



INDEERO PRIVACY POLICY

A subsidiary of Celora Holdings

Effective Date: 09th June 2026

Last Updated: 19th July 2026

This Privacy Policy explains how **Celora Holdings** ("**Celora Holdings**", "**we**", "**us**", or "**our**") collects, uses, stores, shares, protects and otherwise processes personal data through the **Indeero** platform ("the Platform"), including but not limited to Personal Listings, Community Listings, Workspaces, recruitment services, subscriptions, Listing Boosts and all associated products and services.

Indeero is a subsidiary platform operated under the governance and control of Celora Holdings. All personal data processed through the Platform is managed in accordance with the **United Kingdom General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, the **Privacy and Electronic Communications Regulations (PECR)** and guidance published by the **Information Commissioner's Office (ICO)**.

This Privacy Policy should be read alongside our Terms of Service, Cookie Policy and any additional policies published by Celora Holdings.

Data Controller

For the purposes of the United Kingdom General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018, **Celora Holdings** is the sole Data Controller responsible for determining the purposes and means of processing all personal data collected through the Indeero Platform.

Indeero operates solely as a platform and service owned by Celora Holdings. All customer data, account information, recruitment data, subscription information and associated records remain under the exclusive control and governance of Celora Holdings.

Celora Holdings is registered as a Data Controller with the Information Commissioner's Office (ICO).

ICO Registration Reference: ZC175994

Registered Address: Unit 168670, PO Box 7169, Poole, Dorset, BH15 9EL

Data Protection Officer: dpo@celoraholdings.co.uk

Access to Customer Data

In accordance with **Article 5(1)(f)** UK GDPR (Integrity and Confidentiality), **Article 24** UK GDPR (Responsibility of the Controller), **Article 25** UK GDPR (Data Protection by Design and by Default) and **Article 32** UK GDPR (Security of Processing), access to customer data is strictly restricted.

Personal information may only be accessed by individuals within Celora Holdings who:

- require access for authorised business purposes;
- have successfully completed approved Data Protection and UK GDPR training;
- hold a valid and in-date Data Protection and UK GDPR certification recognised by Celora Holdings;
- are subject to confidentiality obligations;
- operate under role-based access permissions;
- are monitored through internal audit and security logging.

Access permissions are reviewed regularly and may be revoked immediately where no longer required.

No employee, contractor or representative may access customer information without appropriate authorisation.

Data Protection Compliance

Celora Holdings processes all personal data in accordance with:

- United Kingdom General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)
- Information Commissioner's Office guidance

Processing activities are conducted in accordance with the principles contained within **Article 5 UK GDPR**, namely:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

In accordance with **Article 5(2)** UK GDPR, Celora Holdings is responsible for demonstrating compliance with these principles through documented governance, policies, staff training and security procedures.

Information We Collect

Account Information

When you create an Indeero account or purchase services through the Platform we may collect:

- Full name
- Email address
- Username
- Encrypted password
- Discord username
- Roblox username
- Account preferences
- Subscription status
- Account verification information
- Login history
- Information relating to purchased account plans
- Information relating to Listing Boost purchases
- Billing preferences
- Transaction references
- Purchase history
- Customer support interactions

Celora Holdings does not store complete payment card numbers or card verification values (CVV).

Profile Information

Where voluntarily supplied, we may collect:

- Personal Listings
- Community Listings
- Skills
- Experience
- Employment history
- Portfolio information
- Uploaded documents
- Images
- Videos
- Social media links
- Website links
- Biography information

Users remain responsible for the information they choose to publish publicly through the Platform.

Recruitment and Workspace Information

Where recruitment functionality is used we may process:

- Job vacancies
- Workspace information
- Applications
- CVs and résumés
- Cover letters
- Supporting documents
- Recruitment communications
- Internal Workspace messaging
- Interview scheduling
- Recruitment activity logs
- Audit history
- Moderation history

Technical Information

To maintain the integrity and security of the Platform we automatically collect technical information including:

- IP addresses
- Browser information
- Device information
- Operating system
- Login timestamps
- Security events
- Authentication records
- Platform activity logs
- Indexer monitoring logs
- Fraud prevention records
- Error reports
- Performance diagnostics
- Session identifiers
- Cookie identifiers

This information assists us in complying with Article 32 UK GDPR regarding the ongoing confidentiality, integrity, availability and resilience of processing systems.

