Mynt

Data processing agreement

Table of contents

1. Definitions

Adequate Country

Means a country or territory that is recognized under European Data Protection Laws as providing adequate protection for Personal Data.

Affiliate

Means an entity that directly or indirectly Controls, is Controlled by, or is under common Control with an entity.

Agreement

Means Mynt's Terms and Conditions of Use, which governs the provision of the Services to Customer, as such terms may be updated by Mynt from time to time.

Applicable Data Protection Laws

Means any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction which relates to the protection of individuals with regard to the Processing of Personal Data to which a party is subject, including but not limited to; the GDPR, UK GDPR and the UK Data Protection Act 2018 and (b) any code of practice or guidance published by the ICO or other applicable Regulator or the European Data Protection Board.

Control

Means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" shall be construed accordingly.

Customer Data

Means any Personal Data that Mynt processes on behalf of Customer as a Processor in the course of providing Services, as more particularly described in this DPA.

Controller

Means an entity that determines the purposes and means of the processing of Personal Data.

Data Subject

Means the identified or identifiable natural person who is the subject of Personal Data.

Data Protection Laws

Means all laws and regulations of the European Union, the European Economic Area, their member states, and the United Kingdom applicable to the processing of Personal Data under the Main Agreement (including, where applicable, (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "EU GDPR"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (the "UK GDPR"); (iii) the e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii), (iii), (iv).

EEA

Means, for the purposes of this DPA, the European Economic Area.

Mynt

Means Mynt AB, org. nr. 559100-8874.

Personal Data

Means any information relating to an identified or identifiable natural person (Data Subject) as defined in Article 4(1) of the GDPR where such data is Customer Data.

Processor

Means an entity that processes Personal Data on behalf of a Controller.

Processing

Means any operation or set of operations performed on 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, and “Process”, “Processes” and “Processed” shall be construed accordingly.

Security Incident

Means any unauthorised or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Customer Data.

Services

Means any product or service provided by Mynt to Customer pursuant to the Terms and Condition of Use.

Standard Contractual Clauses

Means contractual clauses annexed to the European Commission's Implementing Decision 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.

Sub-processor

Means any Processor engaged by Mynt or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Terms and Condition of Use or this DPA. Sub-processors may include third parties or Mynt’s affiliates.

Supervisory Authority

Means any independent public authority responsible for monitoring the application of the Data Protection Laws, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing and to facilitate the free flow of personal data within the EU and the UK or else (as applicable).

UK Addendum

Means the International Data Transfer Addendum (Version B1.0) issued by the Information Commissioner's Office under s.119 (A) of the UK Data Protection Act 2018, as updated or amended from time to time.

2. DPA execution and applicability

2.1 Execution. The DPA shall be deemed executed at the same time as the execution of the Agreement. By executing the DPA, the Customer enters into this agreement on behalf of itself and its Affiliates.

2.2 Scope. This DPA applies to Mynt's processing of Personal Data under the Agreement for the provision of services rendered to the Customer.

2.3 Integral document. This DPA is an addendum to and forms an integral part of the Agreement.

3. Relationship to the Agreement

3.1 Priority of terms. Except for the changes made by this DPA, the Agreement remains in full force. If there is a conflict, this DPA shall prevail regarding data protection matters.

3.2 Limitation of liability. Any claims brought under this DPA shall be subject to the exclusions and limitations set forth in the Agreement.

3.3 Governance and jurisdiction. This DPA is governed by the laws and jurisdiction specified in the Agreement unless required otherwise by Applicable Data Protection Laws.

3.4 Termination. This DPA terminates upon expiration of the Agreement. Certain obligations, such as those related to AML and accounting laws, extend beyond termination.

4. Roles and responsibilities

4.1 Standard roles. The Customer acts as the Controller of the Customer Data, and Mynt acts as the Processor.

4.2 Multiple roles. Where the Customer acts as a processor for a third-party controller, Mynt acts as a sub-processor, and the Customer warrants its instructions are authorised by the relevant controller.

4.3 Joint Controllership disclaimer. The parties acknowledge that Mynt may act as a Joint Controller with third-party partners (e.g., Visa for "Click to Pay"). Such processing is governed by the Mynt Privacy Statement and relevant Data Processing Agreements and falls outside the scope of this DPA.

4.4 Privacy statement integration. The Parties acknowledge that Mynt processes certain Personal Data in the capacity of a Controller (as described in the Mynt Privacy Statement), including but not limited to data processed for identity verification, credit assessments, and compliance with Anti-Money Laundering (AML) and accounting legislation. Such data is expressly excluded from the definition of 'Customer Data' under this DPA, and the Customer shall have no right to issue instructions regarding such processing.

5. Scope of processing and instructions

5.1 Compliance. Customer shall comply with its obligations as a Controller and ensure it has obtained all necessary consents for Mynt to process Customer Data.

5.2 Documented instructions. Mynt shall process Customer Data only in accordance with Customer's documented lawful instructions.

