

Verified Privacy Policy

Effective as of May 20, 2024.

This Privacy Policy describes how Verified Network Inc. (“**Verified**”, “**we**”, “**us**” or “**our**”) processes personal information that we collect through or in connection with our services (the “**Services**”), including:

- our website located at <https://www.verified.inc> (the “**Site**”),
- the “**Digital ID Service**,” a service linked to our web wallet solution for storing and sharing your digital identifiers (the “**Verified Web Wallet**”) through which you can share personal information that you have submitted to, and that has been verified by, our third-party verification partners (“**Issuers**”) with other of our third-party business partners with whom you have a relationship (“**Relying Parties**”), and
- the “**Verified Email Service**,” a service linked to the Verified Web Wallet that allows senders of email messages to verify their identities and recipients to classify the messages they receive and ask unverified senders to verify themselves.

For the purposes of this Privacy Policy, the terms “you,” and “your,” refer to the individuals about whom we collect personal information through the Services, including from Issuers, Relying Parties, and users of the Verified Web Wallet and Site.

NOTICE TO EUROPEAN USERS: Please see the [Notice to European Users](#) section for additional information for individuals located in the European Economic Area or United Kingdom (which we refer to as “**Europe**”, and “**European**” should be understood accordingly) below.

Index

Personal information we collect

Information you provide to us.

General

Personal information you may provide to us through any of the Services includes:

Digital ID Service

In addition to the personal information identified in the “General” section, above, personal information you may provide to us through the Digital ID Service may also include:

Verified Email Service

In addition to the personal information identified in the “General” section, above, personal information you may provide to us through the Verified Email Service includes:

Third-party sources. We may combine personal information we receive from you with personal information we obtain from other sources, such as:

- Issuers, which may provide identity data to your Verified Web Wallet with your consent.
- Users of the Verified Email Service. We may obtain personal information about you from a user of the Verified Email Service when you send that user an email.
- Third-party services, such as social media services, that you use to log into, or otherwise link to, your Verified Web Wallet. This data may include your username, profile picture and other

information associated with your account on that third-party service that is made available to us based on your account settings on that service.

Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Verified Web Wallet and Site, our communications, such as:

Cookies and similar technologies. Some of the automatic collection described above is facilitated by the following technologies:

How we use your personal information

Service delivery and operations. We may use your personal information to:

Research and development and analytics. We may use your personal information for research and development and analytics purposes, including to analyze and improve the Services and our business and to understand user activity on the Services. For example, we use Google Analytics for this purpose. You can learn more about Google Analytics and how to prevent the use of Google Analytics relating to your use of the Services here: <https://tools.google.com/dlpage/gaoptout?hl=en>. As part of these activities, we may create aggregated, de-identified or other anonymous data from personal information we collect. We may use this anonymous data and share it with third parties for our lawful business purposes, including to analyze and improve the Services and promote our business, and will not attempt to reidentify any such data.

Marketing and advertising. If you are a user of the Verified Web Wallet or the Site, we and our service providers may collect and use your name, email address and other contact details for our marketing purposes, including to send you direct marketing communications. You may opt-out of our marketing communications as described in the Opt-out of marketing section below. We may also use your personal information for interest-based advertising. Our third-party advertising partners may use cookies and similar technologies to collect information about your interaction (including the data described in the automatic data collection section above) with the Services, our communications and other online services over time, and use that information to serve online ads that they think will interest you. This is called interest-based advertising. We may also share information about our users with these companies to facilitate interest-based advertising to those or similar users on other online platforms. You can learn more about your choices for limiting interest-based advertising in the Your choices section, below.

Compliance and protection. We may use your personal information to:

Cookies and similar technologies. In addition to the other uses included in this section, we may use the Cookies and similar technologies described above for the following purposes:

With your consent. In some cases, we may specifically ask for your consent to collect, use or share your personal information, such as when required by law.

How we share your personal information

Google restricted scopes data (applicable only to Verified Email Service)

Your choices

Access or update your information. If you have registered for an account with us, you may review and update certain account information by logging into the account.

