Privacy Policy

Maxiq Limited, d/b/a 16 Persons (collectively, "**16 Persons**," "**we**," "**us**" or "**Company**") respects the privacy of its website users ("**User(s)**" or "**you**") and is committed to protecting Users' personal information. We believe you have a right to know our practices regarding the information we may collect and use about you when you use our website at https://16persons.com/ and its subdomains (collectively, the "**Site**"). Please read the following carefully to understand 16 Persons' views and practices regarding your personal information and how 16 Persons will treat it. Capitalized terms not defined here have the meanings given in our **Terms of Use** at https://16persons.com/terms-conditions/, into which this Privacy Policy is incorporated by reference.

Table of Contents

1) Who We Are

Controller. The controller of your personal data is **Maxiq Limited,** with the registered office at Markou Drakou, 2A, Livadia 7060, Larnaca, Cyprus ("**16 Persons**," "**we**," "**us**," or "**Company**").

What this Policy covers. This Privacy Policy applies to your use of https://16persons.com/ and its subdomains, and to services we provide through the Site, including **16 Persons** results (e.g., Detailed personality report) and the **IQBooster** brain-training service (together, the "**Services**").

Relationship to our Terms. This Privacy Policy forms part of, and is incorporated into, our **Terms of Use** available at https://16persons.com/terms-conditions/.

Global application; California notice. This Policy applies globally. **California residents** should also review the **California Privacy Notice (Section 12)** for information specific to California law.

What's not covered. This Policy does not apply to third-party websites, services, or payment platforms that are not controlled by us (for example, certain independent payment providers); their privacy practices are governed by their own policies.

2) Key Definitions

- **Personal Data** — any information that identifies or relates to an identified or identifiable individual (for example, name, email, IP address, account ID, purchase history, test results/score, support records).
- **Processing** — any operation performed on Personal Data, such as collection, recording, organization, storage, use, disclosure, transmission, or deletion.
- **Controller** / **Processor** — under GDPR: the **Controller** determines the purposes and means of Processing Personal Data; a **Processor** processes Personal Data on behalf of the Controller under a contract.
- **Service Provider** — under California law, an entity that processes Personal Data for a **business purpose** for us and is contractually restricted from using the data for other purposes (similar to a GDPR Processor).
- **Third Party** / **Independent Controller** — an entity that is **not** our Service Provider and determines its own purposes/means of processing (e.g., certain payment platforms like PayPal when acting on their own behalf).
- **Sale** (California) — disclosing or making available Personal Data to a Third Party **for monetary or other valuable consideration**, as defined by California law.
- **Share** (California) — disclosing or making available Personal Data to a Third Party **for cross-context behavioral advertising** (targeting based on activity across sites/apps), whether or not money is exchanged.
- **Targeted Advertising** — showing ads to you based on your activities across non-affiliated sites, applications, or services over time (also called cross-context behavioral advertising).
- **Sensitive Personal Information (SPI)** — certain data defined by California/GDPR as sensitive (e.g., **account log-in with password**, precise geolocation, government ID numbers, financial account credentials, health/biometric data). We describe any SPI we process and its uses in Sections 3–5 and 12.
- **Cookies / Tracking Technologies** — small files, pixels, SDKs, or similar tech stored on or read from your device or browser to enable core functions, analytics, security/fraud prevention, and (where applicable) advertising. Your choices are described in **Cookie Settings** and Section 6.
- **Cookies/SDK Preferences** — your selections in our consent or preference tools that control non-essential cookies/SDKs (e.g., analytics, advertising).

3) What We Collect

We collect the types of information described below when you use the Site and Services, contact us, or otherwise interact with us. Some of this information is collected directly from you; some is collected automatically from your device/browser; and some may be received from service providers (e.g., payment and analytics).

3.1 Information you provide to us

- **Account & contact details.** Name, email address, account credentials (see **SPI** note below), communication preferences.
- **Test participation & results.** Your engagement with 16 Persons (for example, questions you answer, selected answers, timestamps, test date/time) and outputs such as **Personality results** and **Detailed report** derived from your participation.
- **Support communications.** Messages you send via forms or email (including Test ID numbers you provide), and our correspondence with you for quality assurance and service improvement.
- **Marketing choices.** Your subscriptions/unsubscribe settings and related preferences.

