

# ID5 Platform Privacy Policy

Last Modified: 29 June 2026

## Introduction

ID5 provides an evolving suite of identity solutions for the digital advertising ecosystem, designed to prioritize user privacy while enabling effective advertising. Our technology platform enables publishers and advertisers to more effectively recognize browsers and other devices over time by generating a unique, pseudonymous ID. More about the ID5 Platform is in “What is the ID5 Platform” section, below.

In general, the ID5 Platform is used by businesses that wish to advertise their products and services on websites, mobile apps and other digital media properties (which we collectively refer to as "**Digital Properties**"), as well as the Digital Properties themselves. We consider any business that owns or controls a Digital Property which has enabled the ID5 Platform to be a "**Client**" and any business that might leverage the ID5 Platform on a Digital Property controlled by a different business to be a "**Partner**".

This ID5 Platform Privacy Policy (this "**Privacy Policy**") describes how ID5 collects, uses, shares and otherwise processes Platform Data. It describes how ID5 may enable or allow Clients and Partners to use Platform Data, but otherwise does not apply to our Clients' or Partners' practices. If you are interested in our website privacy policy, please click [here](#).

For quick access to the ID5 Privacy Preference Center, where you can exercise your rights as a data subject, please click [here](#).

## The ID5 Platform Privacy Policy at a Glance

Question	Summary
<b>What information do we collect and use?</b>	The Platform is designed to collect and use Platform Data (i.e., Device Data, Client Data, and ID5 IDs) such as cookie IDs, IP addresses, browser information, and hashed emails. We do not collect directly identifiable data like your name or address, nor do we collect sensitive data.

<b>How do we collect information?</b>	The Platform uses cookies, pixels, tags, mobile SDKs, and similar technologies to collect Platform Data about web browsers and devices across websites and apps.
<b>For what purposes do we use the collected information?</b>	ID5 uses the information collected via the Platform to provide and enhance our identity services. This includes facilitating device identification, fraud prevention, and improving our identity graph through algorithmic analysis.
<b>In European Jurisdictions, on what legal basis do we process Personal Data?</b>	Our legal basis is generally your consent, obtained for us by the operators of the Digital Properties that use our technology and transmitted to us via the IAB TCF framework.
<b>What information do we share with third parties?</b>	Where permitted by law and your expressed choices, we provide Platform Data to our Clients, Partners, and service providers for the purpose of operating and enhancing our and their services, for security, or as required by law.
<b>How is the information stored and how long is it kept?</b>	Platform Data is stored using generally accepted security standards. It is usually aggregated or deleted within 100 days, but may be retained for up to 18 months for specific non-commercial purposes such as security and service improvement.
<b>What are your privacy choices?</b>	We support the IAB Europe Transparency and Consent Framework (TCF). You may also opt out of ID5's Platform and services directly via our <a href="#">privacy preference center</a> . We honor legally recognized universal opt-out signals like the Global Privacy Control.
<b>What are your rights?</b>	Depending on your jurisdiction, you may have rights to access, correct, delete, or port your data, and to object to or opt-out of certain processing.
<b>Questions?</b>	Please email us at <a href="mailto:privacy@id5.io">privacy@id5.io</a> .

## What is the ID5 Platform (or the "Platform")?

ID5 operates an identity platform for the digital advertising industry. By "identity", we mean that we have a technology that enables our systems to recognize a browser or device (a "user") over time without identifying an actual person. By "Platform", we mean we provide technology that websites, mobile apps and publishers of other internet-connected properties (such as internet-connected TVs) use to recognize users on their Digital Properties. Advertisers, or companies working on an advertiser's behalf, use the

Platform to manage ad campaigns and target advertising to users in a more efficient way. Digital publishers and other "sellers" want their ads to be relevant to their readers, which helps them to offer content for no cost or lower cost. Advertisers, advertising agencies, and other "buyers" want to use their advertising dollars efficiently by reaching the right audiences, and by measuring the effectiveness of their ads. To accomplish these goals, We enable Clients—including digital publishers and advertising technology platforms and their service providers—to use our Platform to more efficiently and effectively recognize their users and/or to enable their own Clients to do so. ID5 is not an ad network, a media buyer or seller. We do not create ad targeting profiles via the Platform.