Opt-out of communications. You may opt-out of marketing-related emails by following the opt-out or unsubscribe instructions at the bottom of the email, or by contacting us. Please note that if you choose to opt-out of marketing-related emails, you may continue to receive service-related and other non-marketing emails.

If you receive text messages from us, you may opt out of receiving further text messages from us by replying STOP to our message.

Blocking images/clear gifs: Most browsers and devices allow you to configure your device to prevent images from loading. To do this, follow the instructions in your particular browser or device settings.

Do Not Track. Some Internet browsers may be configured to send “Do Not Track” signals to the online services that you visit. We currently do not respond to “Do Not Track” signals. To find out more about “Do Not Track,” please visit <http://www.allaboutdnt.com>.

Declining to provide information. We need to collect personal information to provide certain services. If you do not provide the information we identify as required or mandatory, we may not be able to provide those services.

Advertising choices. You may be able to limit use of your information for interest-based advertising through the following settings/options/tools:

- Browser settings. Changing your internet web browser settings to block third-party cookies.
- Privacy browsers/plugin-ins. Using privacy browsers and/or ad-blocking browser plug-ins that let you block tracking technologies.
- Platform settings. Google and Facebook offer opt-out features that let you opt-out of use of your information for interest-based advertising. You may be able to exercise that option at the following websites:
 - Google: <https://adssettings.google.com/>
 - Facebook: <https://www.facebook.com/about/ads>
- Ad industry tools. Opting out of interest-based ads from companies that participate in the following industry opt-out programs:
 - Network Advertising Initiative: http://www.networkadvertising.org/managing/opt_out.asp
 - Digital Advertising Alliance: optout.aboutads.info.

Platform settings. As noted above, you may be able to prevent the use of Google Analytics relating to your use of the Services here: <https://tools.google.com/dlpage/gaoptout?hl=en>.

Linked third-party platforms. If you are a user of the Verified Email Service, as the Verified Email Service is connected through your email provider, you may be able to use your settings in your account with that platform to limit the information we receive from it. If you revoke our ability to access information from your email provider, that choice will not apply to information that we have already received from that third party.

Other sites and services

The Services may contain links to websites, mobile applications, and other online services operated by third parties. In addition, our content may be integrated into web pages or other online services that are not associated with us. These links and integrations are not an endorsement of, or representation that we are affiliated with, any third party. We do not control websites, mobile applications or online services operated by third parties, and we are not responsible for their actions. We encourage you to read the privacy policies of the other websites, mobile applications and online services you use.

Security

We employ technical, organizational and physical safeguards designed to protect the personal information we collect. However, security risk is inherent in all internet and information technologies and we cannot guarantee the security of your personal information.

International data transfer

We are headquartered in the United States and may use service providers that operate in other countries. Your personal information may be transferred to the United States or other locations where privacy laws may not be as protective as those in your state, province, or country.

Children

The Services are not intended for use by anyone under 18 years of age. If you are a parent or guardian of a child from whom you believe we have collected personal information in a manner prohibited by law, please contact us. If we learn that we have collected personal information through the Services from a child without the consent of the child's parent or guardian as required by law, we will comply with applicable legal requirements to delete the information.

Changes to this Privacy Policy

We reserve the right to modify this Privacy Policy at any time. If we make material changes to this Privacy Policy, we will notify you by updating the date of this Privacy Policy and posting it on the Services or other appropriate means. Any modifications to this Privacy Policy will be effective upon our posting the modified version (or as otherwise indicated at the time of posting). In all cases, your use of the Services after the effective date of any modified Privacy Policy indicates your acknowledging that the modified Privacy Policy applies to your interactions with the Services and our business.

How to contact us

Notice to European users

Controller. Verified is the controller in respect of the processing of your personal information covered by this Privacy Policy for purposes of European data protection legislation (i.e., the EU GDPR and the so-called 'UK GDPR' (collectively, the "GDPR"). See the 'How to contact us' section above for our contact details.

