CPS Privacy Notice

Last updated: 19.01.2026

1. Overview

This Privacy Notice explains how CPS (CPS Europe S.A., a company duly incorporated under the laws of Luxembourg) collects, uses, and protects personal data in compliance with the EU General Data Protection Regulation (GDPR) and applicable Luxembourg data protection law. It applies to all individuals whose data CPS processes in the context of its services – including consumer users, business customers (Merchants) and their representatives, as well as end-consumers who use payment services via those Merchants.

CPS as Controller and Processor

1.1. CPS provides services both directly to users and on behalf of other businesses, and therefore operates under two data protection roles:

1.1.1. CPS is the controller for personal data that it collects and uses in the course of its own services and operations – for example, data about individuals who sign up for CPS accounts or use CPS platforms, and data about the owners or representatives of corporate clients. In this context CPS decides why and how personal data is processed.

1.1.2. CPS also acts as a processor for personal data that it handles on behalf of Merchant end-users when providing payment processing and related services. In these cases, the Merchant is the controller determining the purposes and the means of processing, and CPS processes the data strictly under the Merchant's instructions and contractual obligations. Such processing is governed by a separate Data Processing Agreement (DPA) between CPS and the Merchant. CPS does not control or use such data for its own purposes and retains, discloses, or otherwise handles it only as permitted by the Merchant and applicable law.

1.2. If CPS processes personal data on behalf of a Merchant, the Merchant's own privacy notice will describe how that data is used. CPS will typically direct end-users to contact the relevant Merchant for information or to exercise data-subject rights, although CPS will assist Merchants in responding to such requests where required.

2. Categories of Personal Data Processed

2.1. CPS only collects personal data that is relevant and necessary for the purposes described in this Notice. Depending on the relationship with CPS, the following categories of data may be processed:

2.2. Identity and contact information (Full name, title, postal address, email address, phone number, date of birth and other identifiers). For business clients this may include company name and role or job title; for consumers this may include contact details provided for receipts or customer support.

2.2.1. Identification and verification data (Copies of or data from government-issued IDs or other KYC documents (e.g. passport number, national ID, driver's licence, nationality, proof of address), customer IDs, and account registration credentials, as required for onboarding, due diligence and regulatory compliance).

2.2.2. Financial and transaction data (data necessary to provide payment services, such as payment account numbers or IBANs, card details (handled securely), transaction records (amounts, currency, dates, payee/payer, Merchant details), funding and withdrawal information, account balances and payment history).

2.2.3. Business-related data (professional details of company representatives (e.g. position, authority to represent the company) and information about beneficial owners or directors where required for regulatory compliance. This can include shareholding information or company registration documents containing personal data).

2.2.4. Usage and technical data (when a user interacts with CPS online services or platforms, CPS may collect device and usage data, such as IP address, browser type, operating system, login timestamps, and activity logs (e.g. actions taken, features used). This is used to secure services and improve user experience).

2.2.5. Communication data (content of communications sent to CPS or submitted through customer support (emails, chat logs, call recordings), as well as preference information (language preferences, marketing opt-ins/opt-outs, etc.))

2.2.6. CPS does not actively seek to collect special categories of personal data (e.g. health, biometric, or ethnic data) in the ordinary course of providing services. However, CPS may process certain sensitive data if required for legal compliance – for example, data relating to criminal convictions or offences as part of anti-money-laundering (AML), counter-terrorist-financing (CFT) and fraud-prevention checks. Such processing is carried out only where permitted by law and subject to appropriate safeguards.

2.3. If a data subject fails to provide personal data that CPS is required to collect by law or under a contract (for example, identity information needed to open an account or process a payment), CPS may be unable to provide or continue providing services.

3. Purposes of Processing

3.1. Provision of services

To set up and administer accounts, issue electronic money, process payments, facilitate transactions and transfers, and generally perform contracts with customers and Merchants. This includes processing payment instructions, verifying that payments are completed, and maintaining records of balances and transactions.

3.2. Identity verification and compliance

To verify identity and conduct due diligence (KYC and related checks) as required by law, and to comply with obligations under financial regulations (including AML/CFT and sanctions screening). This includes monitoring transactions, screening against sanctions and PEP lists, and retaining records mandated by law.

3.3. Customer service and communications

To communicate about accounts or transactions (e.g. confirmations, notifications of changes, security alerts) and to respond to inquiries or support requests. CPS also uses personal data to notify users about updates to terms, this Privacy Notice, or other important information.