## What do we mean by Platform Data?

The Platform is designed to use certain types of information, that collectively we call "**Platform Data**". Platform Data includes: (i) "**Device Data**"— information collected from browsers and devices by our technology, products and services on Digital Properties, including but not limited to Digital Identifiers (defined below); (ii) "**Network Data**" – information made available by the network infrastructure, such as DNS information; (iii) "**Client Data**"— information provided or uploaded to us via our Platform by our Clients; and (iv) "**ID5 IDs**" - random unique identifiers that we create and connect to Device Data and/or Client Data.

Some Platform Data (for example, cookie IDs, mobile advertising identifiers, ID5 IDs, and IP addresses) may help our systems recognize or single out a particular computer or device, and may be considered "**Personal Data**" or "**personal information**" in some jurisdictions, including the European Economic Area, United Kingdom, and certain U.S. states. This data allows us to recognize a particular computer or device over time. We call cookie IDs, mobile advertising IDs, ID5 IDs, hashed email addresses ("HEMs") and other random unique identifiers "**Digital Identifiers**". Digital Identifiers are also considered Personal Data in most places.

Our Platform is not designed to utilize information that by itself identifies an individual in the "real world", such as someone's name, address, phone number, raw (un-hashed) email address, or government identifier. We also do not knowingly collect, process, or store "sensitive" or "special category" personal data, such as health information, data revealing racial or ethnic origin, or data about children.

## Glossary of Certain Terms

- **Browser:** A browser, or web browser, is the user interface or application through which you view web Digital Properties.
- **Cookie:** A cookie is a small text file that is stored in a web browser by a website. By saving information

in a cookie, websites and servers can remember preferences or recognize web browsers from one visit to another.

- **Cross-Device Graph:** A map of pseudonymous identifiers that are determined to likely belong to the same user across multiple devices, such as a laptop, smartphone, and tablet.
- **ID Syncing:** A common process in the digital advertising industry that enables advertisers to link up pseudonymous data sets from multiple advertising platforms.
- **Interest-Based Advertising:** Associates a user's activity and interest information with a browser cookie or other online identifier in order to provide more useful and relevant advertising and/or content. It is sometimes also called "ad targeting" "online behavioral advertising", "targeted advertising", "cross-context behavioral advertising" or "tailored advertising".
- **Mobile Advertising Identifiers:** Unique IDs associated with individual mobile devices (e.g., Apple's IDFA or Google's AAID).
- **Persistent Identifier:** An identifier that is stored on a user's device or otherwise associated with a user over an extended period. This allows a browser or device to be recognized across different Browser sessions or over time. Common examples of persistent identifiers include cookies and mobile advertising identifiers.
- **Probabilistic Identification:** The process of using a combination of pseudonymous signals passively made available by a device or browser (such as operating system, browser type, IP address, and user agent) to infer a likely match to an existing ID5 ID without the use of cookies or other persistent identifiers stored on the device.
- **Profiling:** Any form of automated processing of Personal Data to evaluate, analyze, or predict personal aspects concerning an individual.

## What Information Do We Collect?

- **Device Data.** When you visit a Digital Property that uses our technology Platform, we collect certain information about your browser and device, including:
  - *Information about your browser:* the type of browser, browser language, browser settings, and cookie information.
  - *Information about your device:* information about the device's operating system including its version and connection type, device make, device model, mobile advertising identifiers (such as your Apple IDFA or Google AAID), and the IP address from which the device accesses a Digital Property.
  - *Information about the Digital Properties you visit:* including web pages or apps visited or used and the timestamp of those visits.

- *Information about your Internet service*: including information about which Internet Service Provider (ISP) you use.
- **Network Information**: When you interact with a Digital Property that uses our technology, we may receive information made available by the network infrastructure, such as DNS information, which we use to help create and manage ID5 IDs. We consider this DNS information Personal Data.
- **Client Data**. Our Clients may provide or upload to us or our Platform "Client Data", which typically includes a "hashed" email address ("hashing" prevents us from seeing the actual email address) or other pseudonymous identifiers they hold.
- **Information Used for Probabilistic Identification**. In some cases, where permitted by law and a valid legal basis has been established, we use a combination of the signals above (such as IP address, browser type, and operating system) for the purpose of Probabilistic Identification to recognize a browser or device where a cookie-based ID5 ID is not present.

## How Do We Collect Information?

- The Platform uses cookies, pixels, tags, mobile SDKs, and similar technologies to collect data associated with particular web browsers or devices.
- We and the Platform also receive data from our Clients and other third parties.

