CONFIRMO

CONFIRMO PRIVACY POLICY

Last Updated: 30 December 2025

1. Introduction and Scope of This Policy

This Privacy Policy (or "Policy") explains how the Confirmo Group entities (collectively “Confirmo”, “we”, “us” or “our”) collect, use, store, share, and protect personal data. This Policy (together with our Terms and Conditions, Cookies Policy and any other documents referred to in it) sets out the basis on which any personal data we collect, or that is provided to us, will be processed by us.

This Policy applies to personal data collected from or about three main categories of individuals:

1. **Merchants:** Our B2B clients and their representatives, employees, directors, and ultimate beneficial owners, whose personal data is provided to us during the application, onboarding, and Know Your Business (KYB) processes, and in the general course of our contractual relationship.
2. **End-Customers:** Individuals (such as payers and beneficiaries) who are parties to transactions processed by our Merchants. We do not have a direct relationship with End-Customers; We process their personal data only as required to comply with binding legal and regulatory obligations, such as Financial Action Task Force (FATF) Recommendation 16 and its local implementations ("Travel Rule") such as Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 in the EU .
3. **Site Visitors:** Individuals who visit or interact with our website www.confirmo.com and its related websites (hereinafter "Site").

Please read the following carefully to understand our views and practices regarding personal data and how we will treat it. If you have any questions about this Privacy Policy, please contact us at privacy@confirmo.com.

2. Who We Are: The Confirmo Group and Our Roles

The Confirmo Group is a global financial services organization. Our corporate structure involves several group entities that have distinct roles in the processing of personal data. For the

purposes of the EU General Data Protection Regulation (“GDPR”) or any equivalent data protection law, these roles are as follows:

Data Controllers

A data controller is an entity that, alone or jointly with others, determines the purposes and means (the 'why' and 'how') of processing personal data.

Within the Confirmo Group, the following entities act as separate and independent data controllers. Each entity is responsible for the personal data of the specific clients it services and determines the exact purposes and means of processing for its own contractual and legal obligations:

- **Confirmo Ltd**, with its registered office at 8-34 Percy Place, Dublin 4, Dublin, D04 P5K3, Ireland. (This is our main establishment in the European Union).
- **Confirmo srl**, with its registered office at Calle Gustavo Mejia Ricard No. 54, Torre Solazar, Confirmo Group, Piso 12B, Santo Domingo, Dominican Republic.
- **Confirmo US LLC**, with its registered office at 1209 Orange St Wilmington, DE 19801, USA.

While these entities act as separate controllers, they may share personal data (such as AML/KYB information) with each other. This controller-to-controller intra-group sharing is based on our legitimate interest to manage group-wide compliance and risk, and on our legal obligations under global AML regulations.

Our Data Processor

To ensure operational efficiency and provide centralized technical support, the following entity acts as the group's internal data processor:

- **Confirmo Services s.r.o.**, with its registered office at Křižíkova 148/34, Karlín, 186 00 Praha 8, Czech Republic, ID No 22633022.

This entity processes personal data on behalf of and on the instructions of the data controllers listed above. Its role includes providing centralized IT support, customer support, technical, and operational services for the entire Confirmo Group.

3. Personal Data We Collect and How We Use It

Personal information (or personal data) means any data that can be used to identify an individual directly or indirectly. We collect different types of information depending on your interaction with us (as a Merchant, End-Customer, or Site Visitor).

A. Merchant Data (Our B2B Clients)

As a B2B business, we collect personal data from our Merchants' representatives, employees, directors, and beneficial owners. This information is collected primarily directly from you when you register to use our Site, subscribe to our service, or correspond with us. We collect this information also from cookies, from publicly available resources, public records and information about you that is openly available on the internet, and from third-party service providers and partners where necessary to provide you with the services you have requested. It is necessary for us to enter into a contract with you and to comply with our legal KYB and AML obligations.

This data includes:

- **Personal Identifiers:** Full name, permanent or current address, e-mail address, phone number, date of birth, place of birth, age, sex, citizenship, and photographs
- **Identity Documents:** Identity document type and number (e.g., passport, driver's license), country and authority of issue, date of expiry, and photographs of identification cards
- **Corporate and Financial Information:** Company name, company seat, tax or other identification numbers, bank account or card account information, transaction history, details about annual income, source of income or account funds, and net worth details.
- **Residual Information:** Information about the purpose of account use and experience with cryptoassets.