3.4. Service improvement and development

To analyse and improve CPS services and user experience, troubleshoot performance issues, test new features, and develop new products. Wherever possible, CPS uses aggregated or de-identified data for analytics.

3.5. Security and fraud prevention

To protect customers, Merchants and CPS from fraud, cyber threats and other illegal activity. CPS monitors transactions and usage for signs of fraud or misuse and uses personal data to enforce terms and investigate or prevent security incidents.

3.6. Legal and regulatory purposes

To establish, exercise or defend legal claims and to cooperate with regulators, law-enforcement bodies or courts. CPS may be required to disclose personal data for tax reporting, regulatory audits or other legal obligations, and will do so only to the extent required by law.

3.7. Marketing

CPS does not sell personal data or engage in mass marketing to consumers. CPS may send information about its own services or promotions to current or prospective business customers, or to individual users where permitted by law. Such marketing is based on CPS's legitimate interest in promoting its services or, where required, consent. Recipients can opt out of marketing communications at any time.

4. Legal Bases for Processing

CPS always relies on a valid legal basis under GDPR for processing personal data. Depending on the specific processing activity, one or more of the following legal bases apply:

4.1. Performance of a contract

Processing is necessary to perform a contract to which the data subject (or the entity the data subject represents) is party, or to take steps at the data subject's request before entering into a contract. This includes processing payment instructions, authenticating identity, and maintaining accounts.

4.2. Compliance with a legal obligation

Processing is necessary to comply with laws and regulations applicable to CPS as an Electronic Money Institution and payment service provider. This includes AML/CFT requirements, record-keeping obligations, tax and accounting rules, and responding to lawful requests from authorities.

4.3. Legitimate interests

Processing is necessary for the legitimate interests pursued by CPS or a third party, provided such interests are not overridden by the data subject's rights and freedoms; or as permitted by the modified Law of 30 May 2005. Examples include ensuring security and fraud prevention, improving services, managing business relationships with corporate clients, and defending legal rights. Data subjects have the right to object to processing based on legitimate interests (see Section 8).

4.4. Consent

In limited cases, CPS may rely on consent (e.g. for certain marketing communications or optional features). Where consent is used, it will be clear, specific and freely given, and can be withdrawn at any time. Withdrawal does not affect the lawfulness of processing carried out before the withdrawal.

5. Sharing of Personal Data

5.1. CPS treats personal data as confidential and does not sell personal information. However, to operate its business and comply with obligations, CPS may share personal data with the following categories of recipients:

5.1.1. **Merchants.** If a data subject uses CPS through a Merchant (for example, as an end-consumer making a payment), relevant transaction details are shared with that Merchant so it can reconcile and manage its payments.

5.1.2. **Service providers**. CPS engages trusted third-party providers to perform certain processing activities on its behalf, such as IT infrastructure and hosting, identity verification and KYC services, payment and banking partners, email/SMS delivery services, analytics and security providers, and customer support tools. These parties are subject to rigorous due diligence by CPS, act under CPS's instructions and are bound by contractual obligations to protect personal data.

5.1.3. **Financial institutions and payment schemes**. Banks, card networks and other financial intermediaries involved in the transaction chain may receive transaction-related data (e.g. account/card numbers, amounts, dates, and supporting information) to process payments. These parties often act as independent controllers for their own compliance obligations.

5.1.4. **Credit reference and fraud-prevention agencies**. Subject to applicable law, CPS may share data with credit reference bureaux or fraud-prevention databases to verify identity, assess risk, and prevent fraud.

5.1.5. **Corporate group entities**. Where CPS is part of a corporate group, personal data may be shared with affiliates or subsidiaries for business administration, consolidated reporting, security operations or support, subject to appropriate safeguards and intra-group agreements.

5.1.6. **Professional advisers and auditors**. External auditors, legal counsel, accountants and other professional advisers may access personal data where necessary for their services or for corporate governance and compliance.

5.1.7. **Regulators and public authorities**. CPS may disclose personal data to supervisory authorities, law-enforcement agencies, courts or other public bodies where required by law or regulation (for example, to the Luxembourg FIU, CSSF or CNPD).

5.1.8. **Business acquirers**. In the event of a merger, acquisition, restructuring or sale of all or part of CPS's business, personal data may be transferred to the relevant acquiring or merging entity. Any such transfer will be subject to safeguards ensuring continued protection of the data and compliance with this Notice and applicable law.