3.2 Information collected automatically (device, usage, cookies)

- **Device & technical data.** Browser type/version, OS, screen resolution, language settings, device identifiers (e.g., IP address, cookie ID, mobile/advertising IDs where applicable), and diagnostic logs.
- **Usage & interaction data.** Pages viewed, links clicked, time on page, referring/exit pages, and clickstream/activity on the Site and within the Services.
- **Approximate location. IP-based** location for fraud/security, service localization, and analytics. We **do not** collect **precise** (GPS-level) geolocation.
- **Cookies/SDKs.** We and our service providers use cookies, pixels, tags, and similar technologies for core functionality, security, analytics, and (where applicable) advertising. See **Section 6 (Cookies, Analytics & Advertising)** and **Cookie Settings** for details and choices.

3.3 Information related to purchases and payments

- **Payment processing.** If you make a purchase, your payment is handled by our payment providers (e.g., Stripe, SolidGate, **PayPal**). We **do not store full payment card numbers** on our systems. We may receive **tokenized references**, transaction metadata, and (where applicable) the **last four digits** of your card for records, fraud prevention, and customer support. Some payment providers (e.g., PayPal) act as **independent controllers**—their use of your data is governed by their own privacy policies. We **do not store full payment card numbers or CVV** on our systems; we receive tokenized references and limited metadata from our payment providers.

3.4 Information from other sources

- **Service providers & partners.** We may receive limited data from analytics, anti-fraud, or support tools (for example, aggregate usage metrics, error diagnostics, or coarse location derived from IP).
- **Public or commercial sources.** Where permitted by law, we may supplement our records with publicly available information or datasets to maintain accuracy, prevent fraud, or improve the Services.

3.5 Inferences we create

- **Service inferences.** We may generate **inferences** from your activity and test participation (for example, grouping scores or creating segments used to generate your **report** or to improve the Services). We do **not** use such inferences to make decisions that produce legal or similarly significant effects.

3.6 Sensitive Personal Information (SPI)

- **What we consider SPI here.** We may process **account log-in and password**, which is treated as **Sensitive Personal Information** under certain laws.
- **Purpose & limits.** We use SPI **only** for permitted purposes such as **authentication, security, and fraud prevention**. We **do not** use SPI to infer characteristics about you.
- **What we do not collect.** We do **not** collect government-issued ID numbers, precise geolocation, or special-category data (e.g., health/biometric data) through the Services.
- We **do not offer a "Limit the Use of My Sensitive Personal Information"** option because we use SPI **only** for permitted purposes (authentication/security/fraud) and **do not** use it to infer characteristics.

3.7 Combined data; links to other sections

We may combine information described above (for example, device data with account data) where necessary to operate, secure, and improve the Services. Any Non-personal Information that is linked to Personal Data will be treated as **Personal Data** for as long as the link exists. Additional details about how we use, share, retain, and transfer data appear in **Sections 5–9**, and California-specific disclosures (including category mapping for the last 12 months) appear in **Section 12 (California Privacy Notice)**.

4) Sources of Personal Data

We obtain Personal Data from the following sources:

4.1 Directly from you.
Information you provide when you use the Services (e.g., take a test, request results, create/manage an account), contact us (forms, email), set marketing preferences, or engage with customer support.

4.2 Automatically from your device/browser.
Technical and usage data collected via your access to the Site (e.g., IP address, device and browser details, language, pages viewed, clicks, timestamps) and **cookies/SDKs** used for core functionality, security/fraud prevention, analytics, and (where applicable) advertising. See **Section 6 (Cookies, Analytics & Advertising)** and **Cookie Settings**.

4.3 Payment providers.
If you make a purchase, we receive limited payment metadata from our payment providers (**Stripe, SolidGate, PayPal**). We do **not** receive or store full card numbers. Note that some providers (e.g., **PayPal**) may act as **independent controllers**; their processing is governed by their own privacy policies.

4.4 Service providers (processors).
Vendors that help us operate and secure the Services—such as **hosting/CDN, analytics, anti-fraud, security monitoring, customer-support tools,** and email delivery—may provide us with aggregated metrics, error diagnostics, fraud signals, or interaction data collected on our behalf under contract.

4.5 Support and communications channels.
We collect information contained in messages you send us (including attached order IDs/Test IDs) and may receive related metadata from our helpdesk and email systems for quality assurance and troubleshooting.

