

GLOBAL NETWORK AND PLATFORM PRIVACY POLICY

Private Community[®] & 'Combine[®]' Artificial Intelligence Platform

1. GENERAL FRAMEWORK AND DATA CONTROLLERSHIP (GDPR ARTS. 13 AND 14)

This Privacy Policy describes how the personal data of users, affiliates, members and visitors ("Users" or "Members") are collected, used, shared and protected within the global franchise network known as "Private Community[®]", the related websites, mobile applications and the associated Artificial Intelligence platform known as "Combine[®]" (the "Services").

A. Global Data Controller

Powered Community Worldwide Pte Ltd, with registered office at 22 Sin Ming Lane, #04-82 Midview City, Singapore 573 969, Unique Entity Number (UEN) 202 537 854Z, holds the exclusive Worldwide Master Licence for the commercial exploitation and management of the franchise and the Combine[®] platform (whose trademarks and intellectual property rights belong to their respective founders and licensors) - Privacy/Legal contact email: privacy@privatecommunity.net

B. Operational Data Processors (Local Master Franchisees and Territorial Affiliates)

For the operational management of the network in each territory, coordination of service distribution, country-level accounting, onboarding and the operational management of members, Powered Community Worldwide Pte Ltd (PCW) engages:

- **Local Master Franchisees:** independent entities that manage the network in their respective national territories and act as Data Processors pursuant to Article 28 GDPR on behalf of PCW.
- **Affiliates:** individual operating locations and local partners forming part of the Private Community[®] network, appointed as Data Processors pursuant to Article 28 GDPR and entrusted with membership enrolment, local support, direct contact and the provision of local services to members in their area.

Transparency Notice: The company names, tax details and privacy contact addresses of the relevant Local Master Franchisee and the affiliates operating in the User's country are available on the web portal or may be requested from the Data Controller.

C. Technical and AI Infrastructure Sub-processor

The development, maintenance, cybersecurity, systems administration and server management of the Combine[®] Artificial Intelligence platform are entrusted exclusively to Delfisoft S.r.l. ("Delfisoft"), with registered office in Agliè (TO), Italy, acting as an External Sub-processor bound by specific contractual instructions (Data Processing Agreement - DPA pursuant to Article 28 GDPR).

2. CATEGORIES OF PERSONAL DATA COLLECTED

Depending on the User's interactions with the Services, the following categories of data are processed:

1. Identification and Contact Data: First name, surname, company name, business role, email address, telephone number, login credentials (username and password) and profile photograph.

2. Transaction and Billing Data: Data relating to network membership, membership fees, subscriptions, payment history, tax and billing information. Depending on the payment method available in the relevant country or through the relevant territorial Affiliate:

Online/Card Payments: These are managed directly by authorised Payment Service Providers (PSPs) operating in the relevant country; the Platform and the network do not store complete payment-card data.

Bank Transfers and Direct B2B Payments: Banking data are processed by Powered and/or the Data Processors responsible for accounting, collections and invoicing.
3. Technology and Usage Data (Log Files): IP addresses, device identifiers, browser type, operating system, pages visited, access times, crash diagnostics and network performance.
4. Data entered into the 'Combine®' AI Platform (Prompts and Input Data): Text, files, documents, business data, prompts or questions entered by the User into the AI system for the development of business strategies (Elevate to Admiration® Method).
5. Special Categories of Data (Sensitive Data under Article 9 GDPR): Use of the ordinary services does not require the provision of sensitive data (e.g. health data, political opinions or religious beliefs). If the User voluntarily chooses to enter such data into the platform or AI system, they will be processed only with separate, explicit consent.

3. PURPOSES AND LEGAL BASES OF PROCESSING

The processing of personal data is based on the following legal grounds (Articles 6 and 9 GDPR):

Purpose of Processing	Categories of Data Involved	Legal Basis
<u>Performance of the Contract</u> : Account creation, management of membership in Private Community®, provision of access to the Combine® platform, customer support, and organisation of webinars and training events.	Identification Data, Contact Data, Transaction Data, Credentials.	Article 6(1)(b) GDPR: Performance of the contract or steps taken prior to entering into a contract.
<u>Provision of AI Services through Combine®</u> : Generation of outputs, strategic reports and organisational analyses in response to prompts/documents uploaded by the User.	Input Data, Prompts, Uploaded Documents.	Article 6(1)(b) GDPR: Performance of the services requested by the User.
<u>Security and Fraud Prevention</u> : Access monitoring, prevention of cyberattacks, mitigation of security risks, rate limiting and resolution of technical malfunctions.	Technology Data, IP Addresses, System Logs.	Article 6(1)(f) GDPR: The Data Controller's legitimate interest in ensuring infrastructure security.
<u>Network Visibility and Member Directory</u> : Inclusion of the User's company profile in the directory reserved for other network members to facilitate networking and B2B collaboration.	Identification Data, Role, Professional Contact Details, Photograph.	Article 6(1)(b) GDPR (for the internal network) and Article 6(1)(a) GDPR (consent for optional extended visibility).