5.2. CPS shares only the minimum data necessary for each purpose and requires all third parties to handle personal data securely and lawfully

6. International Data Transfers

6.1. CPS is based in the European Economic Area (EEA) (Luxembourg) and primarily processes and stores personal data on servers located within the EEA. However, some of the third parties and affiliates who process personal data (as described above) may be located outside the EEA.

6.2. Whenever CPS transfers your personal data to a third country, CPS puts in place appropriate safeguards to ensure that your data remains protected. These safeguards typically include:

6.2.1. relying on the European Commission's adequacy decisions (if the destination country is approved as having essentially equivalent privacy laws); or

6.2.2. implementing the EU Standard Contractual Clauses (SCCs) with the recipient, which contractually oblige the recipient to protect your information in accordance with EU GDPR standards.

6.3. CPS also considers any guidance from regulators regarding international data transfers and adopts any required measures (for instance, assessing local laws that might affect data privacy and implementing supplementary protections as needed).

6.4. You can request a copy of the relevant transfer safeguards (e.g. SCCs) by contacting CPS. CPS ensures that your personal data, no matter where it is processed, receives a high standard of protection in line with this Notice and applicable law.

7. Data Retention

7.1. CPS retains personal data only for as long as it is necessary to fulfil the purposes described in this Notice, or as required by law (whichever is longer).

7.2. For customers and Merchant representatives, CPS retains personal data for the duration of the relationship (while there is an active account or ongoing contract with CPS) and thereafter for a limited period. Once an account is terminated or services are discontinued, most personal data will be archived or deleted after a defined retention period.

7.3. Even after an account is closed or CPS services cease to be used, CPS is subject to laws that require certain data to be retained. For example, anti-money-laundering regulations oblige CPS to keep transaction records and identity-verification data for five (5) years from the end of the business relationship or the date of an occasional transaction. In Luxembourg, this 5-year retention period may be extended to a maximum of ten (10) years where legally mandated or justified by specific circumstances. CPS may also retain data as needed to fulfil other legal obligations (such as tax, accounting or regulatory reporting) for the periods required by those laws.

7.4. If CPS is handling an ongoing dispute, investigation or legal claim involving a customer, Merchant or other data subject, CPS will retain the necessary personal data until the issue is resolved and no further claims are expected, even if this extends beyond standard retention periods.

7.5. In some cases, CPS may retain limited information for longer periods for legitimate business interests, such as fraud prevention or record-keeping. For instance, CPS may keep a suppression list of email addresses of individuals who opt out of marketing to ensure that such opt-outs are honoured indefinitely.

7.6. When determining retention periods, CPS considers the amount, nature and sensitivity of the data, the potential risk of harm from unauthorised use or disclosure, the purposes of processing and whether those purposes can be achieved by other means. CPS securely erases or anonymises personal data that is no longer needed. In some cases, data may persist in backups for a short duration beyond active deletion, but CPS continues to safeguard such data and deletes it in accordance with backup rotation schedules.

8. Your Rights as a Data Subject

8.1. Under the GDPR, you have various rights regarding your personal data. CPS is committed to honouring these rights. Your key rights include:

8.1.1. Right of access

You can request confirmation of whether CPS is processing your personal data and, if so, ask for a copy of the data CPS holds about you. This includes information on what data is held, the purposes of processing, and with whom it has been shared. The first copy will be provided free of charge.

8.1.2. Right to rectification

If any of your personal data held by CPS is inaccurate or incomplete, you have the right to have it corrected or updated without undue delay. You may also provide supplemental information to complete your records.

8.1.3. Right to erasure

You have the right to request that CPS delete your personal data in certain circumstances. This is sometimes called the “right to be forgotten”. Please note that, due to legal obligations, CPS may not be able to immediately erase some data (for example, transaction records required for AML purposes during the mandatory retention period). CPS will inform you of any such constraints.

8.1.4. Right to restrict processing

You can ask CPS to limit the processing of your personal data (i.e. to store it but not otherwise use it) in certain cases – for example, while a request to correct data or an objection is being assessed, or if you need CPS to preserve data for a legal claim. When processing is restricted, CPS will not use your data except to store it or as necessary for legal or regulatory compliance.

8.1.5. Right to object

You have the right to object to CPS's processing of your personal data when the processing is based on legitimate interests or public interest (including profiling on those bases). If you object, CPS will stop the processing unless CPS demonstrates compelling legitimate grounds that override your interests, rights and freedoms, or the processing is needed for the establishment, exercise or defence of legal claims. You have an absolute right to object to your personal data being used for direct marketing at any time. If you opt out of marketing communications, CPS will cease processing your data for that purpose without delay.