B. End-Customer Data (Travel Rule Compliance)

To comply with our binding legal obligations under global anti-money laundering regulations, including the Travel Rule, we are required to collect, verify, and transfer certain personal data from our Merchants about their End-Customers (the payers and beneficiaries of virtual asset transactions).

This information may be collected directly from the End-Customer, but it is usually provided to us by the Merchant or another Virtual/Crypto Asset Service Provider processing the transaction.

This data includes:

- Full name.
- Account number (or wallet address).
- Full physical address.
- Date and place of birth.
- Official personal document number.

C. Information We Collect Automatically

With regard to each of your visits to our site we may automatically collect the following information from Site Visitors and Merchants:

- **Technical Information:** The internet protocol (IP) address used to connect your computer to the Internet, your login information, browser type and version, time zone setting, browser plug-in types and versions, operating system, and platform.
- **Usage Information:** Details about your visit, including the full Uniform Resource Locators (URL) clickstream to, through and from our site (including date and time), products you viewed or searched for, page response times, download errors, and page interaction information (such as scrolling, clicks, and mouse-overs).

D. Information We Receive From Other Sources

We work closely with third parties and may receive information about you from them. This includes information We obtain from ID verification agencies, sanctions screening providers, and public databases for the purposes of verifying your identity (as a Merchant representative or beneficial owner) in order to comply with our obligations under anti-money laundering law and other regulations.

E. Summary of Processing Activities

The following table summarizes our main processing activities, the data involved, and the legal basis for processing under the GDPR:

Category of Data Subject	**Personal Data Collected**	**Purpose of Processing**	**Legal Basis (GDPR Art. 6)**
Merchant Representatives	Identifiers (name, email, phone, DOB), ID documents, Corporate data, Financial data	To set up and manage your account; To perform our contract; To verify identity (KYB); To comply with AML/CTF legal obligations	Performance of a Contract; Legal Obligation
End-Customers (Travel Rule)	Name, address, DOB, POB, wallet/account,	To comply with global AML/CTF	Legal Obligation

	official personal document number.	regulations (FATF Travel Rule)	
Site Visitors & Merchants	Technical Info (IP, browser), Usage Info (clickstream)	To administer and secure our site; For internal operations (analytics, research, troubleshooting)	Legitimate Interests
All Subjects	Any relevant data	To establish, exercise, or defend legal claims; To prevent fraud or other illegal activities	Legitimate Interests

4. Legal Basis for Processing Your Personal Data

We only process personal data when we have a valid legal basis to do so under the GDPR. Our processing activities rely on the following bases:

1. **Performance of a Contract (Art. 6(1)(b) GDPR):** We process personal data to carry out our obligations arising from any contracts entered into between us and our Merchants, and to provide the information, products, and services that you request from us.
2. **Compliance with a Legal Obligation (Art. 6(1)(c) GDPR):** This is a primary basis for our processing. As a financial services provider, We are subject to stringent legal and regulatory requirements. This basis covers all processing related to our KYB, AML, and CTF obligations, including identity verification and the collection and processing of End-Customer data under the Travel Rule.
3. **Legitimate Interests (Art. 6(1)(f) GDPR):** We process data for our legitimate interests, provided these are not overridden by your fundamental rights and freedoms. This includes:
    - Administering our Site and for internal operations (troubleshooting, data analysis, testing, research).
    - Keeping our Site and services safe and secure, and preventing potentially prohibited or illegal activities.
    - Improving our services and ensuring content is presented effectively.
    - Managing our corporate structure, including sharing information within the Confirmo Group for administrative and compliance purposes.

4. **Consent (Art. 6(1)(a) GDPR):** We will only rely on consent for processing that is not covered by the bases above. This is primarily limited to sending direct marketing communications to new customers. Where we rely on consent, you have the right to withdraw it at any time by contacting us at privacy@confirmo.com.