Purpose of Processing	Categories of Data Involved	Legal Basis
<u>Compliance with Legal Obligations:</u> Maintenance of accounting records, tax compliance and responses to requests from judicial or data-protection authorities.	Tax Data, Transactions, Logs.	Article 6(1)(c) GDPR: Compliance with legal obligations.
<u>Direct B2B Marketing:</u> Communications concerning services or events similar to those already purchased (soft opt-in).	Business Email Address, Name.	Article 6(1)(f) GDPR: Legitimate interest (with the right to opt out at any time).

4. RULES GOVERNING 'COMBINE®' ARTIFICIAL INTELLIGENCE

With regard to the use of Artificial Intelligence ("AI") modules:

1. Use of Prompts and Service Personalisation (Dedicated Fine-Tuning): The personal data, confidential information, text and files uploaded by the User ("Prompt/Input") are processed and used by Combine® solely to provide the service and to personalise/train the platform's responses and functions to meet the specific needs of the individual User or the organisation that submitted them. This processing is necessary for the performance of the contract and the provision of the advanced functions of the Service requested by the User (Article 6(1)(b) GDPR).
2. No training of general or third-party models: Personal data and confidential information submitted by an individual User are never used, sold or shared with third parties for the training or retraining (training/fine-tuning) of general, public or third-party artificial-intelligence models, nor to profile the User for the benefit of other members or parties outside the platform. The submitted data remain segregated and confidential within the environment of the User/Company that provided them.
3. No Fully Automated Decision-Making: The Combine® platform provides strategic support tools. No decision producing legal or similarly significant effects on the User is made solely on the basis of automated AI processing without human intervention (pursuant to Article 22 GDPR).

5. COMMUNICATION, DISCLOSURE AND INTERNATIONAL TRANSFERS OF DATA

For purposes connected with the performance of the franchise agreement, provision of the Combine® platform and management of the global network, Users' personal data may be disclosed to specific recipients both within and outside the European Union.

5.1 Technology Service Providers and Cloud Providers (Processors/Sub-processors): Delfisoft S.r.l. (for the development, technical management and maintenance of the Combine® platform), as well as leading third-party providers of international cloud-server and database infrastructure (including, by way of example, Microsoft Ireland Research / Microsoft Corporation - Azure, or equivalent providers) that supply hosting and data-storage services.

5.2 Categories of Recipients

Personal data may be shared with:

- *Group Companies, Master Franchisees and Local Affiliates:* For the management of territorial chapters, organisation of B2B events and publication of company profiles in the directory reserved for network members.
- *Technology and Systems Service Providers (Processors/Sub-processors):* Including Delfisoft S.r.l. (for the development, technical management, support and maintenance of the Combine® platform servers), as well as

third-party providers of cloud hosting, server infrastructure, cybersecurity services and email-delivery platforms.

- *Public Authorities and Supervisory Bodies:* Where required by law or for compliance with tax and accounting obligations by local operating entities.

5.3 Transfers of Data Outside the EU and Onward Transfers (Chapter V GDPR)

As the Global Data Controller, Powered Community Worldwide Pte Ltd, has its registered office in Singapore and operates as the parent company of a worldwide franchise, personal data relating to individuals located in the European Economic Area (EEA) are transferred to third countries outside the European Union. Pursuant to Chapter V GDPR (Articles 44-50), all direct transfers of data from the EU to Singapore, as well as any onward transfers by Powered Community Worldwide Pte Ltd to Master Franchisees, affiliates or third-party technology providers located in other non-EU countries, take place subject to one of the following safeguards:

1. *Standard Contractual Clauses (SCCs):* Adoption of the SCC modules approved by the European Commission through Implementing Decision (EU) 2021/914 (including the specific modules governing onward transfers from a controller/processor outside the EU to another controller/processor outside the EU), which bind overseas recipients to the same data-protection standards established by the GDPR.
2. *Adequacy Decisions:* Transfers to third countries that the European Commission has officially recognised as ensuring an adequate level of personal-data protection pursuant to Article 45 GDPR.
3. *EU-U.S. Data Privacy Framework (DPF):* Limited to transfers to, or the use of, cloud/IT service providers established in the United States of America that are duly listed and active in the register of entities certified under the DPF.