5.3 Authorised purpose. These instructions authorise Mynt to process Customer Data to perform its obligations, including expense management, receipt handling and accounting integration.

5.4 Notification of infringement. Mynt shall immediately inform the Customer if an instruction violates the GDPR or other data protection provisions

6. Sub-processing

6.1 Authorisation. Customer expressly authorises Mynt to engage sub-processors to assist in fulfilling its obligations.

6.2 A list of Mynt's sub-processors. For the purpose of the authorisation in Section 6.1, Mynt shall make available to the Customer the current list of sub-processors for the Services. This list, including the sub-processors' specific functions and the location of the processing of Personal Data, is available at Mynt’s Security Center on the website and may be updated by Mynt from time to time in accordance with the terms set forth in this Agreement.

6.3 Contractual safeguards. Mynt shall enter into a written agreement with each sub-processor imposing data protection obligations no less protective than those in this DPA.

6.4 Notification. Mynt shall notify the Customer of any intended addition or replacement of sub-processors at least fifteen (15) calendar days before the change via the website.

6.5 Objection rights. The Customer may object to a new sub-processor in writing to dataprotection@mynt.com within 15 days of notice.

6.6 Remedies. If Mynt cannot implement a commercially reasonable change to avoid the objected-to sub-processor within sixty (60) days, the Customer’s sole remedy is to terminate the affected Services.

7. Security measures

7.1 Technical and organizational controls. Mynt shall maintain appropriate technical and organisational measures for the protection of the security and integrity of Customer Data, as described in Schedule 2.

7.2 Security incident notification. Mynt shall notify Customer without undue delay, and typically within 48 hours, after becoming aware of a Security Incident impacting Customer Data.

7.3 Incident details. Notices will describe, to the extent possible, details of the Security Incident and steps taken to mitigate potential risks.

7.4 Confidentiality. Mynt shall ensure that all persons authorised to process Customer Data are bound by an appropriate duty of confidentiality.

8. Audit and security reports

8.1 Audit Program and Certifications. Mynt shall maintain a formal audit and compliance program designed to ensure adherence to this DPA and Applicable Data Protection Laws. Customer acknowledges that Mynt’s controls and security practices are regularly assessed through independent certifications, such as ISO 27001, the results of which Mynt shall make available to Customer upon written request, subject to appropriate confidentiality obligations.

8.2 Verification rights and documentation. Customer may verify Mynt’s compliance with this DPA primarily through the review of documentation, certificates, audit summaries, or other security information made available under Section 7.1.

8.3 Remote-First audit approach. A further audit may only be conducted if the information provided under Section 7.1 is, in Customer’s reasonable judgment, insufficient to demonstrate Mynt’s compliance, or following a confirmed Security Incident affecting Customer Data. All such audits shall be conducted remotely (e.g., via questionnaires or videoconferencing) unless an on-site visit is specifically mandated by a competent Supervisory Authority or proven strictly necessary to verify compliance that cannot be evidenced remotely.

8.4 Audit procedures and restrictions. Any audit conducted under Section 8.3 shall:

(i) be limited to once in any twelve-month period, unless otherwise required by law;

(ii) be scheduled with at least twenty-one (21) calendar days' prior written notice;

(iii) have a clearly defined scope agreed upon by Mynt before the commencement of the audit;

(iv) take place during Mynt's normal business hours and in a manner that does not unreasonably interfere with Mynt's day-to-day business activities or compromise the security of other Mynt customers; and

(v) be performed by Customer or an independent third-party auditor reasonably acceptable to Mynt who is not a competitor of Mynt.

8.5 Audit costs and personnel. Customer shall reimburse Mynt for any reasonable personnel costs and expenses directly incurred by Mynt as a result of the audit, with such costs to be mutually agreed upon prior to the commencement of the audit.

9. International transfers

9.1 Data processing locations. Mynt primarily processes Personal Data within the EU/EEA. However, in cases where our Sub-processors or partners are located in third countries outside this zone, Mynt ensures a level of protection equivalent to that of the GDPR. Any such transfers shall occur only to the extent strictly necessary to provide the Services under the Agreement.

9.2 Authorised transfer mechanisms. Any transfer of Personal Data to a third country (including the United Kingdom and the United States) shall occur only under one or more of the following safeguards:

- **Adequacy decisions:** Mynt transfers data to countries that the European Commission has deemed to provide an adequate level of data protection pursuant to Article 45(3) of the GDPR.
- **Standard Contractual Clauses (SCCs):** In the absence, revocation, or suspension of an adequacy decision, Mynt utilizes the latest EU Standard Contractual Clauses (and the UK Addendum, where applicable).
- **Data Privacy Framework (DPF):** For transfers to the United States, Mynt verifies if the recipient is certified under the EU-U.S. Data Privacy Framework.