4.6 Public / commercially available sources.
Where permitted by law, we may supplement our records with limited information from public records or commercial datasets (for example, IP-to-region lookup) to maintain accuracy, prevent fraud, or improve the Services.

4.7 Single sign-on / third-party sign-in (if used).
If you access the Services through a third-party sign-in or SSO, we receive the account details that provider shares with us (e.g., email, name) in accordance with your settings and the provider's privacy policy.

4.8 Combined data.
We may combine information from the sources above (for example, device data with account data) where necessary to operate, secure, and improve the Services. Non-personal data linked to Personal Data is treated as **Personal Data** for as long as the link exists.

5) What are the purposes of the collection and processing of information?

We use Personal Data to operate, secure, and improve the Services. For each purpose below, we identify the primary **GDPR legal basis** (and, where relevant, secondary bases that may also apply depending on the context).

5.1 Provide the Services (tests/results), operate your account, and fulfill purchases/subscriptions
Examples: administer tests; generate and deliver Personality results/reports; provide IQBooster access; maintain your profile and settings; process orders and renewals; send service/transactional messages (e.g., receipts, trial-to-paid confirmations).
Legal basis: Contract (Art. 6(1)(b)); **Legitimate interests** (Art. 6(1)(f)) for ancillary operations (e.g., general service continuity where no contract exists yet).

5.2 Customer support and communications
Examples: respond to inquiries, troubleshoot, handle complaints and refunds where eligible, communicate important service updates or changes to terms/privacy.
Legal basis: Contract (Art. 6(1)(b)) where tied to your use/purchase; **Legitimate interests** (Art. 6(1)(f)) for general support and quality assurance.

5.3 Security, fraud prevention, and abuse detection

Examples: authenticate logins; protect accounts; detect/prevent fraud, spam, or misuse; monitor and enforce our Terms; protect the Service and our users.

Legal basis: Legitimate interests (Art. 6(1)(f)) to keep the Service safe; **Legal obligation** (Art. 6(1)(c)) where specific laws require security/fraud controls.

5.4 Service analytics, performance, and improvement

Examples: measure usage; diagnose errors; improve content, question banks, and UX; develop new features; aggregate statistics; run A/B tests using non-essential cookies/SDKs only with consent where required.

Legal basis: Legitimate interests (Art. 6(1)(f)) for essential measurement and service quality; **Consent** (Art. 6(1)(a)) for **non-essential** analytics cookies/SDKs where required by law.

5.5 Personalization and inferences created by us

Examples: create **inferences** from your test participation (e.g., score-based segments) to generate your report and tailor on-service experience. We do **not** use such inferences to make decisions with legal or similarly significant effects.

Legal basis: Contract (Art. 6(1)(b)) to produce purchased outputs (e.g., your report); **Legitimate interests** (Art. 6(1)(f)) to personalize non-essential aspects of the Service.

5.6 Marketing (where permitted) and outreach

Examples: send email about similar products you've purchased; optional newsletters/promotions; measure campaign performance; (where applicable) show ads for our own Services. Non-essential cookies/SDKs for ads/retargeting are used only with consent where required.

Legal basis: Legitimate interests (Art. 6(1)(f)) for B2C email about similar products/services (subject to opt-out at any time); **Consent** (Art. 6(1)(a)) for electronic marketing where required by law and for **non-essential** advertising cookies/SDKs.

5.7 Payments, accounting, tax, and compliance

Examples: process/refund payments via providers (e.g., Stripe, SolidGate, PayPal); keep transaction records; handle consumer-rights requests; comply with bookkeeping, tax, and regulatory duties.

Legal basis: Contract (Art. 6(1)(b)) to process your purchase; **Legal obligation** (Art. 6(1)(c)) for tax/records and responding to statutory requests; **Legitimate interests** (Art. 6(1)(f)) for audit and compliance readiness.

5.8 Protect our rights, safety, and legal interests

Examples: assert or defend legal claims; respond to lawful requests; prevent harm; address security incidents; enforce our Terms.

Legal basis: Legitimate interests (Art. 6(1)(f)); **Legal obligation** (Art. 6(1)(c)) where applicable.

5.9 Consent where required; withdrawing consent

Where we rely on **Consent** (e.g., non-essential cookies/SDKs, certain marketing), you may **withdraw consent at any time** via **Cookie Settings** or the **unsubscribe** link in our emails (or by contacting us). Withdrawal does not affect prior lawful processing.

