpreted in accordance with the laws of the Netherlands. Each Party consents to the exclusive jurisdiction of the courts of Amsterdam to settle any disputes arising from this DPA. Should any court or administrative body of competent jurisdiction find any provision of this DPA to be\invalid, unenforceable or illegal, the other provisions of this DPA shall remain in full force and effect.

ANNEX A - SPECIFICATION OF PROCESSING PERSONAL DATA

1. PURPOSE OF THE PROCESSING

Processing of Personal Data is directly related to the provision of the services provided under the User Agreement.

The purposes of the processing are:

- Facilitating sending invoices to Controller's Customers via Mollie's products and services

2. CATEGORIES OF DATA SUBJECTS

Processor will Process Personal Data of the following categories of Data Subjects for Controller:

- Customers of Controller (i.e. the payer (consumers, business customers))

3. TYPES OF PERSONAL DATA

Processor will Process the following types of Personal Data for Controller:

- Basic contact details (includes full name, (office) phone number, (business) email address, residential/company address)
- Invoice details (as included by Controller)

No special categories of Personal Data (as defined by article 9 the GDPR) will be processed by Processor.

4. SECURITY MEASURES

Context

As a financial institution, the security controls and operating procedures Mollie has created for our applications, systems and IT processes are subject to review by the Dutch Central Bank (DNB), which in turn uses guidance from the European Banking Authority (EBA) for technical standards licence holders should adhere to.

Furthermore, as Mollie (also) operates as a controller of personal data, Mollie is regulated by other legislation setting standards for security and data protection as well, enforced by additional authorities - notably the GDPR and its regulator within the Netherlands (Autoriteit Persoonsgegevens).

Additionally, the systems processing card data specifically are level 1 PCI DSS compliant systems, which means that this particular application and the procedures for developing and maintaining it are subject to the data protection measures outlined by the PCI Council, the compliance to which Mollie is assessed by an external party yearly.

General Measures

All applications, systems and procedures relating to them are subject to the Mollie Information Security Policy. Highlights from this and other policies that are relevant for the scope of provided services are:

- Employee screening
- Developer's security training program
- Security awareness program
- Segregation of duties
- Change management
- Vulnerability management
- Incident management
- Resilience and backup management
- Strong access control enforcement (IAM and IGA)
- User authorization reviews
- System classification standards
- Data classification standards and data policy
- Secure configuration standards based on industry best practices, policy enforcement (hardening)
- Physical and logical network environment segregation
- Secure encryption standards
- Encryption key management
- Encryption (in transit, in rest for shared infrastructure environments such as cloud)
- Third party risk management

- Availability and error monitoring
- Secure development life cycle
    - Threat modelling on significant changes and new features
    - Dependency management and known vulnerability scanning
    - Static code security analysis
    - Internal and external vulnerability scanning
- Coordinated vulnerability disclosure (CVD) and bug bounty program
- Threat intelligence program (e.g. participation in the Dutch PI-ISAC, payment institution information sharing and analysis centre, dark web monitoring)
- Managed security service provider (MSSP) collaboration for security operations, analysis and forensic investigations
- Security Information and Event Management (SIEM)
- Staff endpoint security
- Email security

Mollie Platform

In addition to the general security measures outlined above, the Mollie Platform application is covered by the following security measures - either resulting from the implementation of our general security policies or as a mitigating measure to address a risk recognized in the application specific risk assessment:

- 2-Factor access control
- Third-party penetration tests
- Security incident event management
- DDoS mitigation
- Security incident response
- Availability monitoring
- Secure credential storage
- Redundant infrastructure
- Disaster recovery failover
- Rate limiting and locking
- Strict Content-Security-Policy
- Captcha
- Web application firewall

ANNEX B - OVERVIEW OF SUB-PROCESSORS

Name sub-processor	**Location**	**Transfer mechanism**	**Purpose**	**Personal data processed**
Monite	Germany	n/a	Email processing	Basic contact details (includes full name, (office) phone number, (business) email address)
Google Cloud Platform	EU (Belgium, The Netherlands, Germany and Finland)	n/a	Public cloud hosting of Mollie dashboard	Basic contact details (includes full name, (office) phone number, (business) email address)