The User may request a copy of the contractual safeguards adopted for data transfers at any time by writing to: privacy@privatecommunity.net.

6. PROCESSING SECURITY, RESILIENCE AND BUSINESS CONTINUITY

6.1 Basic Technical and Organisational Measures

In accordance with Article 32 GDPR, the Data Controller (Powered Community Worldwide Pte Ltd) and the Technical Sub-processor (Delfisoft S.r.l.) adopt appropriate technical and organisational measures to ensure a level of security proportionate to the risk and to protect personal data and confidential information against destruction, loss, alteration, unauthorised disclosure, or accidental or unlawful access. These measures include, by way of example:

- Encryption protocols for communications and transmission channels (SSL/TLS);
- Granular control and profiling of logical access to servers and databases;
- Firewall systems, network-traffic monitoring and automated protection against cyberattacks (including rate-limiting mechanisms);
- Segregation and logical isolation of business data and prompts entered into the Combine® platform.

6.2 Cloud Security Architecture and Disaster-Recovery Services

Data on the Combine® platform are stored in high-security cloud environments managed by leading international infrastructure providers (e.g. Microsoft or equivalent providers).

- *Standard Profile:* Includes security, encryption and backup measures at standard frequencies and under standard procedures.
- *Optional Disaster-Recovery Module:* To address complex cyberattacks or critical incidents, an advanced Disaster-Recovery module is available, providing frequent backup procedures and priority restoration.

- Technology Limitations and Accidental Events / Force Majeure: The User acknowledges that activation of the Disaster-Recovery module provides enhanced security protection but does not guarantee the absolute infallibility of data restoration in the event of force majeure, accidental events, disasters, widespread telecommunications-network failures, or unforeseeable and exceptional cyberattacks (e.g. zero-day attacks or large-scale breaches directly affecting the infrastructure of an external cloud provider) beyond the reasonable and direct control of Powered, the Data Processors and Delfisoft.

6.3 Management of Personal Data Breaches and Technology Limitations

In the event of a personal data breach, the Data Controller will promptly fulfil the notification obligations owed to the competent Supervisory Authority and, where applicable, communicate the breach to data subjects in accordance with Articles 33 and 34 GDPR.

The User acknowledges that any loss or corruption of data resulting from accidental events, force majeure, unlawful third-party interference or cyberattacks directed at the infrastructure of an external cloud provider is an inherent risk of using information systems connected to the internet. Exclusions of liability for indirect damage and operational indemnities arising from third-party hacker attacks, force majeure or failure to restore data - including where the Disaster-Recovery service has been subscribed to - are governed by the agreement and the General Terms and Conditions / B2B Terms of Service.

7. DATA RETENTION

Personal data are retained for no longer than is strictly necessary to fulfil the purposes for which they were collected:

- Membership / Franchising Data: Retained for the entire duration of the contractual relationship and for 10 years after its termination, in compliance with tax and legal obligations.
- Combine® Prompts and Logs: Technical logs and prompts are retained for the period strictly necessary for the operation and security of the service, except where they are archived in anonymised form or required for the establishment, exercise or defence of legal claims.
- Marketing Data: Retained until consent is withdrawn or the right to object is exercised (opt-out).

8. RIGHTS OF DATA SUBJECTS

Users may exercise the rights guaranteed by the GDPR at any time:

1. Right of Access and Rectification: Obtain confirmation as to whether their data exist, access those data and request their correction.
2. Right to Erasure ('Right to be Forgotten'): Request the deletion of data that are no longer necessary or have been processed unlawfully.
3. Right to Restriction and Objection: Object to processing based on legitimate interests or to direct marketing.
4. Right to Data Portability: Receive the data provided in a structured, commonly used format.
5. Right to Withdraw Consent: Withdraw consent at any time without affecting the lawfulness of processing carried out before its withdrawal.
6. Complaint to a Supervisory Authority: Lodge a complaint with the national data-protection authority or the Supervisory Authority of the EU Member State of residence.

To exercise their rights, Users may submit a written request to the following email address: privacy@privatecommunity.net.