

BULLS OUT, LLC PRIVACY POLICY

Last updated: April 2, 2026

Effective date: April 2, 2026

1. INTRODUCTION AND SCOPE

1.1 About Us

Bulls Out, LLC ("Bulls Out," "we," "our," or "us") is a wholly owned subsidiary of JBI Holdings LLC ("JBI"). Bulls Out operates a competitive, social finance game that rewards users for their financial knowledge, strategy, and market timing through league-based challenges and performance tracking. Our platform enables users to build watchlists, track market performance, compete in leagues, and climb leaderboards (the "Platform"). Bulls Out utilises technology infrastructure and services provided by Communify Group, LLC (doing business as Communify, "Communify"), an affiliate within the JBI group of companies.

Our principal place of business is at 1728 Olympic Blvd., Santa Monica, CA 90404, United States of America.

1.2 Scope of This Policy

This Privacy Policy describes how Bulls Out collects, holds, uses, discloses, and otherwise manages personal information in connection with the Platform and our services. Personal information collected by Bulls Out may be shared with our parent company JBI Holdings LLC and related entities within the JBI group (including Communify Group, LLC, Communify On Demand, Inc., and Communify LLC) as described in this Policy.

This Policy applies to all individuals who use the Platform or interact with our services, regardless of location. Additional rights and obligations may apply to you based on the jurisdiction in which you reside, as set out in the Regional Provisions (Section 16).

This Policy should be read in conjunction with our Terms and Conditions. In the event of any inconsistency between this Policy and the Terms and Conditions, this Policy will prevail to the extent of the inconsistency regarding privacy matters.

Capitalised terms used but not defined in the PP have the meanings given in the Terms and Conditions.

1.3 What Is Personal Information?

"Personal information" (also referred to as "personal data" in some jurisdictions) means information that identifies, relates to, or could reasonably be used to identify an individual. The precise definition applicable to you depends on the data protection law in your jurisdiction (see Section 16).

"Sensitive information" (also referred to as "special category data" in some jurisdictions) is a subset of personal information that includes information about an individual's racial or ethnic origin, political

opinions, religious beliefs, health information, biometric information, sexual orientation, or criminal record. The specific categories vary by jurisdiction.

2. PERSONAL INFORMATION WE COLLECT

2.1 Information You Provide

We collect the following kinds of personal information depending on how you interact with us:

Account and Registration Information: Name, email address, and phone number.

Transaction and Payment Information: Billing address, payment card details (processed and stored by our third-party payment processors), transaction history, subscription details, and purchase records.

Platform Usage Information: Watchlists, league selections, competition entries, leaderboard rankings, chat messages and communications with other users within your leagues, feedback and support requests, and user-generated content.

Employment and Recruitment Information: Curriculum vitae or resume, cover letter, employment history, educational qualifications, professional references, work eligibility documentation, and interview records.

Business Contact Information: Business name, business address, job title, professional email address, and professional phone number.

2.2 Information Collected Automatically

When you use our Platform, we may automatically collect:

Technical Information: IP address, browser type and version, device type, operating system, unique device identifiers, and mobile network information.

Usage Analytics: Aggregate and de-identified data about how users interact with our Platform, including page views, click patterns, feature usage, session duration, and navigation paths. We collect analytics data in aggregate form and do not use it to identify individual users.

Cookies and Similar Technologies: We use cookies, pixels, and similar tracking technologies to facilitate the operation of our Platform, remember your preferences, and collect usage analytics. You can manage cookie preferences through your browser settings. Additional cookie-specific requirements for your region are set out in Section 16.

2.3 Information from Third Parties

We may receive personal information from third parties, including:

- Market data and financial information providers who supply data displayed on our Platform
- Identity verification and fraud prevention service providers
- Payment processors

- Social media platforms (if you choose to link your account)
- Business partners who refer you to our services
- Publicly available sources

2.4 Sensitive Information

We do not generally collect sensitive information. If we need to collect sensitive information, we will do so only with your explicit consent or as otherwise permitted or required by applicable law.

3. HOW WE COLLECT PERSONAL INFORMATION

3.1 Collection Methods

We collect personal information through the following means:

- Directly from you when you create an account, complete a registration form, subscribe to a service, make a purchase, participate in a competition or league, communicate with other users within your leagues, submit a support request, apply for employment, or otherwise interact with our Platform or services
- Automatically through our Platform using cookies, analytics tools, and server logs
- From third parties as described in Section 2.3
- From publicly available sources

3.2 Collecting Directly from You

Where it is reasonable and practicable to do so, we will collect personal information directly from you. There may be occasions where we collect personal information about you from a third party (for example, from a referee you have nominated as part of a job application, or from a business partner who refers you to our services).