- Right of information – You have the right to obtain information about how and on what basis your personal information is processed and a copy of these information.
- Your right of access - You have the right to ask us for copies of your personal Information.
- Your right to rectification - You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
- Your right to erasure - You have the right to ask us to erase your personal Information in certain circumstances.
- Your right to restriction of processing - You have the right to ask us to restrict the processing of your information in certain circumstances.
- Your right to object to processing - You have the right to object to the processing of your personal information in certain circumstances. For example, you have the right to object to our reliance on our legitimate interests as the basis of our processing of your personal information in certain circumstances.
- Your right to data portability - You have the right to ask that we transfer the information you gave us to another organisation, or to you, in certain circumstances.
- Your right to withdraw consent - You have the right to withdraw your consent at any time where we rely on your consent to process your personal information.
- Cross-Border Data Transfer - You can obtain a copy of or access safeguards under which your personal information is transferred outside of Europe.
- Direct marketing - If your personal information is processed for direct marketing purposes, you have the right to object at any time to the processing of personal information concerning you for such marketing. In this case your personal information will no longer be processed for such purposes by us.

Personal information we collect

Information you provide to us.

General

Personal information you may provide to us through any of the Services includes:

- **Contact data**, such as your first and last name, salutation, email address, billing and mailing addresses, professional title and company name, and phone number.
- **Communications data** based on our exchanges with you, including when you contact us in relation to the Services.
- **Marketing data**, such as your preferences for receiving our marketing communications and details about your engagement with them.

Digital ID Service

In addition to the personal information identified in the “General” section, above, personal information you may provide to us through the Digital ID Service may also include:

- **Credentials**, such as the username and password that you may set to establish an online account on the Verified Web Wallet.
- **Identity data**, such as your name, email address, telephone number, government-issued identifier data, and any other personal information you may verify with an Issuer or otherwise share with the Verified Web Wallet.
- **Transactional data**, such as information regarding the categories of identity data you share with the Verified Web Wallet from Issuers and that you share through the Verified Web Wallet with Relying Parties.

Verified Email Service

In addition to the personal information identified in the “General” section, above, personal information you may provide to us through the Verified Email Service includes:

- **Credentials**, such as the username and password that you may set to establish an online account on the Verified Web Wallet.
- **Email data**, such as the contents of your email inbox, including metadata from emails you send and receive and the contents of your messages. ***Due to constraints of the Gmail and Outlook platforms, it is not currently feasible for Verified to offer the Verified Email Service without requesting access to the contents of your email inbox. However, please note that although Verified has the ability to access the contents of your email messages, Verified will never do so unless required for legal, safety or security reasons.***

Third-party sources. We may combine personal information we receive from you with personal information we obtain from other sources, such as:

- **Issuers**, which may provide identity data to your Verified Web Wallet with your consent.
- **Users of the Verified Email Service.** We may obtain personal information about you from a user of the Verified Email Service when you send that user an email.
- **Third-party services**, such as social media services, that you use to log into, or otherwise link to, your Verified Web Wallet. This data may include your username, profile picture and other information associated with your account on that third-party service that is made available to us

based on your account settings on that service.

Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Verified Web Wallet and Site, our communications, such as:

- **Device data**, such as your computer or mobile device's operating system type and version, manufacturer and model, browser type, screen resolution, RAM and disk size, CPU usage, device type (e.g., phone, tablet), IP address, unique identifiers (including identifiers used for advertising purposes), language settings, mobile device carrier, radio/network information (e.g., Wi-Fi, LTE, 3G), and general location information such as city, state or geographic area.
- **Online activity data**, such as pages or screens you viewed, how long you spent on a page or screen, the website you visited before browsing to the Site, navigation paths between pages or screens, information about your activity on a page or screen, access times and duration of access, and whether you have opened our emails or clicked links within them.
- **Location data**, such as city, state or region from which you accessed the Verified Web Wallet or Site or location data derived from your IP address.
- **Communication interaction data** such as your interactions with our email or other communications (e.g., whether you open and/or forward emails) – we may do this through use of pixel tags (which are also known as clear GIFs), which may be embedded invisibly in our emails.

