Privacy statement

1. Introduction and commitment

Mynt AB ("Mynt", "we", "us"), reg. no. 559100-8874, is a financial institution under the supervision of the Swedish Financial Supervisory Authority (Finansinspektionen). We process Personal Data with the highest degree of security and transparency in accordance with the General Data Protection Regulation (GDPR).

This policy outlines our commitment to protecting the privacy of our customers, business contacts, and website visitors, ensuring that all data processing is conducted lawfully, fairly, and transparently.

2. Key definitions

To provide clarity and ensure compliance with Article 4 of the GDPR, we apply the following definitions:

- **Personal Data:** Any information relating to an identified or identifiable natural person (**"Data Subject"**). This includes names, job titles, and professional contact details (such as individual work emails or direct phone numbers).
- **Data Controller:** The entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
- **Data Processor:** The entity which processes Personal Data on behalf of the Data Controller.
- **Sub-processor:** Any third-party service provider engaged by Mynt to process Personal Data in the capacity of providing services to us (e.g., cloud infrastructure or KYC providers).
- **Processing:** Any operation performed on Personal Data, such as collection, recording, storage, or transmission.
- **Personal Data Breach:** A security incident resulting in the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of Personal Data.
- **Special Categories of Personal Data:** Sensitive data as defined under Article 9 of the GDPR, including data revealing ethnic origin, political opinions, or biometric data for identification.

3. Roles and responsibilities

Mynt operates in different capacities depending on the service provided:

- **Mynt as Data Controller:** We are the Controller for Personal Data concerning our own customers, corporate representatives, and potential business leads for our corporate cards offering. This includes mandatory processing for identity verification (KYC), credit assessments, and Anti-Money Laundering (AML) compliance.
- **Mynt as Data Processor:** When you utilise Mynt's expense management solution, the customer is the Controller and Mynt is the Processor regarding any Personal Data provided, submitted, or otherwise made available to the platform (e.g., through manual input, software integrations, or automated syncing). This processing is governed exclusively by our Data Processing Agreement (DPA).
- **Independent Controller:** Under certain collaborative arrangements, Mynt and our strategic partners function as Independent Controllers. This relationship arises when both Mynt and the partner independently determine the purposes and legal grounds for processing Personal Data, distinct from a Joint Controllership or a Controller-Processor relationship.

- **Joint Controllership:** In specific instances, Mynt determines the purposes and means of processing jointly with a partner.

3.1 Joint controller arrangement – Click to Pay

For the **Click to Pay** feature, Mynt acts as a **Joint Controller** with the card network (e.g., **Visa**).

- **Allocation of Duties:** Under this arrangement, Mynt is responsible for collecting your enrollment information (including Personal Data), transmitting it to the network, and managing your opt-out preferences. Visa is responsible for storing your profile in their global database and performing identity verification.
- **Point of Contact:** Mynt acts as your primary point of contact for any GDPR-related queries regarding this specific arrangement.

3.2 Independent Controller – Partner relationships

In certain instances, Mynt's service delivery is facilitated through collaborative partnerships where both Mynt and the partner function as Independent Controllers. This arrangement applies when each party independently determines the purposes and legal grounds for processing Personal Data, distinct from a Joint Controllership.

- **Reciprocal data exchange**: Within these partnerships, Mynt may disclose Personal Data to a partner to facilitate specific services, and correspondingly, Mynt may receive Personal Data from such partners.
- **Independent accountability:** Each party maintains autonomous responsibility for ensuring that its data processing activities comply with the GDPR.
- **Governance and transparency:** As these partners operate independently, their processing activities are governed by their respective privacy statements. We encourage you to consult the privacy statement of the relevant partner (where applicable) for comprehensive information on their specific data handling practices.

4. How We collect data

We collect Personal Data via:

- **Digital Channels:** Registrations, newsletter sign-ups, or loan applications.
- **Offline:** Phone calls, meetings, or events.
- **Third-Party sources**: Public registers (e.g., Bolagsverket), partners, or individuals acting on your behalf. We may combine this data with info we already hold to improve our services.

5. Categories of personal data processed

We process the following categories of Personal Data to provide our services and meet legal requirements:

- **Identification and contact data:** E.g., name, email, phone number, personal identity number, and copies of ID documentation.
- **Financial data:** E.g., transaction history, credit history, account details and Level 3 (L3) itemised receipt data.

- **Usage data:** E.g., information on product usage, contract types, and how services are utilised.
- **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).
- **Compliance & Screening data:** Information required for KYC/AML/sanctions procedures, including data from global sanction lists and PEP (Politically Exposed Persons) lists (e.g., name and date of birth).
- **Special Categories of Personal Data:** See Section 7 below for details on when and how we process biometric data.