9.3 Transfer Impact Assessments (TIAs). Mynt shall perform TIAs as required under Applicable Data Protection Laws to evaluate the adequacy of protection in the relevant third country and to ensure the recipient can comply with the applicable transfer mechanisms.

10. Return or deletion of data

10.1 Termination and data return. Upon termination or expiration of the Agreement, Mynt shall, at the Customer's election, delete or return all Customer Data (including copies) in its possession or control. The Customer is responsible for exporting any transactional data directly through the Mynt application prior to the termination date.

10.2 Statutory retention and backups. The requirement to delete or return data shall not apply to the extent that Mynt is required by applicable law (such as AML or accounting regulations) to retain certain Customer Data. Additionally, Mynt may retain Customer Data stored on archived backup systems, provided such data is securely isolated and protected from further processing, except as required by law.

11. Data subject rights and cooperation

11.1 Assistance. Mynt shall promptly notify the Customer if it receives a Data Subject Request and provide reasonable assistance in responding to such requests. The Customer shall export any transactional data directly through the Mynt application.

11.2 Law Enforcement demands. If a law enforcement agency sends Mynt a demand for Customer Data, Mynt shall attempt to redirect the agency to the Customer and provide reasonable notice of the demand unless legally prohibited.

SCHEDULE 1: Subject matter & details of processing

1. Nature and purpose of the Processing

Service provision: Mynt processes Personal Data as necessary for the provision of the expense management solution, including receipt management and accounting system integration.

Data usage restrictions: Mynt does not sell Customer Data (or end-user information within such Customer Data) and does not share such end-user information with third parties for compensation or for those third parties' own business interests.

Instruction-based processing: Mynt will process Customer Data as a Processor in accordance with the Customer's documented instructions as outlined in Section 5 (Customer Instructions) of this DPA to perform its obligations under the Agreement.

Authorised operations: The purpose of the data processing is the provision of the Services to the Customer, including transaction reconciliation, billing, technical support and account management.

2. Subject matter of the Processing

Scope: The subject matter of the data processing under this DPA is the Customer Data.

3. Duration of the Processing

Term: As agreed between Mynt and the Customer, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.

Post-termination retention: Upon termination, all Customer Data (processed by Mynt as a Processor) shall be deleted or returned at the Customer's election.

Controller-led retention: Data required for Mynt’s own legal compliance (such as KYC, AML, and Statutory accounting) is processed by Mynt as a Controller and is not Customer Data under this DPA. This data will be retained by Mynt for the statutory periods required by Swedish financial regulations and is governed exclusively by the Mynt Privacy Statement.

4. Categories of Data Subjects

Users: Any individual accessing and/or using the Services through the Customer's account.

Third parties: Individuals with whom the Customer or Customer's users have a commercial or business relationship, such as vendors or suppliers whose information appears on uploaded documents.

5. Types of Customer Data

Customer and users:

- **Identification and contact data:** E.g., name, email, phone number and personal identity number
- **Financial data:** E.g., transaction history, account details and Level 3 (L3) itemised receipt data.
- **Usage data:** E.g., information on product usage, contract and how services are utilized.
- **Technical data**: E.g., IP addresses, operating systems, and system logs (error messages and timestamps).

- **Communication data:** Records of interactions with customer success teams (chat conversations and email correspondence).

Third parties:

Information in uploaded documents: Contact details (name, email) and identity information relating to individuals who appear in receipts, invoices, or email communications processed for bookkeeping or accounting purposes.

6. Sensitive Data

General status: The Services are not intended for the processing of Special Categories of Data as defined in Article 9 GDPR.

Incidental processing: The Parties acknowledge that Sensitive Data may be incidentally processed if contained within documents (e.g., pharmacy receipts) uploaded by the Customer or its users.

Customer responsibility: The Customer warrants it has a valid legal basis for such processing and shall instruct users to minimise the upload of unnecessary sensitive information.

Safeguards: Mynt applies robust technical and organizational measures to all Customer Data as described in Schedule 2.

SCHEDULE 2: Security program

Leadership & compliance: Appointment of a CISO and DPO to monitor security and privacy functions. Mynt maintains a formal Information Security Management System (ISMS) aligned with, and independently assessed against, the ISO/IEC 27001 standard.

Access administration: Unique user accounts, strong passwords, regular access reviews, and multifactor authentication (MFA).

Vulnerability management: Vulnerability scans and patch management.

Encryption: Data encrypted at rest (AES-256) and in transit (TLS 1.2+).

Development: Test Driven Development, Clean code and Architecture. Dependencies updated continuously.

Intrusion detection and prevention: Continuous monitoring of communications within the production environment.

Business continuity: Regular backups and annual disaster recovery tests.

Incident management: Defined incident management and crisis communication procedures.

Third-party risk management: Security and privacy review of service providers. DPAs signed, when applicable.

Personnel: Background screening and annual security awareness training.

Contact Information:

- **DPO:** dataprotection@mynt.com
- **Support:** support@mynt.com