## Our use of Cookies and Similar Technologies

To provide our services, we use cookies and similar technologies (like pixels and tags) to be placed on the browsers of individuals who visit the Digital Properties of our Clients. Cookies are small text files that contain a string of characters. Specifically, we use cookies for the following purposes:

- To store the ID5 ID, which is our core function for recognizing a browser over time.
- To store a user's privacy choices, such as an opt-out preference, so we can honor that choice on subsequent visits.
- To facilitate the ID Syncing process with our Partners.

Our cookie is set in a third-party context and has a duration of 12 months from when it is last updated. In jurisdictions where the ePrivacy Directive or similar laws mandating consent apply, we rely on the consent obtained by our Clients and Partners on their Digital Properties to set these cookies. You can control and manage cookies in various ways through your browser settings. Full information on ID5's use of cookies and local storage, including duration and purpose, are available [here](#).

## How Do We Use the Information We Collect?

- To provide products and services to our Clients and Partners, including in connection with ID5 IDs, our identity graph, and our cross-device graph.
- To develop, maintain, and improve our products and services, including:
  - Conducting research and development to better optimize the efficiency of our Platform.
  - Investigating, protecting against and deterring malicious or fraudulent activity.
- To enable ID5 to analyze the data we collect and improve the accuracy and efficiency of our Platform. We may utilize algorithmic analysis and modeling on Platform Data to improve the accuracy and efficiency of our identity resolution services. We conduct these activities only where we have a valid legal basis to do so.

The ID5 service works by helping our Clients and Partners recognize a browser or device over time. In some instances, our technology may create more than one ID5 ID for the same user. The process of linking these multiple IDs together to understand they belong to a single user may be considered 'profiling' under certain data protection laws, like the GDPR, which is the only reason why we ask for your consent for this limited activity (specifically under IAB TCF Purpose 3 and 5). **To be clear, ID5 does not use this information to build ad targeting profiles or to decide which ads you see.** Our role is strictly to provide a pseudonymous identifier and its connection to our Client's user identifiers; our Clients use this identifier for their own purposes, in accordance with the data protection laws and their own privacy policies.

## Legal Basis for Processing Personal Data (Europe)

If you are a data subject of a European Jurisdiction (the EEA, UK, or Switzerland), our legal basis for processing your Personal Data will depend on the specific context. We generally rely on **consent** obtained for us by the operators of the Digital Properties that use our technology, except as described below. We are a registered vendor in the IAB Europe Transparency and Consent Framework (TCF) and rely on it to receive and honor your privacy choices.

Specifically, and in line with our IAB Global Vendor List (GVL) registration, we process your data based on the following TCF Purposes and legal bases:

Purpose	Legal Basis

Store and/or access information on a device (Purpose 1)	Consent
Create a personalised ads profile (Purpose 3)	Consent
Create a personalised content profile (Purpose 5)	Consent
Develop and improve products (Purpose 10)	Consent
Ensure security, prevent and detect fraud, and fix errors (Special Purpose 1)	Legitimate Interests
Save and communicate privacy choices (Special Purpose 3)	Legitimate Interests

*Match and combine data from other data sources (Feature 1), Link different devices (Feature 2), and Identify devices based on information transmitted automatically (Feature 3) are used to support the above purposes.*

## How and Why Do We Share the Information We Collect?

ID5 shares Platform Data with the following third parties:

- Clients, Partners and their third-party vendors:** We provide ID5 IDs and associated graph data to our Clients and Partners (defined above), as permitted by your choices on their Digital Properties. All such sharing is governed by the consent signals we receive via the TCF or other legally-valid mechanisms.
- Vendors / Processors:** We share Platform Data with our vendors (including our hosting providers, data analytics providers, and anti-fraud providers) so that they can provide services to us.
- Legal Rights and Compliance with Law:** We may disclose Platform Data if we reasonably suspect malicious activity or believe it is required by law, subpoena, or other legal process, including to meet national security or law enforcement requirements.
- ID5 Affiliates:** We share Platform Data with other companies in the ID5 group of companies. A complete list of ID5 entities is available at the end of this Privacy Policy, below.
- Business Transfers:** We may transfer Platform Data to a successor entity in connection with a corporate merger, consolidation, sale of assets, or other corporate change.

### Additional Disclosures for Specific Jurisdictions

- For Residents of Japan:** The Digital Identifiers we share with our Clients and Partners may be

considered "Personally-Referable Information" under Japan's Act on the Protection of Personal Information (APPI). We take steps, including through our contracts and reliance on industry-standard consent frameworks, to ensure that where this information is transferred to a third party who may link it to identify you and/or transfer that information outside of Japan, the necessary consents have been obtained.