5.10 Sensitive Personal Information (SPI) — limited use

We may process **account log-in and password** (considered SPI in some jurisdictions) **only** for permitted purposes such as **authentication, security, and fraud prevention**. We do **not** use SPI to infer characteristics about you.

5.11 Objection and choices

Where we rely on **Legitimate interests**, you have the **right to object** to processing on grounds relating to your situation; we will honor your request unless we have compelling legitimate grounds or the processing is

necessary for legal claims. You can also manage **non-essential** cookies/SDKs in **Cookie Settings** and opt out of marketing at any time via the unsubscribe link or by contacting us.

6) Cookies, Analytics & Advertising

6.1 What these technologies are.
We and our service providers use cookies and similar technologies (e.g., pixels, tags, SDKs, local storage) ("**Cookies**") to run the Site, keep it secure, measure performance, and—where permitted—support analytics and advertising.

6.2 Types of Cookies we use.

- **Essential (strictly necessary).** Required for the Site to function and to provide features you request (e.g., login, load balancing, security/fraud prevention). These cannot be switched off in our systems.
- **Analytics/Performance.** Help us understand how the Site is used (e.g., page views, session length, error diagnostics) so we can improve the Service.
- **Functional.** Remember choices (e.g., language, region) and enhance features.
- **Advertising/Marketing.** Enable us (or our partners) to measure campaigns and, where applicable, show ads for our Services that may be more relevant to you.

6.3 Your choices.

- **Cookie Settings.** You can manage non-essential Cookies at any time via **Cookie Settings** (link in the header/footer or banner).
- **Browser controls.** Most browsers let you block/delete Cookies. If you block essential Cookies, some features may not work.
- **Analytics opt-outs.** Some providers offer their own browser add-ons or settings to limit measurement (see provider resources, if applicable).
- **Mobile settings.** Your device OS may offer advertising preference settings that limit ad tracking.

6.4 Analytics & service measurement.
We use analytics and diagnostics tools to generate aggregated statistics, improve performance, and fix issues (for example, page load times, feature usage, crash/error reports). These vendors act **as our processors** under contract and are not permitted to use the data for their own purposes.

6.5 Advertising & cross-context behavioral advertising.
Where permitted, we may work with advertising or measurement partners to (i) measure the effectiveness of our campaigns and (ii) show ads for our own Services that are more relevant to your interests **based on activity over time and across non-affiliated sites/apps** (also called **cross-context behavioral advertising** or **targeted advertising**). You can control non-essential advertising Cookies in **Cookie Settings**.
*California residents: see **Section 12 (California Privacy Notice)** for additional choices, including the **Do Not Sell or Share My Personal Information** link and opt-out preference signal handling.*

6.6 Partners and disclosures.
We work with categories of partners such as: **hosting/CDN, security/anti-fraud, tag management, analytics/measurement, error monitoring, A/B testing, customer-support tools, and advertising/marketing platforms**. Some partners act as our **service providers/processors**; others (for example, certain payment platforms) may act as **independent controllers**—see their privacy notices. If we publish a vendor list, it will be linked from **Cookie Settings** or our Site.

6.7 Retention.
Cookie lifespans vary. Session Cookies expire when you close your browser; persistent Cookies last longer (e.g., months) unless you delete them earlier or adjust preferences in **Cookie Settings**. Specific durations appear in your browser or in our cookie preference tool.

7) Sharing Personal Information with Third Parties

We do **not** sell your Personal Data. We share Personal Data only as described below and as necessary to operate, secure, and improve the Services.

7.1 Our personnel and affiliates (need-to-know).
Personal Data may be accessed by Company personnel and affiliated entities on a **need-to-know** basis to operate the Services, provide support, and perform the activities described in this Policy. All personnel are subject to confidentiality obligations.

7.2 Service providers / processors (under contract).
We share Personal Data with vendors that process data **on our behalf** and under written agreements that limit their use of Personal Data to our instructions and applicable law. Typical categories include:

- **Hosting / CDN & infrastructure** (site hosting, content delivery, storage, backup)
- **Security & anti-fraud** (threat detection, abuse prevention, authentication aids)
- **Analytics / measurement & diagnostics** (usage metrics, error/crash reporting)
- **Customer support & communications** (helpdesk, email/SMS delivery)
- **Payments & billing logistics** (tokenized payment references, invoicing metadata)

7.3 Independent controllers / third parties.
Some partners act as **independent controllers** and process Personal Data for their own purposes under their privacy notices. Examples include certain **payment platforms (e.g., PayPal)** and, where applicable, advertising/measurement platforms. When you choose such services, their terms and privacy policies govern their use of your data.