3.3 Necessity of Collection

We only collect personal information that is reasonably necessary for the purposes described in this Policy. If you choose not to provide certain personal information, we may not be able to provide you with the relevant Platform features or services.

3.4 Lawful and Fair Collection

We collect personal information only by lawful and fair means. We will not collect personal information in a way that is unreasonably intrusive.

3.5 How We Hold Personal Information

We hold personal information in a combination of:

- Electronic databases and systems hosted on secure servers located in Australia (using data centre infrastructure shared with our affiliate FinextraPro) and in the United States

- Cloud-based storage services provided by reputable third-party providers
- Physical records stored in secure facilities (limited)

4. PURPOSES FOR COLLECTION, USE, AND DISCLOSURE

4.1 Primary Purposes

We collect, hold, use, and disclose personal information for the following purposes:

- To provide, operate, maintain, and improve our Platform and services
- To create and manage your user account
- To enable you to participate in leagues, competitions, leaderboards, and other interactive features
- To display your first name and last name to other users for the purpose of social features, invitations, and in-league communication
- To process transactions and send related information, including purchase confirmations and invoices
- To send you technical notices, updates, security alerts, and administrative messages
- To respond to your enquiries, comments, feedback, and support requests
- To communicate with you about products, services, promotions, events, and other news and information we think may be of interest to you (subject to Section 6 on direct marketing)
- To monitor and analyse trends, usage, and activities in connection with our Platform
- To detect, investigate, and prevent fraudulent transactions, abuse, and other illegal activities, and to protect the rights, property, and safety of Bulls Out, JBI, our users, and others
- To comply with legal and regulatory obligations
- To assess job applications and manage employment relationships

4.2 Legal Bases for Processing

The legal basis on which we process your personal information depends on the applicable law in your jurisdiction. See Section 16 for the specific legal bases that apply to you.

4.3 Consent

Where we rely on consent as a legal basis for processing, you may withdraw your consent at any time by contacting us using the details in Section 14. Withdrawal of consent will not affect the lawfulness of any processing before withdrawal.

5. DISCLOSURE TO THIRD PARTIES

We may disclose personal information to the following categories of recipients:

Related entities: Our parent company JBI Holdings LLC, and affiliated companies within the JBI group, including Communify Group, LLC, Communify On Demand, Inc., Communify LLC, Communify Europe Limited, and Communify On Demand Limited, for the purposes described in this Policy.

Service providers: Third-party providers who perform services on our behalf, including cloud hosting, data storage, payment processing, analytics, customer support, email delivery, identity verification, and fraud prevention. We take reasonable steps to ensure these providers are bound by contractual obligations to handle personal information in a manner consistent with applicable data protection law.

Market data providers: Third parties who supply financial market data displayed on our Platform.

Professional advisers: Lawyers, accountants, auditors, and insurers who provide professional services to us.

Law enforcement and regulators: Government authorities, regulators, law enforcement agencies, and courts, where we are required or authorised to do so by law or where disclosure is reasonably necessary for the enforcement of the law, the protection of public safety, or the protection of public revenue.

Business transaction parties: In connection with any merger, acquisition, sale of assets, financing, or restructuring involving Bulls Out or JBI, where personal information may be disclosed to the relevant counterparties and their advisers, subject to confidentiality obligations.

6. DIRECT MARKETING

6.1 Marketing Communications

We may use your personal information to send you direct marketing communications about our products, services, and promotions where we have your consent or where applicable law otherwise permits us to do so.

6.2 Opt-Out

Every marketing communication we send will include a clear and simple mechanism for you to opt out (such as an "unsubscribe" link in emails). You may also contact us at any time using the details in Section 14 to request that we stop sending you marketing communications. We will give effect to your request within a reasonable period.

6.3 Third-Party Marketing

We will not disclose your personal information to third parties for their own direct marketing purposes without your express consent.

7. ANONYMITY AND PSEUDONYMITY

Where it is lawful and practicable, you have the option of not identifying yourself, or of using a pseudonym, when dealing with us. In many cases, it will not be practicable for us to deal with you on

an anonymous or pseudonymous basis. For example, we require your identity to create an Account, process a payment, comply with applicable laws, or respond to a support request. If you do not provide us with the requested personal information, we may not be able to provide you with the relevant service.