## How Is Platform Data Stored, and How Long Is It Kept?

- **Security:** ID5 uses generally accepted industry security mechanisms, including data encryption at rest and in transit, and strict access controls, to protect information.
- **Retention:** We practice data minimization. For the provision of our live services, such as creating and providing ID5 IDs, data is held for a maximum of 100 days before being deleted or aggregated. We may retain a separate, limited dataset for up to 18 months strictly for non-commercial purposes like maintaining the security and integrity of our platform, such as preventing fraud and invalid traffic (IVT). This security data is not linked to our identity graph or used for any advertising purposes.

## What Are Your Privacy Choices?

- **IAB Europe Transparency and Consent Framework:** We are a registered vendor with the TCF, which is designed to provide you with transparency and choice about the third parties used on Digital Properties. You can manage your choices through the consent management platform on any website that participates in the TCF.
- **ID5 Universal Opt Out:** You may visit our [Privacy Preference Center](#) to opt out of ID5's processing of your Personal Data for our own business purposes.
  - *How it Works:* When you opt out via your browser, an opt-out cookie is stored in your web browser. While our systems may generate a new ID5 ID on a subsequent visit, the presence of the opt-out cookie prevents us from processing this new ID or any associated data for purposes beyond honoring your opt-out.
  - *Email Opt-Out:* Our preference center also allows you to opt out by providing your email address. **We will hash your email address to match it against hashed emails in our systems and add it to a suppression list.**
- **Global Privacy Control (GPC):** We honor opt-out preference signals received from GPC as a valid request to opt out of the sale or sharing of your Personal Data under applicable US State Privacy Laws.

## What Happens if this Privacy Policy is Changed?

Please check this page for changes. ID5 may change this Privacy Policy at any time, but if we make changes, those changes will only apply to Personal Data collected or received by ID5 *after* the date of that Privacy Policy edition. For any of your Personal Data held by ID5 prior to that date, the Privacy Policy in effect on that date will continue to apply. You may find an archive of ID5 Privacy Policies and applicable dates [here](#).

## Your Rights

As we only process pseudonymous data, we do not know the real-world identity of the individuals associated with an ID5 ID. This presents challenges for verifying identity when you make a rights request. We have balanced this against your right to privacy and have adopted a 'best efforts,' privacy-protective approach. When you use our opt-out tools, we will honor all requests associated with the signals you provide (such as your browser cookie or a hashed email address) without requiring further proof of identity. Our priority is to ensure your choice is respected, even if it means we 'over-opt-out' a user who did not make the request. The only consequence for a data subject is that our advertiser, publisher Clients and/or Partners can no longer use their ID5 ID, which we consider a low risk to the individual.

For jurisdiction-specific rights, disclosures, and information, please refer to the "Additional Information and Disclosures for Specific Jurisdictions" section [below](#).

## Your Rights Regarding Automated Decision-Making

In certain jurisdictions, you have the right to be informed when a decision is made about you based exclusively on an automated process. While ID5 does not make advertising decisions, our Clients and Partners may use the ID5 ID or ID5's services to do so. Should you wish to understand the logic involved in such a decision, you may have the right to request an explanation and to have the decision reviewed by a person. Please direct such requests to the operator of the website or app where you saw the advertisement. For more information specific to your jurisdiction, please see the "Additional Information and Disclosures for Specific Jurisdictions" section.

## European Jurisdiction Data Subject Rights

If you are a data subject of a European Jurisdiction, you have the right to: (i) access and obtain a copy of your Personal Data; (ii) erasure of your Personal Data; (iii) rectification of your Personal Data; (iv) object to processing; (v) restrict processing; and (vi) data portability. You may exercise these rights via our [Privacy Preference Center](#) or by emailing us at [privacy@id5.io](mailto:privacy@id5.io). You also have the right to lodge a complaint with a European Data Protection Authority.

## Your Rights under Certain U.S. State General Privacy Laws

If you are located in a U.S. state with an effective general privacy law (such as California, New Jersey, Colorado, Connecticut, Virginia, or Utah), you may have some or all of the following rights:

- **The Right to Know/Access:** The right to request information about the categories and specific pieces of personal information we have collected about you.
- **The Right to Delete:** The right to request the deletion of your personal information, subject to certain exceptions.
- **The Right to Correct:** The right to request that we correct inaccurate personal information that we maintain about you.
- **The Right to Data Portability:** The right to request a copy of your personal information we have collected about you in a portable format that allows you to transmit the information to another entity.
- **The Right to Non-Discrimination for Exercising Your Rights:** The right not to receive discriminatory treatment for exercising any of your privacy rights.
- **The Right to Opt-Out of Sale or Sharing:** The right to opt-out of the "sale" or "sharing" of your personal information for purposes of cross-context behavioral advertising. While we do not sell your Personal Data collected via the Website for money, our use of third-party analytics cookies may be considered a "sale" or "share". You can exercise this right by opting out through the ID5 Preference Center or by enabling the Global Privacy Control (GPC) signal in your browser, which we honor.