7.4 Legal, compliance, and protection.
We may disclose Personal Data when we believe in good faith that it is necessary to: (i) comply with applicable law, regulation, legal process, or government request; (ii) enforce our Terms, protect our operations or rights, or defend against legal claims; (iii) detect, prevent, or address fraud, security, or technical issues; or (iv) protect the rights, property, or safety of the Company, our users, or the public.

7.5 Corporate transactions.
We may share or transfer Personal Data in connection with an actual or contemplated **merger, acquisition, financing, reorganization, sale of assets, or insolvency/bankruptcy** event. Where legally required, we will notify you and take appropriate steps to ensure the recipient honors this Policy or provides equivalent protection.

7.6 Aggregated or de-identified information.
We may share **aggregated** statistics or **de-identified** information that **does not identify** you, for research, analytics, or service improvement. We maintain and use such information in a manner designed to **not re-identify** individuals.

7.7 International transfers.
Some recipients may be located outside your jurisdiction (for example, service providers in the U.S.). See **Section 8 (International Data Transfers)** for how we safeguard cross-border transfers.

7.8 Advertising & cross-context behavioral advertising.
Where we work with advertising or measurement partners, we describe those activities and your choices in **Section 6 (Cookies, Analytics & Advertising)**. **California residents** should also review **Section 12 (California**

Privacy Notice) for “Do Not Sell or Share” options and opt-out preference signal handling.

8) International Data Transfers

8.1 Where your data is processed.
We are established in the **European Union (Cyprus)**. The Services are **primarily hosted in the EU**. Some Service Providers and independent partners (for example, certain payment, analytics, support, or security vendors) may process Personal Data **outside** your country, including in countries that **may not provide the same level of data protection** as your home jurisdiction (e.g., the **United States**).

8.2 Safeguards for cross-border transfers (GDPR/EEA).
When we transfer Personal Data from the EEA to a country without an adequacy decision, we implement appropriate safeguards, such as:

- **EU Standard Contractual Clauses (SCCs)** with recipients, including onward-transfer requirements; and
- **Supplementary measures** where needed (e.g., encryption in transit and at rest, strict access controls, data minimization, and vendor due-diligence).

Where applicable, we may also rely on an **EU adequacy decision** (for example, participation in the **EU–U.S. Data Privacy Framework** by a recipient) for specific transfers.

8.3 UK transfers (if applicable).
If we later target UK residents and transfer Personal Data from the UK to third countries, we will use the **UK IDTA** or the **UK Addendum** to the EU SCCs (and supplementary measures where needed), or rely on a **UK adequacy regulation**, as applicable.

8.4 Other lawful bases for specific transfers.
In limited scenarios, we may rely on **derogations** permitted by law (e.g., performance of a contract at your request, establishment/exercise/defense of legal claims, or your **explicit consent**).

8.5 How to obtain information about our transfer safeguards.
You may **contact us** (see Section 15) to request more details about the safeguards we use for cross-border transfers or to obtain a copy of the relevant SCCs (redacted to protect confidential terms).

8.6 Vendor oversight.
We conduct **risk assessments** of key vendors that handle Personal Data and periodically review their technical and organizational measures to help ensure an appropriate level of protection.

9) Retention

We keep Personal Data **only for as long as necessary** to fulfill the purposes described in this Policy (see Section 5), including to meet legal, accounting, or reporting requirements, resolve disputes, and enforce our agreements. When data is no longer needed, we **delete or de-identify** it, unless a longer retention period is required or permitted by Applicable Law.

9.1 Category-based periods/criteria

- **Account & profile data (name, email, preferences).** Kept **while your account is active**, then typically **up to 24 months** after last activity for support, fraud prevention, and recordkeeping, unless you request deletion earlier (subject to legal holds).
- **Test participation & results (answers, timestamps, score, certificates/reports).** Retained **while necessary to provide your purchased outputs** and to support your legitimate requests (e.g., re-delivery), then typically **12–24 months** after last activity, unless law requires a different period.