8. CROSS-BORDER TRANSFERS

8.1 Transfers

Bulls Out is a wholly owned subsidiary of JBI Holdings LLC, whose principal place of business is in the United States. Our parent company and related entities are incorporated and operate in the United States. Accordingly, personal information collected from users outside the United States will be transferred to and processed in the United States.

8.2 Countries

The countries in which recipients of your personal information are likely to be located include:

United States of America: The location of our parent company JBI Holdings LLC and several affiliated entities, including Communify Group, LLC, Communify On Demand, Inc., and Communify LLC. Our primary corporate systems and certain data processing activities are conducted in the United States.

Australia: Our Platform infrastructure for Australian users is hosted on servers located in Australia, using data centre infrastructure shared with our affiliate FinextraPro.

United Kingdom and Ireland: Certain affiliated entities (including Communify Europe Limited and Communify On Demand Limited) may access personal information for the purpose of providing services or support.

Other countries: From time to time, we may engage service providers located in other countries. Where this occurs, we will update this Section or notify you as appropriate.

8.3 Safeguards

Before transferring personal information internationally, we take steps required by applicable law to ensure the protection of your personal information. The specific safeguards depend on the applicable data protection law in your jurisdiction (see Section 16).

9. DATA SECURITY

9.1 Security Measures

We take reasonable steps to protect the personal information we hold from misuse, interference, loss, and from unauthorised access, modification, or disclosure. Our security measures include:

Technical measures:

- Encryption of personal information in transit and at rest

- Firewalls, intrusion detection systems, and network monitoring
- Role-based access controls that limit access to personal information to authorised personnel who need it for their roles
- Multi-factor authentication for access to sensitive systems
- Regular security testing, vulnerability assessments, and penetration testing
- Secure data centre infrastructure located in Australia (shared with our affiliate FinextraPro) and in the United States, with environmental and physical access controls

Organisational measures:

- Staff training on privacy and information security obligations
- Internal privacy policies and procedures
- Confidentiality obligations for employees, contractors, and service providers
- Incident response plans and procedures for data breach management
- Regular reviews of our security practices

9.2 Data Breach Response

In the event of a data breach, we will comply with the notification requirements under applicable law in the jurisdictions affected by the breach. See Section 16 for jurisdiction-specific breach notification obligations.

9.3 Data Retention and Destruction

We retain personal information only for as long as reasonably necessary for the purposes described in this Policy, or as required by applicable law. When we no longer need personal information, we will take reasonable steps to destroy the information or ensure it is de-identified.

10. YOUR RIGHTS

10.1 General Rights

Depending on the jurisdiction in which you reside, you may have some or all of the following rights in relation to your personal information:

- Access: The right to request access to the personal information we hold about you.
- Correction: The right to request correction of inaccurate, out-of-date, incomplete, or misleading information.
- Deletion: The right to request deletion of your personal information in certain circumstances.
- Portability: The right to receive your personal information in a structured, commonly used, and machine-readable format.
- Restriction: The right to request that we restrict the processing of your personal information in certain circumstances.

- **Objection:** The right to object to our processing of your personal information in certain circumstances.
- **Withdrawal of consent:** Where we rely on your consent, the right to withdraw that consent at any time.
- **Complaint:** The right to lodge a complaint with the applicable data protection authority.

The specific rights available to you depend on the data protection law in your jurisdiction. See Section 16 for details.

10.2 How to Exercise Your Rights

To exercise any of the rights described above, please contact our Privacy Officer using the details in Section 14. We will respond to your request within the timeframe required by applicable law (typically 30 days, subject to extensions permitted by law).

10.3 Identity Verification

We may need to verify your identity before processing your request. We will not charge you for making a request, but we may charge a reasonable fee where requests are manifestly unfounded or excessive, as permitted by applicable law.

10.4 Refusal

We may refuse to comply with a request where applicable law permits us to do so. If we refuse, we will provide you with written reasons for the refusal and information about how to make a complaint.

11. GOVERNMENT RELATED IDENTIFIERS

We will not adopt, use, or disclose a government related identifier as our own identifier for an individual, unless permitted by applicable law. Where we collect government related identifiers (for example, for identity verification or employment purposes), we will handle them in accordance with applicable law.