8.1.6. Right to data portability

For personal data that you have provided to CPS and which CPS processes by automated means based on your consent or a contract, you can request to receive that data in a structured, commonly used and machine-readable format, and you have the right to have that data transmitted to another controller where technically feasible. In practice, this could include basic account information or transaction data that you have provided.

8.1.7. Right not to be subject to automated decisions

You have the right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you, unless the decision is necessary for entering into or performing a contract, authorised by law, or based on your explicit consent. CPS's decisions that significantly affect you typically involve some human review or are authorised under financial regulations. CPS does not carry out fully automated decision-making that produces legal effects without human involvement. If you believe you have been subject to an improper automated decision, you can contact CPS to have it reviewed.

8.1.8. Right to withdraw consent

Where CPS processes your personal data on the basis of your consent, you have the right to withdraw that consent at any time. Once consent is withdrawn, CPS will stop the specific processing that was based on that consent. Withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal.

8.1.9. Right to lodge a complaint

If you have concerns about CPS's data-processing practices, you have the right to file a complaint with a supervisory authority – in particular, in the EU Member State where you live, work, or where the alleged infringement occurred. CPS's lead supervisory authority is Luxembourg's National Data Protection Commission (CNPD), whose contact details are available on the CNPD website. CPS nevertheless encourages you to contact the DPO first, so that CPS has an opportunity to address your concerns directly.

8.2. You can exercise any of the above rights by contacting CPS at legal@enum8.com. For security reasons, CPS may need to verify your identity before fulfilling a request. CPS will respond as soon as reasonably possible and in any event within one month, as required by the GDPR. This period may be extended by up to two additional months for complex or numerous requests, in which case CPS will inform you of the extension and the reasons for it.

9. How CPS Protects Your Data

9.1. CPS takes the security of personal data very seriously and has implemented a range of technical and organisational measures to protect personal data against unauthorised access, loss, alteration or disclosure. These measures are designed to provide a level of security appropriate to the risks arising from the processing of personal data. They include:

9.1.1. Technical safeguards. Encryption of sensitive data in transit (e.g. SSL/TLS for CPS websites and apps) and, where appropriate, at rest; firewalls and network security controls to prevent external attacks; access-control mechanisms (password protection, multi-factor authentication, role-based access restrictions, VPN) to ensure that only authorised personnel can access data required for their job; and regular data backups. CPS also uses intrusion-detection and prevention systems and monitors its systems for potential vulnerabilities or attacks.

9.1.2. Organisational measures. Internal policies and staff training on data protection and information security, so that employees handle personal data with care and confidentiality. Access to personal data is limited to personnel who need it to perform their duties. CPS conducts due diligence on its service providers to ensure that they maintain high security standards and includes appropriate data-protection clauses in contracts with them. CPS also maintains incident-response plans to handle any suspected data breach swiftly and mitigate any harm.

9.1.3. Compliance standards. CPS is subject to legal requirements applicable to the financial sector such as Regulation (EU) 2022/2554 on digital operational resilience (DORA). As a financial entity licensed in Luxembourg, CPS is subject to regulatory requirements by the Commission de Surveillance du Secteur Financier (CSSF) covering technical and organizational security measures. CPS operates an information security program which aligns with the technical requirements of ISO/IEC 27001. CPS is subject to periodic audits and assessments of its controls.

9.2. Although CPS strives to protect personal data, no system can be 100% secure. CPS continuously updates and improves its security measures to address new threats and to help ensure that personal data remains safe. If you have reason to believe that your interaction with CPS or your data may no longer be secure, you should contact CPS immediately so that CPS can assist.

10. Changes to this Privacy Notice

10.1. CPS may update this Privacy Notice from time to time to reflect changes in its practices, legal requirements or other operational reasons. When significant changes are made, CPS will notify affected data subjects in an appropriate manner – for example, by posting a prominent notice on the CPS website (enum8.com) or, where changes are material and contact details are available, by sending a notification in advance. The "Last updated" date at the top of this Notice indicates when the latest changes were made.

10.2. Data subjects are encouraged to review this Notice periodically to remain informed about how CPS protects and processes personal data. Where required by law, CPS will seek consent for any substantial changes that affect the manner in which personal data is used.

11. Contact

If you have any questions or concerns about this Privacy Notice or how CPS handles your personal data, please do not hesitate to contact DPO of CPS at legal@enum8.com.