# Privacy Policy

Conio S.r.l. – Information notice pursuant to article 13 of Regulation (EU) 2016/679

Last updated: 11/11/2026

## 1. Introduction and scope

This Privacy Policy explains how Conio S.r.l. processes the personal data of members of the 499P Hyperclub programme (the "Programme") who use the platform 499P SDK Integration (the "Platform"). It is provided under article 13 of Regulation (EU) 2016/679 ("GDPR").

Through the Platform, Conio provides two crypto-asset services regulated under Regulation (EU) 2023/1114 ("MiCAR"): custody and administration of crypto-assets on behalf of clients, and exchange of crypto-assets for funds involving EURC, an e-money token. All other Platform features fall outside MiCAR Private Messages and Auction. This policy covers the processing for both regulated and non-regulated services. The services are governed by the Platform's Terms and Conditions and the custody agreement (together, the "Terms").

This policy applies to members who are individuals. For corporate members, it also applies to their legal representatives, attorneys, authorised signatories and beneficial owners (all referred to as "you" or the "Member" below).

This policy does not cover processing by Ferrari for the Programme itself. Ferrari's processing is explained in its own privacy notice (see section 2.3).

The Platform may show you additional, specific notices about particular features or data. Where it does, those notices supplement this policy.

## 2. Data controllers and contact details

### 2.1 Conio

The controller of the processing described in this policy is **Conio S.r.l.** ("Conio", "we"). Its registered office is at Via Agostino Bertani 6, 20154 Milan, Italy. Conio is a crypto-asset service provider authorised under MiCAR.

- General contact: info@conio.com
- Data protection requests: dpo@conio.com

### 2.2 Data Protection Officer

Conio has appointed a Data Protection Officer. You can contact the DPO at **dpo@conio.com** with any question about the processing of your personal data or to exercise your rights.

### 2.3 Ferrari as an independent controller

Ferrari S.p.A., with registered office at Via Emilia Est 1163, Modena, Italy, runs the Programme. Ferrari decides independently how to process members' data for membership, events, hospitality and its own communications. For that processing, Ferrari is an **independent controller**, separate from Conio. Its privacy notice is available at https://www.ferrari.com/it-IT/my-ferrari-privacy-policy.

Ferrari does not send Conio any member data: you provide all the data Conio needs directly to Conio. Conio sends Ferrari only the limited data needed for the auction of the tokenised Ferrari 499P, as described in section 5.2. Conio does not process your data for Ferrari's purposes, and Ferrari has no access to your KYC, AML or account data.

## 3. Personal data we process

We collect personal data from you directly and from the providers we use to verify your identity and screen transactions.

| Category | Examples |
|---|---|
| Identification and contact data | Name, date and place of birth, nationality, residential address, email, phone number, tax code / TIN |
| Identity verification (KYC) data | Copy of identity document, selfie or video for liveness checks, collected through Sumsub, proof of address |
| AML due diligence data | PEP status, sanctions and adverse-media screening results, occupation, source of funds and wealth, purpose of the relationship, risk rating |
| Corporate member data | For legal representatives, signatories and beneficial owners: identification, KYC and AML data; role and powers of representation |
| Crypto-asset and transaction data | Custody account details, wallet addresses, token holdings, transfer history (including member-to-member transfers), auction participation |
| Travel Rule data | Originator and beneficiary name, wallet address, account number, address or ID number, as required by Regulation (EU) 2023/1113 |
| Payment and banking data | IBAN and bank account holder, payment details |
| Communications | Support requests, emails and chat messages exchanged with us |
| Technical and usage data | IP address, device identifiers, log files, session and navigation data, crash reports |
| Tax reporting data | Data needed for reporting under Directive (EU) 2023/2226 (DAC8) and Italian tax law |

We do not intend to process special categories of data (art. 9 GDPR) or data on criminal convictions and offences (art. 10 GDPR). The exception is where AML screening reveals such data incidentally; in that case we process them only as required by law.

Providing the data marked as mandatory on the Platform is necessary to enter into the Terms and to comply with anti-money laundering law. If you do not provide them, we cannot onboard you or provide our services.