Cookies and similar technologies. Some of the automatic collection described above is facilitated by the following technologies:

- **Cookies**, which are small text files that websites store on user devices and that allow web servers to record users' web browsing activities and remember their submissions, preferences, and login status as they navigate a site. Cookies used on our sites include both "session cookies" that are deleted when a session ends, "persistent cookies" that remain longer, "first party" cookies that we place and "third party" cookies that our third-party business partners and service providers place.
- **Local storage technologies**, like HTML5, that provide cookie-equivalent functionality but can store larger amounts of data on your device outside of your browser in connection with specific applications.
- **Session-replay technologies**, such as those provided by Sentry, that employ software code to record users' interactions with the Services in a manner that allows us to watch video replays of those user sessions. The replays include users' clicks, mobile app touches, mouse movements, scrolls and keystrokes/key touches during those sessions. These replays help us diagnose usability problems and identify areas for improvement. You can learn more about Sentry at <https://sentry.io/privacy/>.
- **Web beacons**, also known as pixel tags or clear GIFs, which are used to demonstrate that a webpage or email was accessed or opened, or that certain content was viewed or clicked.

How we use your personal information

Subject to the [Google restricted scopes data](#) section, below, which (notwithstanding anything to the contrary herein) governs our use of Google restricted scopes data in connection with the Verified Email Service, we may use your personal information for the following purposes or as otherwise described at the time of collection:

Service delivery and operations. We may use your personal information to:

- Provide and operate the Services, including enabling you to share information verified by Issuers and other personal information with Relying Parties (with respect to users of the Digital ID Service) and to verify the identity of email senders and to send emails on behalf of our users to unverified senders (with respect to users of the Verified Email Service);
- personalize the service, including remembering your selections and preferences as you navigate the Services;
- establish and maintain your Verified Web Wallet;
- enable security features of the Services, such as by using cookies and other tracking technologies to remember devices from which you have previously logged in and by sending you security codes via email or SMS;
- communicate with you about the Services, including by sending service-related announcements, updates, security alerts, and support and administrative messages;
- provide support for the Services, and respond to your requests, questions and feedback.

Research and development and analytics. We may use your personal information for research and development and analytics purposes, including to analyze and improve the Services and our business and to understand user activity on the Services. For example, we use Google Analytics for this purpose. You can learn more about Google Analytics and how to prevent the use of Google Analytics relating to your use of the Services here: <https://tools.google.com/dlpage/gaoptout?hl=en>. As part of these activities, we may create aggregated, de-identified or other anonymous data from personal information we collect. We may use this anonymous data and share it with third parties for our lawful business purposes, including to analyze and improve the Services and promote our business, and will not attempt to reidentify any such data.

Marketing and advertising. If you are a user of the Verified Web Wallet or the Site, we and our service providers may collect and use your name, email address and other contact details for our marketing purposes, including to send you direct marketing communications. You may opt-out of our marketing communications as described in the [Opt-out of marketing](#) section below. We may also use your personal information for interest-based advertising. Our third-party advertising partners may use cookies and similar technologies to collect information about your interaction (including the data described in the [automatic data collection](#) section above) with the Services, our communications and other online services over time, and use that information to serve online ads that they think will interest you. This is called interest-based advertising. We may also share information about our users with these companies to facilitate interest-based advertising to those or similar users on other online platforms. You can learn more about your choices for limiting interest-based advertising in the [Your choices](#) section, below.

Compliance and protection. We may use your personal information to:

- comply with applicable laws, lawful requests, and legal process, such as to respond to subpoenas, investigations or requests from government authorities;
- protect our, your or others' rights, privacy, safety or property (including by making and defending legal claims);
- audit our internal processes for compliance with legal and contractual requirements or our internal policies;
- enforce the terms and conditions that govern the Services; and

- prevent, identify, investigate and deter fraudulent, harmful, unauthorized, unethical or illegal activity, including cyberattacks and identity theft.