The methods by which you may exercise these rights, as well as additional information about your options, are described below.

- **Exercising Your Rights:** You may exercise your rights to access, delete, or correct your data via our [Privacy Preference Center](#) or by calling our toll-free telephone number: 1-888-821-2911.
- **Exercising Your Right to Opt-Out:** You may exercise your right to opt-out via our [Privacy Preference Center](#) or by enabling the Global Privacy Control signal in your browser.
- **Appealing Data Subject Rights Decisions:** Some states offer the right to appeal a decision we make related to your data subject rights request. You may appeal any decision by ID5 by emailing [privacy@id5.io](mailto:privacy@id5.io). We provide further information on how to make an appeal directly via certain state authorities below.
- **Authorized Agents:** You may use an authorized agent to submit requests on your behalf where applicable law grants you such rights. Your authorized agent will need to provide us with a copy of a written permission that is signed by you. While any user or designated agent can use our automated browser and email opt-out tools without providing proof, for sensitive requests such as data access or deletion made by an agent, we require signed permission from you. This is a security

measure to protect your data from potentially fraudulent access by an unauthorized third party.

## Categories of Personal Data Processed under US State Privacy Law

We collect (and during the last 12 months have collected) the following categories of personal information: **Identifiers** (such as cookie IDs, mobile ad IDs, ID5 IDs, IP addresses, and hashed emails) and **Internet or other electronic network activity information** (such as browser information, user agent, timestamps, and network information). We do not knowingly collect, use, or disclose sensitive Personal Data.

## Disclosure of Personal Data for purposes of US State Privacy Laws:

- **"Sales"/"Sharing"**: We "sell" and/or "share" (as defined by applicable US State Privacy Laws) Identifiers and Internet or other electronic network activity information to our Clients and Partners in connection with their advertising activities, including cross-context behavioral advertising. We do not knowingly sell or share the Personal Data of children under 18, or, where such minimum age is lower under applicable US State Privacy Laws, the applicable minimum age.
- **"Disclosures for a Business Purpose"**: We disclose these categories of Personal Data for a business purpose to our service providers/processors as described above.

## Appealing Data Subject Rights Decisions

Some U.S. states provide you with the right to further appeal our determination to a consumer protection agency located in that state where we deny your data subject rights request. For your ease of access, you may find links to some applicable regulatory authorities below, or you may email [privacy@id5.io](mailto:privacy@id5.io).

- Colorado – The [Colorado Attorney General's Office](#).
- Connecticut – The [Connecticut Attorney General's Office](#).
- Maryland – Maryland Attorney General [Consumer Protection Division](#).
- Nebraska – Nebraska [Attorney General's Office](#).
- New Hampshire – [Data Privacy Unit](#) of the Consumer Protection and Antitrust Bureau of the New Hampshire Attorney General's Office.
- New Jersey - [Division of Consumer Affairs](#) in the Department of Law and Public Safety of New Jersey.
- Texas - For denied appeals, visit the Texas Attorney General's Office, [Consumer Protection Division](#).
- Virginia – For denied appeals, visit the Virginia Attorney General's Office, [Consumer Protection Division](#).

## Additional Disclosures

### California Data Broker Registration

ID5 is registered as a data broker in the State of California.

### "Do Not Track"

ID5 does not currently respond to browser "Do Not Track" signals due to a lack of industry standards regarding how such signals should be interpreted. However, we do honor Global Privacy Control signals as described above.

### Global Operations and Data Transfers

ID5 is a global company headquartered in the United Kingdom.

- To the extent that we transfer Personal Data from European Jurisdictions, via certain Clients and Partners, we rely on appropriate data protection safeguards such as the EU-U.S. Data Privacy Framework, the UK Extension to the DPF, and/or the European Commission's Standard Contractual Clauses, as applicable.
- We are committed to complying with all applicable laws governing data transfers, including U.S. export controls and national security regulations, and do not transfer data to prohibited entities or jurisdictions.
- For transfers from other jurisdictions, such as South Africa and Quebec, we conduct a transfer impact assessment to ensure that the destination country provides a level of protection for personal information that is equivalent to that offered in your jurisdiction. Where this is not the case, we rely on appropriate safeguards, such as binding corporate rules or standard contractual clauses, to protect your data.