12. AUTOMATED DECISION-MAKING

12.1 Current Position

Our Platform may use algorithms and automated processes to generate leaderboard rankings, match users to leagues, analyse market data, and personalise the user experience. These processes use personal information (such as your selections and activity within the Platform) to generate outputs.

12.2 Your Rights

Depending on the jurisdiction in which you reside, you may have rights in relation to automated decision-making that significantly affects you. See Section 16 for jurisdiction-specific rights.

13. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in our information handling practices, our business operations, or applicable laws. When we make material changes, we will notify you by posting the updated Policy on our Platform, updating the "Last updated" date at the top of this Policy, and, where appropriate, providing additional notice (such as an in-app notification or email).

We encourage you to review this Policy periodically. Your continued use of our Platform after any changes constitutes your acceptance of the updated Policy.

14. CONTACT US

If you have any questions about this Privacy Policy, our information handling practices, or if you wish to exercise any of your rights, please contact:

Privacy Officer Bulls Out, LLC Email: privacy@bullsout.com Postal Address: Suite G860, Pacific Design Center, 750 N. San Vicente Boulevard, West Hollywood, CA 90069, United States of America

Telephone: +1 729 657 2115

This Privacy Policy is made available free of charge on our Platform and on our website. If you would like a copy of this Policy in a particular form, please contact our Privacy Officer and we will take reasonable steps to provide it in the form you have requested.

15. DATA QUALITY

We take reasonable steps to ensure that the personal information we collect, use, and disclose is accurate, up-to-date, complete, and relevant, having regard to the purpose for which it is collected, used, or disclosed. We encourage you to contact us to update your personal information if it changes or if you believe the information we hold is inaccurate or incomplete.

16. REGIONAL PROVISIONS

The following provisions apply based on the jurisdiction in which you reside. These regional provisions supplement, and where they conflict with, override the general provisions in Sections 1 through 15.

16.1 Australia

a. Applicable Law. This Policy is governed by the Privacy Act 1988 (Cth) and the Australian Privacy Principles ("APPs") contained in Schedule 1 of the Privacy Act. "Personal information" for Australian users has the meaning given in the Privacy Act 1988 (Cth).

b. Collection (APP 3). We only collect personal information that is reasonably necessary for one or more of our functions or activities (APP 3.2). We collect personal information by lawful and fair means (APP 3.5). We will only collect sensitive information with your consent or as otherwise permitted by APP 3.3.

- c. Notification (APP 5). At or before the time we collect your personal information, we will take reasonable steps to notify you of the matters required by APP 5.
- d. Use and Disclosure (APP 6). We will use and disclose your personal information only for the primary purpose of collection, or for a related purpose (or directly related purpose, in the case of sensitive information) where you would reasonably expect such use or disclosure (APP 6.2(a)), or where you have consented (APP 6.2(b)), or as otherwise permitted by the APPs.
- e. Cross-Border Disclosure (APP 8). Before disclosing personal information to an overseas recipient, we take reasonable steps to ensure that the overseas recipient does not breach the APPs (APP 8.1). We remain accountable for acts or practices of an overseas recipient that would breach the APPs (section 16C of the Privacy Act), except where an applicable exception applies. Personal information collected from Australian users will be disclosed to recipients in the United States, United Kingdom, and Ireland as described in Section 8.
- f. Unsolicited Personal Information (APP 4). If we receive personal information that we did not solicit, we will determine within a reasonable period whether we could have collected it under APP 3. If we could not have collected it, we will destroy or de-identify it as soon as practicable, provided it is lawful and reasonable to do so.
- g. Government Related Identifiers (APP 9). We will not adopt, use, or disclose a government related identifier as our own identifier for an individual, unless an exception under APP 9 applies.
- h. Data Quality (APP 10). We take reasonable steps to ensure personal information is accurate, up-to-date, complete, and relevant (APP 10).
- i. Security (APP 11). We take reasonable steps to protect personal information from misuse, interference, loss, and unauthorised access, modification, or disclosure (APP 11.1). When personal information is no longer needed, we take reasonable steps to destroy it or de-identify it (APP 11.2).
- j. Notifiable Data Breaches. In the event of an eligible data breach (as defined in the Privacy Act), we will comply with the Notifiable Data Breaches scheme under Part IIIC of the Privacy Act, including notifying the Office of the Australian Information Commissioner ("OAIC") and affected individuals if serious harm is likely.
- k. Access (APP 12). You have the right to request access to your personal information (APP 12.1). We will respond within 30 days.
- l. Correction (APP 13). You have the right to request correction of inaccurate, out-of-date, incomplete, irrelevant, or misleading personal information (APP 13.1). We will respond within 30 days at no cost to you.
- m. Complaints. If you believe we have breached the APPs, you may lodge a complaint with our Privacy Officer (Section 14). We will acknowledge your complaint within 7 days and provide a written response within 30 days. If you are not satisfied with our response, you may lodge a complaint with the OAIC:

Office of the Australian Information Commissioner GPO Box 5218, Sydney NSW 2001 Telephone: 1300 363 992 Email: enquiries@oaic.gov.au Website: www.oaic.gov.au

n. Automated Decision-Making. From 10 December 2026, the Privacy Act will require us to include additional information in this Policy if we arrange for a computer program to use personal information to make decisions that could reasonably be expected to significantly affect the rights or interests of an individual (APP 1.7-1.9). We will update this Policy before that date to include any required additional information.

o. Anonymity and Pseudonymity (APP 2). Where lawful and practicable, you have the option of not identifying yourself, or of using a pseudonym, when dealing with us (APP 2.1).

16.2 United States and Canada

a. Applicable Law. In the United States, there is no single comprehensive federal privacy law. Your rights depend on the state in which you reside. This section addresses your rights under applicable state privacy laws, including the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA/CPRA"), and other state privacy laws. In Canada, your rights are governed by the Personal Information Protection and Electronic Documents Act ("PIPEDA") and applicable provincial privacy legislation.

b. Categories of Personal Information Collected (California). For the purposes of the CCPA/CPRA, we collect the following categories of personal information: identifiers (name, email, phone number, IP address); commercial information (transaction history, purchase records); internet or network activity (browsing history, interaction with our Platform); geolocation data (derived from IP address); and inferences drawn from the above categories.

c. Purposes. We collect and use personal information for the business purposes described in Section 4, including: providing the Platform, processing transactions, communicating with you, analytics, fraud prevention, and legal compliance.

d. Disclosure for Business Purposes. We disclose personal information to the categories of recipients described in Section 5 for the business purposes described in Section 4.

e. Sale and Sharing. We do not "sell" your personal information as that term is defined under the CCPA/CPRA. We do not "share" your personal information for cross-context behavioural advertising as defined under the CCPA/CPRA.

f. Your Rights (California). If you are a California resident, you have the right to:

- Know what personal information we collect, use, disclose, and sell or share
- Request deletion of your personal information, subject to certain exceptions
- Request correction of inaccurate personal information
- Opt out of the sale or sharing of your personal information (we do not sell or share)
- Limit the use and disclosure of sensitive personal information (we do not use sensitive personal information for purposes beyond those permitted under the CCPA/CPRA)
- Non-discrimination for exercising your privacy rights

To exercise these rights, contact us at privacy@bullsout.com.

g. Your Rights (Other U.S. States). If you reside in a U.S. state with a comprehensive privacy law (including Colorado, Connecticut, Virginia, Utah, Texas, Oregon, Montana, Iowa, Indiana, Tennessee, Delaware, New Hampshire, New Jersey, Nebraska, Maryland, Minnesota, Kentucky, and Rhode Island), you may have rights including access, deletion, correction, portability, and the right to opt out of targeted advertising, the sale of personal information, and certain profiling. To exercise these rights, contact us at privacy@bullsout.com.

h. Appeals. If we deny your privacy request, you may appeal by contacting us at privacy@bullsout.com with the subject line "Privacy Appeal." We will respond within the timeframe required by applicable law.

i. Your Rights (Canada). Under PIPEDA and applicable provincial legislation, you have the right to: access the personal information we hold about you; request correction of inaccurate information; withdraw consent to the collection, use, or disclosure of your personal information (subject to legal or contractual restrictions); and lodge a complaint with the Office of the Privacy Commissioner of Canada.

Office of the Privacy Commissioner of Canada 30 Victoria Street, Gatineau, Quebec K1A 1H3
Telephone: 1-800-282-1376 Website: www.priv.gc.ca

j. Data Breach Notification. In the event of a data breach, we will comply with applicable notification requirements under state and federal law, including notifying affected individuals and applicable state attorneys general as required.

k. Children's Privacy. We do not knowingly collect personal information from individuals under 18 years of age. If we learn that we have collected personal information from a child under 18, we will take steps to delete that information promptly.