- **Subscription & billing records (plan, billing history, invoices/receipts).** Core transaction records are retained **for the period required by tax and accounting laws** (generally **7 years** in many jurisdictions).
- **Payment tokens/metadata (no full card numbers).** Retained **as long as needed** for charge handling, fraud prevention, and reconciliations, typically **up to the transaction recordkeeping period**.
- **Customer support communications (emails, tickets, attachments).** Retained **while your request is open** and then typically **12–24 months** for quality assurance, training, and to defend/establish legal claims.
- **Security/fraud logs (access, auth, abuse indicators).** Retained **for security lifecycle needs**, typically **6–24 months**, or longer if required to investigate incidents or comply with law.
- **Analytics/diagnostics data (aggregated usage metrics, error logs).** Retained in identifiable form **only as needed for troubleshooting and improvement**, then **aggregated or de-identified** for longer-term trend analysis.
- **Legal/compliance records (consents, privacy requests).** Retained **as required by law** (e.g., to demonstrate compliance with consent and rights-request obligations).

9.2 Cookies & similar technologies

Cookie/SDK lifespans vary by type and purpose. **Session cookies** expire when you close your browser; **persistent cookies** remain for a set period unless you delete them. See **Section 6 (Cookies, Analytics & Advertising)** and the **Cookie Settings** tool (and, where available, the cookie list within that tool) for details and choices.

9.3 De-identification & aggregation

Where appropriate, we **de-identify** or **aggregate** data so it can no longer reasonably identify you. We maintain such data in that form and **do not attempt to re-identify** it. Aggregated/de-identified data may be retained and used for legitimate business purposes (e.g., service improvement, statistics).

9.4 Criteria we use

When determining retention, we consider: (i) the **volume, nature, and sensitivity** of the data; (ii) the **purposes** of processing and whether they can be achieved by other means; (iii) **legal/regulatory** requirements; (iv) **risk** of harm from unauthorized use or disclosure; and (v) our **contractual** obligations and ability to support user requests.

9.5 Deletion upon request

Subject to Applicable Law and documented exemptions (e.g., tax/legal obligations, security, or dispute resolution), we honor **deletion requests**—see **Your Rights** (Sections 11 and 12) for how to submit a request.

10) Security

We implement **reasonable technical and organizational measures** designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. These measures are calibrated to the nature of the data and our processing activities and are reviewed periodically.

What this generally includes (illustrative):

- **Access controls & least-privilege:** role-based access, need-to-know, authentication safeguards.
- **Encryption & transmission security:** encryption in transit and at rest where appropriate; secure transport protocols.
- **Network & application protections:** segmentation, logging/monitoring, vulnerability management, and change controls.
- **Vendor oversight:** contractual security requirements for service providers and periodic risk reviews.
- **Resilience & recovery:** backups and business continuity/incident response procedures designed to reduce downtime and data loss.

No absolute guarantee.

No method of transmission or storage is 100% secure. While we work to protect your information, we **cannot guarantee** absolute security.

Incident response & notifications.
If we become aware of a breach of security that affects Personal Data, we will **investigate** and **notify affected individuals and/or regulators as required by applicable law** and in accordance with our incident response procedures.

Your role.
You are responsible for maintaining the confidentiality of your account credentials and for promptly notifying us of any suspected unauthorized access to your account (see **Section 4** and **Your Privacy Choices** for contact options).

11) Your Rights

You may have rights over your Personal Data under Applicable Law. You can make a request through **Your Privacy Choices** (link in the header/footer) or by emailing **info@16persons.com**. We may ask you to **verify your identity** before acting on a request. Certain rights are subject to **limitations or exemptions** (e.g., where fulfilling a request would infringe the rights of others or conflict with legal obligations).

11.1 EU/EEA

If you are in the **EU/EEA** (and, if we later target the UK, the **UK**), you have the following rights under the GDPR (and UK GDPR where applicable):

- **Access** — obtain confirmation whether we process your Personal Data and receive a copy.
- **Rectification** — correct inaccurate or incomplete Personal Data.
- **Erasure** — request deletion in certain circumstances (e.g., no longer needed; you withdraw consent and there is no other legal basis; unlawful processing).
- **Restriction** — request we limit processing in certain cases (e.g., while accuracy is contested).
- **Portability** — receive Personal Data you provided to us in a structured, commonly used, machine-readable format and (where technically feasible) have it transmitted to another controller where processing is based on **consent** or **contract** and carried out by automated means.
- **Object** — object to processing based on **legitimate interests**, including profiling on that basis; we will stop unless we demonstrate compelling legitimate grounds or need the data for legal claims. You may also object at any time to processing for **direct marketing**.
- **Withdraw consent** — where we rely on **consent** (e.g., non-essential cookies/SDKs or certain marketing), you can withdraw at any time (see **Cookie Settings** or the **unsubscribe** link in our emails); this does not affect prior lawful processing.

