iMobile

MoneyCounter

Country Annex — European Union

Vendor statement of facts relevant to local requirements

Document ID	IM.MONEYCOUNTER.EU.A1
Document version	1.0
Date of issue	2026-10-06
Applies to	MoneyCounter 2.0.0.0
Language	English
Publisher	iMobile

© 2026 iMobile. https://new-imobile.com

Contents

1. Purpose and status . . . 3
2. Product facts . . . 3
2.1. Personal data the product can process . . . 3
2.2. Where data is stored . . . 3
2.3. Data sent to the vendor . . . 3
3. Data protection — GDPR . . . 4
3.1. Roles . . . 4
3.2. What the product provides (Articles 25 and 32) . . . 4
3.3. What remains with the customer . . . 4
4. Product cybersecurity — Cyber Resilience Act . . . 4
5. Supply-chain security — NIS2 . . . 5
6. Accessibility . . . 5
7. Language . . . 5
8. Documents usually requested and where to find them . . . 5

© 2026 iMobile

About this document

This annex supplements the documentation of MoneyCounter version 2.0.0.0 for customers in the European Union and the European Economic Area. It sets out the facts about the product that matter under the local rules named below and shows which obligations stay with the customer.

The annex is a statement by the vendor about its product. It is not legal advice, not a certificate of conformity and not a substitute for the customer's own assessment.

1. Purpose and status

No CE marking, EU declaration of conformity or certificate under a European cybersecurity certification scheme is claimed for the product in this document.

2. Product facts

Item	Fact
Product and version	MoneyCounter 2.0.0.0
Deployment	Desktop software installed on the customer's computers
Customer content on vendor servers	No
Interface languages	16 languages: English, Russian, German, Spanish, Chinese, Japanese, Korean, Arabic, Turkish, Persian, Portuguese (Brazil), French, Italian, Polish, Vietnamese, Indonesian. The installer is in English only.

2.1. Personal data the product can process

- The e-mail address entered to activate the Pro edition: kept on the computer in an encrypted file and sent to the vendor's account server. Not requested without activation.
- A machine fingerprint (SHA-256 hash of the Windows MachineGuid, the computer name and the system volume serial number): sent to the account server after activation and tied to the e-mail address in the signed terms string.
- Free-text comments to counts typed by the user: kept only in the local database.

2.2. Where data is stored

All data stays on the user's computer, in the Windows user profile: the database `%APPDATA%\MoneyCounter\moneycounter.ste` (SQLite: currencies, denominations, history of counts with logs), the activation file `%APPDATA%\MoneyCounter\license.dat`, and settings in the registry key `HKCU\Software\MoneyCounter` (language, selected currency, history column layout). No count data is stored on vendor servers.

2.3. Data sent to the vendor

- Activation code request: e-mail address, product identifier, interface language code (HTTPS, account server `accounts.new-imobile.com`)
- Activation: e-mail address, code from the e-mail, product identifier
- Edition check — right after activation and in the background on every start of an activated program: activation token, product identifier, machine fingerprint

© 2026 iMobile

- Nothing else: no counts, history, telemetry or error reports are sent and there is no update check; a program that has not been activated opens no network connections

3. Data protection — GDPR

Regulation (EU) 2016/679 (GDPR) applies to the personal data the customer processes with the product.

3.1. Roles

For personal data processed in the product on the customer's own equipment, the customer is the controller. The vendor has no access to that data and is not a processor for it.

For the data listed under "Data sent to the vendor", which the vendor receives in order to perform the licence agreement, the vendor is itself a controller.

Details of the vendor's establishment and, where Article 27 applies, of its representative in the Union are stated in the contract.