6. Purposes and retention

Purpose	Detailed description of processing	Relevant data categories	Legal basis	Retention period
Service delivery & administration	To establish, manage, and administer the contractual relationship. This includes account setup, processing transactions, card issuances, and providing support.	Identification and contact data, Financial data, Usage data, Technical data, and Communication data.	Performance of contract.	No longer than necessary for the duration of the contract and thereafter in accordance with internal retention schedules for the exercise or defence of legal claims.
Credit evaluation & risk management	To assess creditworthiness and perform risk modelling. This involves automated scoring to determine financial capacity and prevent fraud.	Identification and contact data, Financial data, Usage data.	Legitimate interest.	No longer than necessary for the ongoing risk assessment or as required by financial regulations.
KYC & AML/CTF compliance	To fulfil mandatory legal obligations regarding KYC procedures, including the prevention and reporting of money laundering and terrorist financing.	Identification and contact data, Financial data, Usage data, Technical data, and Communication data.	Legal obligation.	For the period prescribed by applicable anti-money laundering and counter-terrorist financing legislation.
Statutory accounting & financial reporting	To maintain accurate financial records and comply with mandatory reporting requirements to tax authorities and financial regulators.	Identification and contact data, Financial data.	Legal obligation.	For the period required under applicable accounting and tax legislation.
Marketing & identification of prospects	To identify potential commercial opportunities and communicate relevant financial solutions to professionals in their corporate capacity.	Identification and contact data.	Legitimate Interest, Consent.	No longer than necessary for the purpose of the potential commercial engagement and in accordance with Mynt's retention schedules, or until you object (opt-out).

Product improvement & analysis	To analyse platform usage and technical performance to develop new features, optimise user experience, and ensure system integrity.	Usage data, Technical data.	Legitimate Interest.	No longer than necessary for the purpose of the specific analytical or development lifecycle and in accordance with Mynt's retention schedules.
Recruitment	To process applications, verify professional background (CV, LinkedIn), and assess suitability for roles within the company.	Identification and contact data, Professional data (CV/LinkedIn), Application content.	Performance of contract (pre-contractual), Legal obligation, Legitimate interest, Consent.	No longer than necessary for the purpose of the recruitment process and in accordance with recruitment retention schedules, or until you withdraw your consent (opt-out).

7. Special Categories of Personal Data

Mynt generally does not seek to collect sensitive personal data. However, in specific instances, we may process Special Categories of Personal Data as defined under Article 9 of the GDPR.

7.1 Identification

Biometric data: We may utilise biometric technology (facial recognition) to compare a live scan of your face with your government-issued identification document. This is only employed in certain circumstances to fulfil our identity verification requirements when other options are not available.

Legal basis:

- **Legal obligation:** This processing is conducted to meet our mandatory identity verification and anti-money laundering obligations under the AML regulations.
- **Consent:** While providing biometric data is voluntary, completing identity verification is a mandatory requirement to proceed with your application. Accessing Mynt’s services is contingent upon successful identity verification; if you choose not to proceed with the biometric method when requested, we will be unable to verify your identity and therefore cannot offer you any services. We collect your explicit consent for this specific method at the point of collection.

7.2 Sales engagements

To ensure the highest standards of quality and training, we record our sales engagements, including video and audio calls. These recordings may inadvertently capture sensitive personal data (special categories of data under the GDPR), such as health information, religious beliefs, or political opinions, should such information be voluntarily disclosed during the conversation. Please note that this refers to content shared during the call; biometric data (such as voiceprints or facial geometry) is inherently captured by the nature of the recording process itself.

Legal basis:

- **Consent:** We process these recordings based on your explicit consent. You maintain full control over your data. You may withdraw your consent at any time or object to the recording before or during the engagement. Upon such a request, we will immediately cease recording or delete the existing file, provided there is no other overriding legal obligation for its retention.

8. Identification of potential business contacts and leads

To offer tailored solutions and expand our market presence, we process data regarding potential customers and business partners.

- **Sources of data:** We strategically source data from specialised third-party providers such as Vainu, Leadpilot, and LinkedIn, as well as public registers (e.g., Bolagsverket and Google).
- **Categories of data:** The Personal Data processed includes names, job titles, and professional contact details. We also process non-personal data, such as organisation names and corporate registration numbers, to provide professional context.
- **Legal Basis:** *Legitimate Interest*. We balance our interest in establishing business relationships against your privacy by limiting contact to professional contexts and providing clear, simple methods to opt-out.

9. Automated decision-making

We utilise automated processes for credit evaluations and risk assessments. This ensures an objective, efficient, and consistent evaluation of your or your company's financial standing.

- **How it works (the logic):** Our system performs an automated assessment of your financial circumstances to determine your capacity to meet payment commitments. This decision is based on probability models that analyse factors such as credit history, payment remarks, existing assets, and liabilities.
- **The consequences:** If the automated assessment indicates a high risk of default or insufficient financial capacity, your application for financing or service may be automatically denied.
- **Legal basis**: This processing is necessary for entering into or performing a contract with you.
- **Your rights (human intervention):** If you disagree with an automated decision or wish to provide additional context, you have the right to:
    1. **Obtain human intervention:** Have your case reviewed by a qualified Mynt representative.
    2. **Express your point of view:** Present additional circumstances or documentation.
    3. **Contest the decision:** Challenge the grounds of the automated refusal.