Cookies and similar technologies. In addition to the other uses included in this section, we may use the [Cookies and similar technologies](#) described above for the following purposes:

- **Technical operation.** To allow the technical operation of the Services, such as by remembering your selections and preferences as you navigate the site.
- **Functionality.** To enhance the performance and functionality of our services.
- **Advertising.** To help our third-party advertising partners collect information about how you use the Services and other online services over time, which they use to show you ads on other online services they believe will interest you and measure how the ads perform.
- **Analytics.** To help us understand user activity on the Services, including which pages are most and least visited and how visitors move around the Services, as well as user interactions with our emails. For example, we use Google Analytics for this purpose. You can learn more about Google Analytics and how to prevent the use of Google Analytics relating to your use of our sites here: <https://tools.google.com/dlpage/gaoptout?hl=en>.

With your consent. In some cases, we may specifically ask for your consent to collect, use or share your personal information, such as when required by law.

How we share your personal information

Subject to the [Google restricted scopes data](#) section, below, which (notwithstanding anything to the contrary herein) governs our use of Google restricted scopes data in connection with the Verified Email Service, we may share your personal information with the following parties and as otherwise described in this Privacy Policy or at the time of collection.

Affiliates. Our corporate parent, subsidiaries, and affiliates.

Service providers/vendors. Third parties that provide services on our behalf or help us operate the Services or our business (such as hosting, information technology, customer support, email delivery, marketing, consumer research and website analytics).

Relying Parties and other third parties designated by you. If you are a user of the Digital ID Service, we may share your personal information with Relying Parties and any other third parties where you have instructed us or provided your consent to do so. For example, you can see which categories of personal information a Relying Party requests from you and you can choose which such categories of personal information you would like to share with that Relying Party.

Linked third-party platforms. If you log into the Verified Web Wallet with, or otherwise link the Verified Web Wallet to, a social media or other third-party service, we may share your personal information with that third-party service. For example, for users of the Verified Email Service, as the Verified Email Service is connected through your email provider, we may share your personal information with your email provider. The third party's use of the shared information will be governed by its own privacy policy and the settings associated with your account with such third-party service. Verified is not responsible for any use of your information by any such third-party platform.

Professional advisors. Professional advisors, such as lawyers, auditors, bankers and insurers, where necessary in the course of the professional services that they render to us.

Authorities and others. Law enforcement, government authorities, and private parties, as we believe in

good faith to be necessary or appropriate for the [Compliance and protection purposes](#) described above.

Business transferees. We may disclose personal information in the context of actual or prospective business transactions (e.g., investments in Verified, financing of Verified, public stock offerings, or the sale, transfer or merger of all or part of our business, assets or shares), for example, we may need to share certain personal information with prospective counterparties and their advisers. We may also disclose your personal information to an acquirer, successor, or assignee of Verified as part of any merger, acquisition, sale of assets, or similar transaction, and/or in the event of an insolvency, bankruptcy, or receivership in which personal information is transferred to one or more third parties as one of our business assets.

With your consent. We may share your personal information with any third parties where you have consented to, or directed us to engage in, such sharing.

Google restricted scopes data (applicable only to Verified Email Service)

The Verified Email Service integrates with Gmail. Verified may request the ability to access, read, write, and modify metadata, headers, Gmail message bodies (including attachments) and settings (“**Restricted Scopes Data**”). Notwithstanding anything else in this Privacy Policy, if you provide the Verified Email Service access to Restricted Scopes Data, Verified Email Service’s use of that Restricted Scopes Data will be subject to these additional restrictions:

- The Verified Email Service will only access, use, read, write, or modify Restricted Scopes Data to provide the Verified Email Service, including to verify the identity of those who email you and to send emails on your behalf to unverified senders, and will not transfer this Restricted Scopes Data to others unless doing so is necessary to provide and improve these features, comply with applicable law, or as part of a merger, acquisition, or sale of assets. ***Please note that although Verified must request the ability to access Gmail message bodies in order to integrate the Verified Email Service with Gmail, Verified will never access Gmail message bodies unless required for legal, safety or security reasons.***
- The Verified Email Service will not use Restricted Scopes Data for serving advertisements.
- The Verified Email Service will not allow humans to read Restricted Scopes Data unless (i) we have your affirmative agreement for specific messages, (ii) doing so is necessary for security purposes such as investigating abuse, to comply with applicable law, or (iii) doing so is necessary for the Verified Email Service’s internal operations and the data have been aggregated and anonymized.