3.2. What the product provides (Articles 25 and 32)

- **Access control.** The program has no sign-in, roles or access control of its own. Access to data is determined by the Windows account: each Windows user has a separate database and activation. The Pro edition is confirmed by an e-mail address and a one-time code sent to it.
- **Logging.** The program keeps no security event log, operation log or diagnostic files. Each saved count is stored with its log: lines about quantity changes, clearing and saving with the breakdown by denomination. The user can delete history records; deletions are not recorded.
- **Export and deletion.** Export: File → Back up… saves a copy of the database — a SQLite file readable with standard tools; there is no export to CSV, Excel or PDF and no printing. Deletion: a single history record with the M- button; all user data by deleting the folder `%APPDATA%\MoneyCounter` and the registry key `HKCU\Software\MoneyCounter` (uninstalling the program does not remove them). Activation data on the account server cannot be deleted from the program — contact iMobile for that.
- **Encryption.** See the section on cryptography below.

3.3. What remains with the customer

- the lawful basis for processing (Article 6) and information to data subjects (Articles 13 and 14);
- the record of processing activities (Article 30) and, where required, a data protection impact assessment (Article 35);
- answering data-subject requests (Articles 15 to 22) with the export and deletion functions above;
- notifying a personal-data breach to the supervisory authority within 72 hours (Article 33);
- for installations on the customer's equipment, the choice of where that equipment is located.

4. Product cybersecurity — Cyber Resilience Act

Regulation (EU) 2024/2847 sets cybersecurity requirements for products with digital elements placed on the Union market. Its main obligations (conformity assessment, EU declaration of conformity, CE marking) apply from 11 December 2027; the manufacturer's duty to report actively exploited vulnerabilities and severe incidents applies from 11 September 2026.

- No EU declaration of conformity under the Regulation has been issued for this version.

© 2026 iMobile

- Vulnerability reports are accepted through the channels named in the Security and Data Protection Statement.
- The period during which security updates are provided is set in the contract.
- The components the product contains are listed in "Delivery Specification and Third-Party Components".

5. Supply-chain security — NIS2

Customers that are essential or important entities under Directive (EU) 2022/2555 must address the security of their supply chain (Article 21(2)(d)). The Security and Data Protection Statement and the Delivery Specification contain the facts usually collected in a supplier assessment.

6. Accessibility

Public-sector buyers apply the standard EN 301 549, which Directive (EU) 2016/2102 uses for public-sector websites and mobile applications. Directive (EU) 2019/882 (European Accessibility Act) has applied since 28 June 2025 to the consumer products and services it lists.

Status of the product: No accessibility evaluation has been carried out; operation with screen readers and in high-contrast mode has not been tested. The display and some buttons are non-standard, custom-drawn controls. For Arabic and Persian the main window keeps a left-to-right layout.

No EN 301 549 conformance report is provided for this version.

7. Language

This package is supplied in English. Member states may require the national language for documentation supplied to consumers or to public bodies (for example France, Law No. 94-665 of 4 August 1994). National-language documentation is not part of this package.

Interface languages of the product: 16 languages: English, Russian, German, Spanish, Chinese, Japanese, Korean, Arabic, Turkish, Persian, Portuguese (Brazil), French, Italian, Polish, Vietnamese, Indonesian. The installer is in English only.

8. Documents usually requested and where to find them

Usually requested	Where it is
Product description, functional specification	Product Description and Functional Specification
Installation and operating instructions	Installation and Administration Guide
User manual	User Guide
Maintenance and support description	Software Lifecycle, Maintenance and Support. Service levels: contract
List of third-party and open-source components	Delivery Specification and Third-Party Components
Security and data-protection description	Security and Data Protection Statement
Technical and organisational measures (Article 32 GDPR)	Security and Data Protection Statement
Data processing agreement (Article 28 GDPR), standard contractual clauses	Contract; needed only where the vendor processes customer data
EN 301 549 accessibility report	Not provided for this version

© 2026 iMobile

Usually requested	Where it is
EU declaration of conformity (Cyber Resilience Act)	Not issued; not yet required
Public-sector standard terms (for example EVB-IT in Germany, CCAG-TIC in France)	Contract; the documents of this package serve as the product description those terms refer to
Licence agreement, warranties, prices	Contract

Document history

Document version	Date	Product version	Change
1.0	2026-10-06	2.0.0.0	First issue

© 2026 iMobile