Response time. We respond **within one (1) month** of receiving your verified request. Where necessary due to complexity or number of requests, we may extend by up to **two (2) further months** and will notify you of the extension and reasons.

Complaints. You have the right to lodge a complaint with a **supervisory authority**. Our lead authority is the **Office of the Commissioner for Personal Data Protection (CPDP), Cyprus**. You may also contact your **local** supervisory authority.

11.2 Global

Depending on where you live, you may have **local privacy rights** under Applicable Law. You are responsible for maintaining the confidentiality of your account credentials and for promptly notifying us of any suspected unauthorized access to your account at **info@16persons.com.** We will handle your request in accordance with the laws of your jurisdiction and this Policy.

Note: California-specific rights and choices (including “Do Not Sell or Share”) are set out in **Section 12 (California Privacy Notice)**.

12) California Privacy Notice (CPRA)

This section applies **only to California residents** and supplements the rest of this Policy. Terms such as **“sell,” “share,” “service provider,”** and **“sensitive personal information (SPI)”** have the meanings given in the CCPA/CPRA. You may have rights over your Personal Data under Applicable Law. You can make a request by emailing **info@16persons.com** (from the address associated with your account, if applicable). We may ask you to verify your identity (and, where permitted, a request from an **authorized agent**) before acting on a request. Certain rights are subject to limitations or exemptions (e.g., where fulfilling a request would infringe the rights of others or conflict with legal obligations).

12.1 Notice at Collection (past 12 months and going forward)

Categories we collect. In the last 12 months (and going forward), we **collected** the following categories of Personal Information from the sources and for the purposes described below:

- **Identifiers** (e.g., name, email, IP address, account ID, cookie/advertising IDs).
- **Customer / billing records** (e.g., purchases, subscription status; tokenized payment references and, where applicable, last 4 digits—**no** full card numbers stored by us).
- **Commercial information** (e.g., products purchased, trial/renewal information).
- **Internet / network activity** (e.g., device/browser details, pages viewed, clicks, timestamps).
- **Approximate geolocation** (derived from IP address).
- **Inferences** we create (e.g., score-based groupings used to generate your report or personalize on-service experience).
- **Sensitive Personal Information (SPI)** limited to **account log-in credentials** (email/username + password).

Categories we do *not* collect. We do **not** collect: protected class characteristics; biometric data; sensory data; professional/employment data; education data; precise geolocation; government IDs; or health/biometric/similar special categories via the Services.

Sources. From **you** (when you use the Services or contact support); **automatically** from your device/browser via cookies/SDKs; from **service providers** (e.g., analytics, anti-fraud, payment processors); and from limited **public/commercial** sources (e.g., IP-to-region lookup).

Purposes. To **provide the Services** (tests/results, IQBooster), operate accounts, **process purchases/renewals**, provide **support**, maintain **security/fraud prevention**, perform **analytics and service improvement**, send **marketing** where permitted, and meet **legal/compliance** obligations. See Section 5 for details and GDPR legal bases.

Recipients. We disclose Personal Information to:

- **Service providers** processing data on our behalf (hosting/CDN, security/anti-fraud, analytics/measurement, diagnostics, support tooling, email delivery, billing logistics).
- **Independent controllers** where you choose their services (e.g., **PayPal**).
- **Authorities**/others as required by law, and in **corporate transactions** (see Section 7).

Retention. We retain Personal Information for the periods/criteria described in **Section 9 (Retention)** (e.g., account data while active + a limited period, transaction records generally 7 years, security logs for security lifecycle needs, cookies per their lifespans).

Sale/Share.

- We **do not “sell”** Personal Information for money.

- We **may "share"** Personal Information for **cross-context behavioral advertising** (targeted advertising) as defined by California law—primarily **online identifiers** (e.g., cookie/advertising IDs) and **internet/network activity** collected via cookies/SDKs, and in limited cases **inferences** used to tailor on-service experience or measure campaigns. You can **opt out** as described below.