Billing and Payment Information

Where purchases are made through the Platform, Celora Holdings may collect:

- Billing name
- Billing address
- Billing postcode
- Billing country
- Contact email address
- Contact telephone number where provided
- Last four digits of the payment card
- Card issuer
- Payment method
- Purchase history
- Transaction identifiers
- Subscription history
- Listing Boost purchase history
- Refund history
- VAT information where applicable

Full payment card numbers, security codes (CVV/CVC) and complete payment credentials are **never** stored by Celora Holdings.

Payments are securely processed by authorised PCI DSS compliant third-party payment service providers.

How We Use Your Information

Celora Holdings processes personal information only where there is a lawful basis under **Article 6 UK GDPR**.

Personal information may be used to:

- Provide Platform services
- Create and maintain user accounts
- Operate Personal Listings
- Operate Community Listings
- Operate Workspaces
- Process subscriptions
- Process Listing Boost purchases
- Authenticate users
- Verify accounts
- Prevent fraud
- Detect abuse
- Investigate security incidents
- Respond to support requests
- Improve platform functionality
- Monitor service performance
- Protect Platform integrity
- Maintain audit records
- Comply with legal obligations
- Respond to lawful requests from public authorities
- Exercise or defend legal claims
- Fulfil contractual obligations

We will only process personal information for purposes that are compatible with those for which it was originally collected unless otherwise required by law.

Legal Basis for Processing

In accordance with **Article 6 UK GDPR**, Celora Holdings relies upon the following lawful bases.

Article 6(1)(a) — Consent

Where consent is required, including certain marketing communications.

Consent may be withdrawn at any time.

Article 6(1)(b) — Contract

Processing necessary for providing the services requested by the user.

Article 6(1)(c) — Legal Obligation

Processing necessary for compliance with legal obligations.

Article 6(1)(f) — Legitimate Interests

Including:

- Cybersecurity
- Fraud prevention
- Service improvement
- Customer support
- Corporate governance
- Platform administration
- Internal auditing
- Risk management
- Business continuity
- Legal compliance

Where legitimate interests are relied upon, appropriate balancing assessments are undertaken to ensure users' rights and freedoms are protected.

Where special category personal data is processed, Celora Holdings will satisfy the additional requirements of **Article 9 UK GDPR** and Schedule 1 of the Data Protection Act 2018 where applicable.

Data Sharing

Celora Holdings is committed to protecting the confidentiality of personal data and does **not** sell, rent, trade or otherwise commercially disclose personal information to third parties.

Personal data is only disclosed where there is a lawful basis under **Article 6 UK GDPR**, where disclosure is necessary to provide the Platform, or where disclosure is required by law.

Personal information may be shared with:

- Authorised Workspace Owners for recruitment purposes.
- Workspace Administrators and authorised Workspace Members where necessary to facilitate recruitment and collaboration.
- Payment service providers responsible for securely processing subscriptions and Listing Boost purchases.
- Hosting and cloud infrastructure providers.
- Email and communications providers.
- Security monitoring and fraud prevention providers.
- Professional advisers, including legal advisers, auditors and insurers.
- Regulatory authorities, law enforcement agencies or courts where required by law.

All third-party providers acting on behalf of Celora Holdings are required to process personal data in accordance with written contractual obligations that comply with **Article 28 UK GDPR** where they act as Data Processors.

Where processors are appointed, Celora Holdings remains responsible for ensuring appropriate technical and organisational measures are maintained.

Workspace Data Responsibility

The Indeero Platform enables organisations to create Workspaces for recruitment and collaboration.