## 4. Why we process your data and on what legal basis

### 4.1 Performance of the contract – art. 6(1)(b) GDPR

- Onboarding you to the Platform and managing your account
- Providing custody and administration of your crypto-assets, including the Programme tokens
- Executing transfers, including member-to-member transfers in line with the Terms
- Handling your requests and providing customer support
- If you take part in the auction of the tokenised Ferrari 499P, sending Ferrari the information it needs to check your eligibility and run the auction correctly (section 5.2)

### 4.2 Compliance with legal obligations – art. 6(1)(c) GDPR

- Customer due diligence, ongoing monitoring, record keeping and suspicious transaction reporting under Legislative Decree 231/2007
- Sanctions screening under EU restrictive measures
- Collecting, checking and sending Travel Rule data with crypto-asset transfers under Regulation (EU) 2023/1113
- Meeting MiCAR conduct, safekeeping and record-keeping requirements
- Tax reporting under DAC8 and Italian tax law
- Responding to requests from competent authorities and courts

### 4.3 Legitimate interest – art. 6(1)(f) GDPR

We have balanced each interest below against your rights and freedoms. You can object at any time (section 9).

| Purpose | Our interest | Safeguards for you |
|---|---|---|
| Fraud prevention and platform security | Protecting your account, your assets and our systems from fraud and unauthorised use | Limited to detecting anomalous or suspicious activity; data kept only as long as checks and possible disputes require |
| Verification and reconciliation of operations | Making sure every transfer and booking is executed and recorded correctly | Access limited to authorised support and reconciliation staff; no assessment of your profile for other purposes |
| Service improvement and statistics | Understanding how the Platform is used so we can improve it | Pseudonymised and aggregated data only; no analysis of individual behaviour; anything shared externally is irreversibly anonymised |
| Defence of legal claims | Establishing, exercising or defending our rights | Only data relevant to the claim; kept until the claim is finally resolved |

### 4.4 No marketing and no automated decisions

We do not use your data for marketing or for profiling. We do not make decisions about you based solely on automated processing that produce legal effects concerning you or similarly significantly affect you (art. 22 GDPR).

### 4.5 Cookies and similar technologies

The Platform uses technical cookies needed for it to work. These do not require consent. We use analytics cookies without consent only where they are configured as anonymised, as the Italian Data Protection Authority's 2021 cookie guidelines allow. Any other cookie or tracking tool is used only with your consent, collected through the cookie banner.

## 5. Who we share your data with

### 5.1 Recipients

We never publish your data. We share them only with the following recipients, and only as far as each purpose requires:

- **Conio staff and collaborators** who are authorised and bound by confidentiality, each within their role

- **Service providers** acting as processors under art. 28 GDPR (section 6)
- **Other crypto-asset service providers and financial intermediaries** involved in your transfers, to the extent required by the Travel Rule
- **Competent authorities**, including the Bank of Italy, CONSOB, the Financial Intelligence Unit (UIF), the Italian Revenue Agency and judicial authorities, where the law requires it
- **Professional advisers, auditors and insurers**, who are bound by professional secrecy or confidentiality
- **Ferrari S.p.A.**, as an independent controller, only for the data listed in section 5.2 when you take part in the auction

You can ask for the current list of processors by writing to dpo@conio.com.

### 5.2 Data shared with Ferrari for the auction

If you take part in the auction of the tokenised Ferrari 499P, Conio may send Ferrari the following data, on Ferrari's request and only for that auction:

- Your identifier as a Hyperclub member membership ID or name
- The number of Ferrari 499P Tokens you hold at the date set for the auction

Ferrari uses these data to check whether you meet the requirements to take part in the auction and to run it correctly. Ferrari processes them as an independent controller, under its Hyperclub Membership agreement 2026-2027 (art. 6(1)(b) GDPR) and its own privacy notice.

Conio does not send Ferrari any other data. This includes your peer-to-peer transfers, transaction values, identity documents and AML information.