### Industry Codes

ID5 supports advertising industry self-regulation, and endorses best practices and self-regulatory requirements that apply to the advertising industry. To learn more about interest-based advertising and industry self-regulation, please visit any of the following organizations:

- **EU:** European Interactive Digital Advertising Alliance
- **US:** Digital Advertising Alliance

## Additional Information and Disclosures for Specific Jurisdictions

### For Residents of Canada (including Quebec)

In addition to the rights described above, you have the right to be informed of the names or categories of third parties to whom we communicate your information. These are described in the section "How and Why Do We Share the Information We Collect?". You also have the right to withdraw your consent to our processing at any time. Our use of cookies and similar technologies may be considered technology that includes functions for identifying or profiling you. You may deactivate these functions by managing your cookie settings in your browser or using our Privacy Preference Center. For more information on your rights regarding automated decision-making, please see the "Your Rights" section.

### For Residents of the United Kingdom

#### How to Raise a Data Protection Complaint

Under the Data (Use and Access) Act 2025 (DUAA), individuals must raise any concerns about how their personal data is handled with us first, before contacting the Information Commissioner's Office (ICO).

If you have questions about how we process your personal data, or if you believe your data-protection rights have not been respected, you can submit a complaint using the contact details below:

#### Data Protection Contact:

iStorm Solutions Ltd

[Richard.merrygold@istormsolutions.co.uk](mailto:Richard.merrygold@istormsolutions.co.uk)

10 John Street, Stratford Upon Avon, CV37 6UB

We will acknowledge your complaint and aim to respond within one month. If your complaint is complex or requires more time, we will keep you informed.

#### Escalating Your Complaint

If you are not satisfied with our response, or if you believe we have not handled your complaint appropriately, you may escalate the matter to the Information Commissioner's Office (ICO).

#### ICO contact details:

Website: <https://ico.org.uk/make-a-complaint/>

Telephone: 0303 123 1113

Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

### For Residents of Brazil

You have the right to be informed about the possibility of not providing consent and the consequences of such a refusal. Providing consent for the processing of your data is voluntary. If you choose not to consent, or to withdraw your consent, an ID5 ID will not be created or shared for advertising purposes. This means that the advertising you see on websites and apps may be less relevant to your interests. It may also impact the ability of digital publishers to fund their content through advertising. You also have the full scope of rights under Article 18 of the LGPD, including confirmation of processing, access, correction, anonymization, portability, and deletion of your data.

### For Residents of South Africa

The provision of your personal information to us is voluntary. However, failure to provide the information may result in our inability to provide our services effectively, meaning the advertising you see may be less relevant. You have the right to lodge a complaint with the Information Regulator.

Contact name and address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001

Email: [complaints.IR@justice.gov.za](mailto:complaints.IR@justice.gov.za).

### For Residents of South Korea

Information on our data destruction methods: When personal information is no longer necessary, it is destroyed in a way that prevents recovery or reuse. Electronic files containing personal information are permanently deleted using a technical method that makes recovery impossible (e.g., cryptographic erasure or overwriting). Any personal information on paper is destroyed by shredding or incineration.

### For Residents of India

You have the right to make a complaint to the Data Protection Board of India. Contact details will be provided here once they are officially established.

### Residents of Japan

The Digital Identifiers we share with our Clients and Partners may be considered "Personally-Referable Information" under Japan's Act on the Protection of Personal Information (APPI). We take steps, including

through our contracts and reliance on industry-standard consent frameworks, to ensure that where this information is transferred to a third party who may link it to identify you and/or transfer that information outside of Japan, the necessary consents have been obtained.

## Contact Information

If you have any questions, please contact our Data Protection Officer at [privacy@id5.io](mailto:privacy@id5.io) or by postal mail:

- **ID5 Technology Ltd:** 8 Devonshire Square, 6th Floor, London EC2M 4YJ, United Kingdom.
- **EU Representative (ID5 Technology SAS):** 14 Rue du Vieux Faubourg, 59800, Lille, France.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please reach out directly to [privacyescalation@id5.io](mailto:privacyescalation@id5.io) and a member of our team will respond to you within five business days.