Where a user submits an application through a Workspace, the information provided may become accessible to:

- Workspace Owners
- Workspace Administrators
- Authorised Workspace Members

Once personal data has been accessed by a Workspace for recruitment purposes, that Workspace Owner may become an independent Data Controller in respect of their own processing activities under UK GDPR.

Celora Holdings cannot control how independent Workspace Controllers subsequently process personal data outside of the Indeero Platform.

Users should review the privacy information provided by the relevant Workspace where available before submitting personal information.

Reporting Misuse of Personal Data

If a user reasonably believes that a Workspace has:

- unlawfully disclosed personal information;
- sold personal information;
- distributed personal information without authority;
- processed personal information contrary to UK GDPR; or
- otherwise misused personal information obtained through the Platform,

The matter should be reported immediately.

Reports should be submitted to: legal@celoraholdings.co.uk

Reports should include supporting evidence where reasonably available.

Following investigation, Celora Holdings may take action including:

- temporary Workspace suspension;
- permanent Workspace removal;
- suspension of associated user accounts;
- permanent termination of accounts;
- referral to the Information Commissioner's Office;
- referral to law enforcement authorities where criminal offences are suspected.

Information Security

Protecting customer information is fundamental to the operation of the Indeero Platform.

In accordance with **Articles 24, 25 and 32 UK GDPR**, Celora Holdings maintains appropriate technical and organisational measures designed to safeguard personal information against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access.

These measures include, but are not limited to:

- encryption of sensitive information;
- encryption of personal data during transmission;
- encrypted password storage;
- role-based access controls;
- least privilege access principles;
- multi-factor authentication for privileged systems where applicable;
- privileged access management;
- internal security auditing;
- continuous security monitoring;
- fraud detection systems;
- Indexer monitoring and logging;
- intrusion detection mechanisms;
- vulnerability management;
- routine software updates;
- security patch management;
- disaster recovery procedures;
- business continuity planning;
- secure backup procedures;
- access logging and audit trails;
- confidentiality agreements for authorised personnel;
- mandatory Data Protection and UK GDPR certification requirements for personnel with access to customer information.

Customer information is accessible only by authorised individuals within Celora Holdings whose duties require such access and who maintain a valid, in-date Data Protection and UK GDPR certification recognised by Celora Holdings.

While Celora Holdings employs industry-standard safeguards, no electronic storage system or method of transmission can be guaranteed to be completely secure.

Data Retention

In accordance with **Article 5(1)(e) UK GDPR**, personal data is retained only for as long as necessary for the purposes for which it was collected.

Retention periods may vary depending upon:

- contractual obligations;
- legal obligations;
- accounting requirements;
- fraud prevention;
- dispute resolution;
- safeguarding the security of the Platform;
- legitimate business requirements.

Where personal information is no longer required, it will be securely deleted, anonymised or otherwise disposed of using appropriate security procedures.

Where legislation requires longer retention periods, Celora Holdings will retain the information for the minimum period required by law.

Your Rights

Under **Articles 12–23 UK GDPR**, individuals have the following rights:

- Right of Access (Article 15)
- Right to Rectification (Article 16)
- Right to Erasure (Article 17)
- Right to Restriction of Processing (Article 18)
- Right to Data Portability (Article 20)
- Right to Object (Article 21)
- Rights relating to Automated Decision Making where applicable (Article 22)

Requests may be submitted to: dpo@celoraholdings.co.uk

Identity Verification

Under **Article 12(6) UK GDPR**, Celora Holdings may request additional information necessary to verify the identity of an individual before responding to a request.

This requirement exists to prevent unauthorised disclosure of personal information and to protect the rights of data subjects.

Failure to provide sufficient information to verify identity may result in delays or refusal of a request where permitted by law.

Personal Data Breaches

In accordance with **Articles 33 and 34 UK GDPR**, where a personal data breach occurs Celora Holdings will:

- identify and contain the incident;
- investigate the cause;
- assess the risks to affected individuals;
- implement remedial measures;
- notify the Information Commissioner's Office where legally required;
- notify affected individuals where there is a high risk to their rights and freedoms.