16.3 European Union and United Kingdom

a. Applicable Law. If you are located in the European Economic Area ("EEA"), your personal information is processed in accordance with Regulation (EU) 2016/679 (the "GDPR"). If you are located in the United Kingdom, your personal information is processed in accordance with the UK General Data Protection Regulation and the Data Protection Act 2018 (together, the "UK GDPR"). References to "GDPR" in this section include the UK GDPR where the context requires.

b. Data Controller. Bulls Out, LLC is the data controller responsible for your personal information. Our contact details are set out in Section 14.

c. Legal Bases for Processing (GDPR Article 6). We process your personal information on the following legal bases:

- Contractual necessity (Article 6(1)(b)): Processing necessary for the performance of our contract with you (the Terms and Conditions), including to create and manage your Account, provide the Platform, process payments, and enable participation in leagues and competitions.
- Legitimate interests (Article 6(1)(f)): Processing necessary for our legitimate interests or those of a third party, provided those interests are not overridden by your data protection rights. Our legitimate interests include: operating, improving, and securing the Platform;

fraud prevention; analytics; and direct marketing (where you have not opted out). You have the right to object to processing based on legitimate interests (see paragraph (g) below).

- Consent (Article 6(1)(a)): Where we rely on your consent (for example, for certain marketing communications or the use of non-essential cookies), you may withdraw consent at any time.
- Legal obligation (Article 6(1)(c)): Processing necessary to comply with a legal obligation to which we are subject.

d. Data Protection Officer. For data protection enquiries, contact our Privacy Officer at privacy@bullsout.com.

e. International Transfers. Personal information collected from EEA and UK users is transferred to and processed in the United States. We rely on the following transfer mechanisms to ensure adequate protection:

- The EU-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework (where applicable and where Bulls Out or its affiliates have self-certified)
- Standard Contractual Clauses approved by the European Commission (for transfers to recipients not covered by the Data Privacy Framework)
- Any other transfer mechanism recognised under the GDPR or UK GDPR

You may request a copy of the relevant transfer safeguards by contacting us at privacy@bullsout.com.

f. Data Retention. We retain personal information for as long as necessary to fulfil the purposes described in Section 4, unless a longer retention period is required or permitted by law. The specific retention periods depend on the nature of the information and the purpose for which it was collected. When personal information is no longer needed, we will securely delete or anonymise it. You may request information about our retention periods by contacting us at privacy@bullsout.com.

g. Your Rights (GDPR). If you are located in the EEA or the UK, you have the following rights under the GDPR:

- Access (Article 15): The right to obtain confirmation of whether we process your personal data and to request a copy.
- Rectification (Article 16): The right to request correction of inaccurate or incomplete personal data.
- Erasure (Article 17): The right to request deletion of your personal data in certain circumstances (the "right to be forgotten").
- Restriction (Article 18): The right to request restriction of processing in certain circumstances.
- Data portability (Article 20): The right to receive your personal data in a structured, commonly used, machine-readable format and to transmit it to another controller.
- Objection (Article 21): The right to object to processing based on legitimate interests or for direct marketing purposes.

- Automated decision-making (Article 22): The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects or similarly significantly affects you.
- Withdrawal of consent: Where we rely on your consent, the right to withdraw that consent at any time without affecting the lawfulness of processing before withdrawal.

To exercise these rights, contact us at privacy@bullsout.com. We will respond within 30 days (extendable by a further 60 days for complex requests, with notice to you).

h. Supervisory Authority. You have the right to lodge a complaint with a supervisory authority in the EEA Member State or UK country in which you reside. For users in Ireland, the relevant authority is:

Data Protection Commission 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland Website: www.dataprotection.ie

For users in the United Kingdom, the relevant authority is:

Information Commissioner's Office Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, United Kingdom Telephone: 0303 123 1113 Website: www.ico.org.uk

i. Cookies and ePrivacy. We use cookies and similar technologies as described in Section 2.2. Under EU and UK ePrivacy law, we will obtain your prior consent before placing non-essential cookies on your device. You can manage your cookie preferences through the cookie consent mechanism presented when you first access the Platform, and through your browser settings.

j. Children's Privacy. We do not knowingly collect personal information from individuals under 18 years of age. The GDPR sets 16 as the default age of consent for data processing (subject to lower ages set by Member States). Regardless, our Terms and Conditions require all users to be at least 18.

17. GOVERNING LAW

This Policy is governed by the Applicable Law specified for your region in the Terms and Conditions.