iMobile

MoneyCounter

Country Annex — United States

Vendor statement of facts relevant to local requirements

Document ID	IM.MONEYCOUNTER.US.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. Privacy . . . 4
3.1. Roles . . . 4
3.2. What the product provides . . . 4
3.3. What remains with the customer . . . 4
4. Accessibility . . . 5
5. Software supply chain . . . 5
6. Cryptography and export controls . . . 5
7. Government contracts . . . 6
8. Language . . . 6
9. Documents usually requested and where to find them . . . 6

© 2026 iMobile

About this document

This annex supplements the documentation of MoneyCounter version 2.0.0.0 for customers in the United States. 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 certification, authorisation or registration by United States federal or state authorities is claimed for the product or for the vendor 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`)

© 2026 iMobile

- 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
- 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. Privacy

The United States has no single federal privacy statute for the private sector. Contracts most often refer to the state consumer-privacy laws, above all the California Consumer Privacy Act as amended by the CPRA (Cal. Civ. Code § 1798.100 et seq.), and to sector laws.

3.1. Roles

For personal data processed in the product on the customer's own equipment, the customer is the business (the CCPA term; "controller" in other state laws). The vendor has no access to that data and is not a service provider 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 business (the CCPA term; "controller" in other state laws).

3.2. What the product provides

- **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 notice at collection and the privacy policy;
- answering consumer requests to know, delete and correct, using the export and deletion functions above;
- deciding whether regulated categories of data may be placed in the product. No assessment of the product against HIPAA, GLBA, FERPA, COPPA or PCI DSS is claimed in this document.

© 2026 iMobile

4. Accessibility

Federal agencies, and many state bodies and universities, buy information technology against Section 508 of the Rehabilitation Act (29 U.S.C. § 794d), whose standards incorporate WCAG 2.0 Level AA, and ask the vendor for an Accessibility Conformance Report on the VPAT template.

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 Accessibility Conformance Report (VPAT) is provided for this version.

5. Software supply chain

Federal agencies set their own software-assurance requirements (OMB Memorandum M-26-05). An agency may ask a software producer for a statement on secure development practices aligned with the NIST Secure Software Development Framework (NIST SP 800-218) and for a software bill of materials (SBOM).

- Development and release practices are described in "Software Lifecycle, Maintenance and Support".
- Third-party components and their licences are listed in "Delivery Specification and Third-Party Components". The list is human-readable; no SBOM in SPDX or CycloneDX format is provided for this version.
- No secure-development attestation is provided for this version.

6. Cryptography and export controls

The product uses cryptography as follows:

- Exchange with the account server uses HTTPS; TLS is provided by Windows and the protocol version is determined by the operating system
- Edition terms signature check: ECDSA on curve P-256 with SHA-256 through Windows CNG; the public key is embedded in the program
- Machine fingerprint: SHA-256 hash through Windows CNG
- The activation file `license.dat` is encrypted with Windows DPAPI under the user account
- The database of counts is not encrypted; the program contains no cryptographic algorithm implementations of its own
- The product has not been validated under FIPS 140-3. Where the list above names cryptographic services of the operating system, their validation status is that of the operating system.
- The product is developed and published outside the United States. No U.S. export classification (ECCN) is claimed for it. A customer that exports or re-exports the product from the United States determines its own obligations under the Export Administration Regulations (15 C.F.R. Parts 730–774).

© 2026 iMobile

7. Government contracts

- **Rights in software.** The software and its documentation are "commercial computer software" and "commercial computer software documentation" within the meaning of Part 12 of the Federal Acquisition Regulation and DFARS 227.7202. U.S. Government end users acquire them with only the rights set out in the vendor's licence agreement.
- **Country of origin.** A statement for the purposes of the Trade Agreements Act (19 U.S.C. § 2501 et seq.; FAR 52.225-5) depends on the contracting entity and is given in the contract; none is made here.

8. Language

This package is supplied in English. This annex is laid out for US Letter paper; the other documents of the package are laid out for A4.

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.

9. 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
Accessibility Conformance Report (VPAT)	Not provided for this version
SBOM (SPDX or CycloneDX), secure-development attestation	Not provided for this version; component list as above
Service-provider terms (CCPA), business associate agreement (HIPAA)	Contract, where applicable
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