5. Disclosure and Sharing of Your Information

We are committed to allowing your personal data to be accessed only by those who have a legitimate purpose to do so. We may share your information in the following circumstances:

A. Intra-Group Sharing

We may share your personal data with any member of the Confirmo Group, which includes the other data controllers (Confirmo Ltd, Confirmo srl, Confirmo US LLC) and our internal processor (Confirmo Services s.r.o.) as defined in Section 2. This sharing is necessary for our legitimate interests in providing centralized operations, security, risk management, and for complying with our group-wide legal and regulatory AML/KYB obligations.

B. Third-Party Sharing

We may share Your information with selected third parties, including:

- **Business partners, suppliers and sub-contractors** for the performance of any contract we enter into with them or you, such as IT and cloud hosting providers, and technical support services.
- **Identity verification agencies, credit reference agencies, and analytics providers** for the purposes of verifying the personal data you have provided and complying with our KYB/AML obligations.
- **Law enforcement agencies, officials, or other third parties** when we are compelled to do so by a subpoena, court order, or other respective legal procedure, or if we are under a duty to disclose or share your personal data in order to comply with any legal obligation.
- **Fraud and Risk Management:** We may exchange information with other companies and organizations for the purposes of fraud protection and risk reduction.

6. International Data Transfers

As a global organization, your personal data may be transferred to, and processed in, jurisdictions outside of the European Economic Area (EEA) to facilitate our global operations. This includes transfers to our group entities and third-party service providers located in:

- **The United States**
- **The Dominican Republic**

We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and applicable data protection laws (specifically Chapter V of the GDPR).

Legal Safeguards for Your Data

We rely on the following legal mechanisms to legitimize these international transfers:

1. **Adequacy Decisions:** We may transfer data to countries that the European Commission has determined provide an adequate level of data protection.
2. **EU-U.S. Data Privacy Framework (DPF):** For transfers to our entity in the United States (Confirmo US LLC), We rely on the European Commission's adequacy decision for the EU-U.S. Data Privacy Framework. Confirmo US LLC shall self-certify its adherence to the DPF Principles. You can verify our participation and certification status on the official DPF List maintained by the U.S. Department of Commerce.
3. **Standard Contractual Clauses (SCCs):** For transfers to the **Dominican Republic**, a country for which no adequacy decision currently exists, We will use the European Commission's approved Standard Contractual Clauses (SCCs). SCCs will also be used as a safeguard for transfers to any of our service providers in the U.S. that are not certified under the DPF. These clauses contractually oblige the data importer to protect your data to the high standards required by the GDPR.

7. Data Security and Retention

Data Security

We are committed to maintaining the confidentiality, integrity, and availability of your personal data. We achieve this by implementing robust technical and organizational measures, including the use of firewalls and encryption, alongside strict internal controls designed to prevent unauthorized access. Access to personal data is authorized only for those employees who require it to fulfil their job responsibilities

Our security program incorporates the following key technical and organizational measures:

1. Encryption Throughout the Data Lifecycle:

- **Data at Rest:** We utilize encrypted databases for the storage of personal data on our secure servers.
- **Data in Transit:** We ensure that all communication channels are secured. Any transactions and data transmission will be secured using current industry-standard Transport Layer Security (TLS) encryption.

2. Strict Access Control and Authentication:

- **Limited Access:** Access to personal data is governed by Role-Based Access Control (RBAC) to ensure that access is authorized only for those employees who require it to fulfil their job responsibilities.
- **Strong Authentication:** We mandate Multi-Factor Authentication (MFA) for all authentication purposes. To further prevent unauthorized access, we utilize forceful security keys or passkeys, which makes remote phishing nearly impossible for accessing our systems.

3. Continuous Security Assessment and Incident Management:

- To assess and maintain the effectiveness of our security standards, we routinely conduct vulnerability scanning and regular penetration testing.
- We maintain a formal Data Security Incident Response Plan to ensure that we can rapidly detect, contain, and recover from any security incidents, thereby protecting the integrity and confidentiality of your data.