How to opt out of "sale/share." Use **Do Not Sell or Share My Personal Information** and adjust **Cookie Settings** (links are in the header/footer). Opt-outs are browser/device-specific unless set while logged in (if available).

12.2 Sensitive Personal Information (SPI)

We process **SPI** only as **account log-in credentials** (email/username + password) for **authentication, security, and fraud prevention**. We **do not** use SPI to infer characteristics about you. Because we do not use SPI for additional purposes, we **do not offer a "Limit the Use of My Sensitive Personal Information"** link at this time.

12.3 Your California Rights & How to Exercise Them

Your rights. Subject to exceptions, California residents have the right to: **(1) Know/Access** (including specific pieces), **(2) Delete**, **(3) Correct** inaccurate Personal Information, **(4) Portability**, and **(5) Opt-out of Sale or Sharing** (including cross-context behavioral advertising). We **will not discriminate** against you for exercising any rights under California law (e.g., no denial of services, different prices, or quality).

How to submit requests. Use **Your Privacy Choices** (link in header/footer) or email **info@16persons.com**.

- We will **acknowledge within 10 days** and **respond within 45 days** of verifying your request (we may take one **additional 45-day** extension where permitted).
- We will **verify your identity** (and, where applicable, your **authorized agent's** authority). Agents must provide written permission from you or power of attorney; we may require you to verify directly with us.

Opt-out of Sale/Sharing. Submit a request via **Do Not Sell or Share My Personal Information** and manage **Cookie Settings**. Opt-out limits the use/disclosure of Personal Information for cross-context behavioral advertising.

Opt-out Preference Signals (GPC). We **honor** recognized **opt-out preference signals** (such as **Global Privacy Control**) as a valid request to **opt out of sale/sharing** for that **browser/session**. To extend your preference across devices, use our **Do Not Sell/Share** link while logged in (if available).

Minors (under 18). We **do not provide the Services to, or knowingly collect Personal Information from, individuals under 18**. We also **do not knowingly sell or share** the Personal Information of consumers under 18. If we learn that we collected or disclosed such information, we will **cease** and **delete** it. If you believe we have information about a minor, please contact us via **Your Privacy Choices** or **info@16persons.com**.

13) Children & Teens

18+ only. The Services are intended **only for individuals 18 years of age or older** (see our Terms). Please do not use the Services if you are under 18.

No knowing collection from children under 13. We do **not knowingly collect** Personal Data from children **under 13**. If you are a parent or guardian and believe your child has provided Personal Data to us, please contact us promptly via **Your Privacy Choices** or at **info@16persons.com**.

What we do if we learn about underage data. If we become aware that we have collected Personal Data from someone **under 18** (including under 13), we will:

- **Delete** the Personal Data without undue delay;
- **Terminate** any related access to the Services; and
- Take reasonable steps to **prevent further collection**.

We may request information from a parent/guardian solely to **verify** the request and to complete deletion.

14) How to Contact Us

For any questions or requests about this Privacy Policy or your Personal Data, you can reach us at:

Email

- **info@16persons.com**

Mailing Address
Maxiq Limited
Markou Drakou 2A
Livadia 7060, Larnaca
Cyprus

15) Changes to This Policy

We may update this Privacy Policy from time to time. The **“Last Updated”** date at the top of this page reflects the most recent changes.

How we’ll notify you.

- For **material changes**, we will make reasonable efforts to provide notice (for example, by posting a clear notice on the Site and/or emailing the address associated with your account, if available).
- Other updates will be effective upon posting the revised Policy with the new **Last Updated** date.

When changes take effect.

- **Material changes** take effect **seven (7) days** after we provide notice, unless a longer period is stated in the notice or required by law.
- Changes made to address **legal, regulatory, security, or operational** requirements may take effect **immediately** as permitted by law.

Your choices.
If you do not agree to the updated Policy, you should **stop using the Services** and adjust your preferences (e.g., **Cookie Settings**) and, if applicable, cancel any subscription as described in our Terms. Your continued use of the Services on or after the effective date **constitutes acceptance** of the updated Policy.

No retroactive effect on disputes.
Updates to this Privacy Policy **do not apply retroactively** to disputes between you and us that arose **before** the effective date of the updated Policy.

Last Revised: 21.10.2025

* Our content is offered in multiple languages through a combination of human and AI-assisted translation. While we make every effort to ensure accuracy, the English version is the official and legally binding text.