To exercise these rights, please contact us at support@mynt.com. A representative with the authority to change the decision will perform a manual review of the information used and any new data you provide.

10. Data sharing and Sub-processors

To provide our services and fulfil our legal and contractual obligations, we share Personal Data with trusted third parties. The categories of recipients listed below are illustrative and not exhaustive, as our network of partners may evolve to enhance our service offering:

- **Sub-contractors:** Essential service providers including cloud infrastructure (e.g., AWS), payment processing partner (e.g., Enfuce), CRM systems, and customer communication platforms.
- **Financial partners:** Card networks (e.g., Visa), payment gateways, and banking partners.
- **Credit & verification:** Credit reference agencies and identity verification services used for risk assessment and mandatory KYC procedures.

- **Authorities:** Regulatory bodies such as Finansinspektionen, the Swedish Tax Agency (Skatteverket), or law enforcement agencies when Mynt is legally mandated to disclose information.
- **Business integrations:** Third-party accounting or ERP systems where you have explicitly instructed Mynt to share data.

Detailed Sub-processor list: For a comprehensive and up-to-date list of the specific entities processing data on our behalf, please visit **Mynt's Security Center** on the website.

11. Security and risk management

We implement a robust framework of technical, organisational, and administrative safeguards designed to protect Personal Data against unauthorised access, loss, or alteration.

- **Standard of protection:** Our measures include industry-standard encryption (AES-256 at rest, TLS 1.2+ in transit), strict identity and access management (IAM), multifactor authentication (MFA), and regular vulnerability assessments.
- **User responsibility:** While we take extensive steps to protect your information, no security protocol can be guaranteed to be 100% secure. Consequently, any transmission of data to Mynt via digital channels is conducted at your own risk.
  - Security Best Practices: We strongly urge you to maintain the total confidentiality of your passwords and account credentials. If you suspect your account has been compromised, contact us immediately at support@mynt.com.

12. International data transfers

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, we ensure a level of protection equivalent to that of the GDPR.

- **Adequacy decisions:** We transfer data to countries that the European Commission has deemed to have an adequate level of data protection.
- **Standard Contractual Clauses (SCCs):** In the absence of an adequacy decision, we utilise the latest EU Standard Contractual Clauses (and the UK Addendum, where applicable). We perform Transfer Impact Assessments (TIAs) to ensure the recipient can comply with these clauses.
- **Data Privacy Framework:** For transfers to the United States, we verify if the recipient is certified under the EU-U.S. Data Privacy Framework.

13. Cookies and analytics

Mynt utilises cookies and similar tracking technologies to optimise our website's performance, analyse user behaviour, and deliver a personalised experience.

- **Information collected:** Through tools such as Google Analytics, we collect aggregated and pseudonymised data, including:
  - Demographics & geography: Age, gender, language preferences, and general location.
  - Technical context: Device type, operating system, and browser version.
  - Interaction data: Time of visit, pages viewed, and referring sources.

- **Managing your preferences:** You have the right to block or delete cookies through your browser settings at any time (see aboutcookies.org). Note that disabling cookies may result in certain features of the Mynt platform becoming unavailable.

14. Your rights

As a Data Subject, you have the following rights:

- **Access:** Request a copy of the Personal Data we process about you. Please note that access may be restricted by law, specifically regarding information related to AML monitoring and reporting.
- **Rectification:** Request correction of inaccurate or incomplete data.
- **Erasure:** Request deletion of your data. This right is subject to mandatory legal retention requirements. For example, AML legislation requires us to store KYC data for at least five years from the date of the action or the end of the business relationship, which overrides the right to erasure during this period. Please note, as certain data is a prerequisite for our services, a request for erasure of essential data will result in the termination of the services.
- **Object:** You may at any time object to our marketing and prospecting activities or processing based on legitimate interest. Note that processing carried out to comply with legal obligations (such as AML checks) cannot be objected to. If you object to the use of biometric verification where no alternative is feasible, we will be unable to establish or maintain the business relationship.
- **Restriction & Portability:** In certain circumstances, you may also request that we restrict the processing of your data or provide your data in a structured, machine-readable format for transfer to another provider.
- **Complaints:** If you believe our processing of your personal data violates data protection regulations, you have the right to lodge a complaint with the Swedish Authority for Privacy Protection (**IMY**).
  - **Phone**: 08-657 61 00
  - **Email:** imy@imy.se
  - **Postal address:** Integritetsskyddsmyndigheten, Box 8114, 104 20 Stockholm

15. Contact

For any questions regarding our processing of Personal Data or to exercise your rights, please contact:

Mynt AB | Email: support@mynt.com | Web: **www.mynt.com**