All suspected security incidents are investigated in accordance with internal incident response procedures.

Marketing Communications

By creating an Indeero account, users may receive service-related communications necessary for the operation of the Platform.

Where permitted by law, users may also receive marketing communications relating to Platform services.

Marketing preferences may be updated at any time through account settings or by contacting: legal@celoraholdings.co.uk

Service notifications relating to security, legal obligations or operation of the Platform may continue to be sent where necessary.

Cookies & Tracking Preferences

The Indeero Platform uses cookies and similar technologies for purposes including:

- user authentication;
- session management;
- security monitoring;
- fraud prevention;
- analytics;
- performance monitoring;
- remembering user preferences;
- improving user experience.

Certain cookies are essential to the operation of the Platform.

Users may manage cookie preferences through their browser settings; however, disabling certain cookies may affect Platform functionality.

This Privacy Policy should be read together with the Indeero Cookie Policy.

Third-Party Services

Celora Holdings may utilise carefully selected third-party service providers to support operation of the Platform, including:

- payment processing;
- cloud hosting;
- infrastructure services;
- content delivery;
- email delivery;
- monitoring services;
- analytics;
- cybersecurity services.

Where third parties process personal data on behalf of Celora Holdings, contractual safeguards meeting the requirements of **Article 28 UK GDPR** are maintained.

Further information regarding third-party processing may be requested by contacting: legal@celoraholdings.co.uk

International Data Transfers

Where personal data is transferred outside the United Kingdom, Celora Holdings ensures that appropriate safeguards are implemented in accordance with **Chapter V UK GDPR**.

Such safeguards may include:

- UK Adequacy Regulations;
- International Data Transfer Agreements (IDTAs);
- Standard Contractual Clauses where applicable;
- documented transfer risk assessments;
- additional technical and organisational safeguards where necessary.

Changes To This Privacy Policy

Celora Holdings reserves the right to amend this Privacy Policy at any time to reflect changes in legislation, regulatory guidance, operational requirements or Platform functionality.

Where significant changes are made, users will be notified through email or appropriate Platform notifications.

Continued use of the Indeero Platform following publication of an updated Privacy Policy constitutes acceptance of the revised Policy.

Contact Information

General Enquiries

hello@indeero.com

Support Centre

<https://support.celoraholdings.co.uk>

Billing Enquiries

billing@indeero.com

Enterprise Enquiries

enterprise@indeero.com

Legal Enquiries

legal@indeero.com

Data Protection Officer

dpo@celoraholdings.co.uk

Regulatory Information

Celora Holdings is the sole Data Controller for the Indeero Platform.

Celora Holdings is registered with the Information Commissioner's Office (ICO) as a Data Controller under registration reference **ZC175994**.

Customer information is processed under the governance of Celora Holdings and is accessible only to authorised personnel with an operational requirement to access such information. Individuals granted access must maintain valid and current Data Protection and UK GDPR certification and are subject to confidentiality obligations, internal policies, audit controls and ongoing compliance monitoring.

Celora Holdings maintains appropriate organisational and technical measures to demonstrate accountability in accordance with **Article 5(2) UK GDPR** and implements data protection by design and by default as required by **Article 25 UK GDPR**.

Summary

Celora Holdings is committed to protecting the privacy, security and integrity of personal information entrusted to it through the Indeero Platform.

Personal data is processed lawfully, fairly and transparently in accordance with:

- the United Kingdom General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018;
- the Privacy and Electronic Communications Regulations (PECR); and
- applicable guidance issued by the Information Commissioner's Office.

By accessing or using the Indeero Platform, users acknowledge that their personal information will be processed as described in this Privacy Policy.

Where users believe that their personal information has been processed unlawfully or in breach of applicable legislation, they are encouraged to contact the Data Protection Officer in the first instance. Individuals also have the right to lodge a complaint with the Information Commissioner's Office if they believe their data protection rights have been infringed.