## 6. Service providers

We use the following providers, appointed as processors where required.

| Provider | Service | Legal basis | Location |
|---|---|---|---|
| Amazon Web Services EMEA SARL | Hosting and backend infrastructure | Contract | EU (Ireland, Milan) |
| Sum and Substance Ltd (Sumsub) | Identity verification and document checks | Legal obligation | United Kingdom (adequacy decision) |
| Refinitiv - London Stock Exchange | Sanctions, PEP and adverse-media screening; blockchain analytics | Legal obligation | United Kingdom |
| Notabene | Exchanging Travel Rule data with other crypto-asset service providers | Legal obligation | EU |
| Intercom R&D Unlimited Company / Intercom Inc. | Customer support and messaging | Contract; legitimate interest | EU |
| Google Ireland Limited – Firebase Cloud Messaging | Push notifications | Contract | EU / US |
| Google Ireland Limited – Crashlytics, Performance Monitoring | Crash reporting and performance monitoring | Legitimate interest | EU / US |

For system maintenance, the Platform and these providers may collect log files containing personal data such as your IP address.

**Device permissions.** On mobile devices, the Platform asks for camera access only to capture identity documents and images for identity checks. You can revoke this permission at any time in your device settings, but you will then be unable to complete identity verification.

## 7. Transfers outside the European Economic Area

We store your data on servers in the European Union, in Ireland and Milan. Some providers, or their sub-processors, are in third countries, mainly the United States and the United Kingdom. We transfer data outside the EEA only on one of these grounds:

- An adequacy decision of the European Commission (art. 45 GDPR), including the EU-US Data Privacy Framework for certified recipients
- Standard Contractual Clauses approved by the European Commission (art. 46 GDPR), with supplementary measures where needed

Travel Rule data may go to a crypto-asset service provider in a third country when you send crypto-assets to a wallet held there. That transfer is necessary to carry out the transfer you requested (art. 49(1)(b) GDPR) and to comply with Regulation (EU) 2023/1113.

You can obtain a copy of the safeguards by writing to dpo@conio.com.

## 8. How long we keep your data

| Data | Retention period |
|---|---|
| Account, KYC/AML, transaction and Travel Rule data | Duration of the relationship plus 10 years after it ends (art. 31, Legislative Decree 231/2007; tax and MiCAR record-keeping) |
| Data for legal claims | Until the decision becomes final |
| Customer support communications | 24 months after closure of the request, or 5 years if linked to a complaint or claim |
| System logs and security data | Up to 12 months, unless authorities need them for longer to investigate offences |
| Onboarding data of people who do not become members | 12 months, unless anti-money laundering law requires longer |

When these periods end, we delete your data or irreversibly anonymise them.

## 9. Your rights

Within the limits set by law, you have the right to:

- **Access** your data and receive a copy (art. 15 GDPR)
- **Rectify** inaccurate or incomplete data (art. 16 GDPR)
- **Erase** your data (art. 17 GDPR), unless we must keep them by law, for example under anti-money laundering rules
- **Restrict** processing (art. 18 GDPR)
- **Data portability**: receive the data you provided in a structured, machine-readable format, where processing is based on contract or consent (art. 20 GDPR)
- **Object** at any time, on grounds relating to your particular situation, to processing based on legitimate interest (art. 21 GDPR)

- **Withdraw consent** at any time, where processing is based on consent, without affecting processing carried out before withdrawal (art. 7(3) GDPR)
- **Lodge a complaint** with the Garante per la protezione dei dati personali (www.garanteprivacy.it) or the supervisory authority of your EU country of residence, or bring legal action

Some rights may be limited under article 2-undecies of the Italian Privacy Code (Legislative Decree 196/2003). For example, access may be restricted where it could prejudice anti-money laundering investigations.

**How to exercise your rights.** Write to dpo@conio.com or use the form at link. Requests are free of charge. We reply without undue delay and in any case within one month; for complex requests this may be extended by two further months, and we will tell you if so. We inform recipients of any rectification, erasure or restriction unless this is impossible or involves disproportionate effort.

## 10. Changes to this policy

We may update this policy, for example when the Programme or the law changes. We will notify you on the Platform and, where possible, by email before the changes take effect. Where a change affects processing based on consent, we will ask for your consent again where required.