Where we have given you (or where you have chosen) a password which enables you to access certain parts of our site, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Risk Disclosure:

Once we have received your information, we use strict procedures and security features to try to prevent unauthorized access. However, you acknowledge that the transmission of information via the internet is inherently not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; **any transmission to our site is therefore undertaken at your own risk**.

Data Retention

We will only retain your personal data for as long as is necessary to fulfil the purposes for which we collected it.

Please note that as a regulated financial services provider, we are subject to legal and regulatory retention requirements. We are required to retain personal data related to our AML, KYB, and Travel Rule obligations for mandatory statutory periods. These laws may require us to hold your data for several years (e.g., ten years or more) after our business relationship with you (or our Merchant) has ended. We do this to satisfy legal, accounting, or reporting obligations, or to resolve disputes.

8. Your Data Protection Rights

If you are a resident of the EEA, you have the following rights under the GDPR. You can exercise these rights at any time by contacting us at privacy@confirmo.com.

- **The right to access:** You have the right to request copies of your personal data.
- **The right to rectification:** You have the right to request that we correct any information you believe is inaccurate or complete information you believe is incomplete.
- **The right to erasure (Right to be Forgotten):** You have the right to request that we erase your personal data, under certain conditions. Please note that this right may be limited by our legal obligations to retain data, particularly for AML purposes.
- **The right to restrict processing:** You have the right to request that we restrict the processing of your personal data, under certain conditions.
- **The right to object to processing:** You have the right to object to our processing of your personal data, under certain conditions, particularly processing based on our legitimate interests.
- **The right to data portability:** You have the right to request that we transfer the data that we have collected to another organization, or directly to you, under certain conditions.
- **The right to withdraw consent:** If we are processing your data based on your consent , you have the right to withdraw that consent at any time.

When we receive a request, we may take steps to verify your identity before complying with the request to protect your privacy and security. Your rights are not absolute, and access may be denied when it is frivolous, vexatious, or for which access is not otherwise required by applicable Law.

You may exercise your rights in respect of and against the specific Confirmo entity that acts as the data controller for your data. However, we have designated privacy@confirmo.com as a central contact point to assist you with any request, regardless of which entity is the controller.

9. Data Protection Officer (DPO)

Under the GDPR, a group of undertakings may appoint a single Data Protection Officer (DPO). The Confirmo Group has appointed a Group DPO to oversee our data protection compliance, provide advice, and act as a point of contact for data subjects and supervisory authorities.

Our DPO is responsible for monitoring compliance with the GDPR and this Policy across all entities in the Group. If you have any questions or concerns specifically for our DPO, you can contact them at: privacy@confirmo.com (Please mark your subject line "For the Data Protection Officer")

10. Cookies and Tracking Technologies

Our Site may use cookies to distinguish you from other users. This helps us to provide you with a good experience when you browse and use our Site and also allows us to improve our Site. A user may choose to set their web browser to refuse cookies, or to alert you when cookies are being sent. If they do so, note that some parts of the Site may not function properly.

For more detailed information on the cookies we use and the purposes for which we use them, please see our separate Cookies Policy.

11. Complaints and Supervisory Authority

We are committed to resolving any questions or concerns you may have about our use of your information. We encourage you to contact us first at privacy@confirmo.com in order to resolve your issue informally.

If you are an EEA resident, you have the right to lodge a complaint with a data protection supervisory authority. As our main establishment in the European Union is in Ireland (see Section 2), our Lead Supervisory Authority under the GDPR for our EU operations is the Irish Data Protection Commission (DPC).

If you are not satisfied with our response or believe we are processing your data not in accordance with the law, you may refer your complaint to the DPC.

Their contact details are:

- **Website:** https://www.dataprotection.ie
- **Contact Form:** https://www.dataprotection.ie/en/contact/how-contact-us
- **Postal Address:** Data Protection Commission, 6 Pembroke Row, Dublin 2, D02 X963, Ireland

12. Changes to Our Privacy Policy

Any changes we may make to our Privacy Policy in the future will be posted on this page and, where appropriate (material change), notified to you by e-mail. Please check back frequently to see any updates or changes to our Privacy Policy.

13. Contact Us

Questions, comments and requests regarding this Privacy Policy are welcomed and should be addressed to our contact point: privacy@confirmo.com.