Please see our [Google API Policy](#) for further information.

Your choices

In this section, we describe the rights and choices available to all users. Users who are located in Europe can find additional information about their rights below.

Access or update your information. If you have registered for an account with us, you may review and update certain account information by logging into the account.

Opt-out of communications. You may opt-out of marketing-related emails by following the opt-out or

unsubscribe instructions at the bottom of the email, or by [contacting us](#). Please note that if you choose to opt-out of marketing-related emails, you may continue to receive service-related and other non-marketing emails.

If you receive text messages from us, you may opt out of receiving further text messages from us by replying STOP to our message.

Cookies. Most browsers let you remove or reject cookies. To do this, follow the instructions in your browser settings. Many browsers accept cookies by default until you change your settings. Please note that if you set your browser to disable cookies, the Services may not work properly. For more information about cookies, including how to see what cookies have been set on your browser and how to manage and delete them, visit www.allaboutcookies.org. You can also configure your device to prevent images from loading to prevent web beacons from functioning.

Blocking images/clear gifs: Most browsers and devices allow you to configure your device to prevent images from loading. To do this, follow the instructions in your particular browser or device settings.

Do Not Track. Some Internet browsers may be configured to send “Do Not Track” signals to the online services that you visit. We currently do not respond to “Do Not Track” signals. To find out more about “Do Not Track,” please visit <http://www.allaboutdnt.com>.

Declining to provide information. We need to collect personal information to provide certain services. If you do not provide the information we identify as required or mandatory, we may not be able to provide those services.

Advertising choices. You may be able to limit use of your information for interest-based advertising through the following settings/options/tools:

- **Browser settings.** Changing your internet web browser settings to block third-party cookies.
- **Privacy browsers/plugin-ins.** Using privacy browsers and/or ad-blocking browser plug-ins that let you block tracking technologies.
- **Platform settings.** Google and Facebook offer opt-out features that let you opt-out of use of your information for interest-based advertising. You may be able to exercise that option at the following websites:
 - Google: <https://adssettings.google.com/>
 - Facebook: <https://www.facebook.com/about/ads>
- **Ad industry tools.** Opting out of interest-based ads from companies that participate in the following industry opt-out programs:
 - Network Advertising Initiative: http://www.networkadvertising.org/managing/opt_out.asp
 - Digital Advertising Alliance: optout.aboutads.info.

Platform settings. As noted above, you may be able to prevent the use of Google Analytics relating to your use of the Services here: <https://tools.google.com/dlpage/gaoptout?hl=en>.

Linked third-party platforms. If you are a user of the Verified Email Service, as the Verified Email Service is connected through your email provider, you may be able to use your settings in your account with that platform to limit the information we receive from it. If you revoke our ability to access information from your email provider, that choice will not apply to information that we have already received from that third party.

Other sites and services

The Services may contain links to websites, mobile applications, and other online services operated by third parties. In addition, our content may be integrated into web pages or other online services that are not associated with us. These links and integrations are not an endorsement of, or representation that we are affiliated with, any third party. We do not control websites, mobile applications or online services operated by third parties, and we are not responsible for their actions. We encourage you to read the privacy policies of the other websites, mobile applications and online services you use.

Security

We employ technical, organizational and physical safeguards designed to protect the personal information we collect. However, security risk is inherent in all internet and information technologies and we cannot guarantee the security of your personal information.

International data transfer

We are headquartered in the United States and may use service providers that operate in other countries. Your personal information may be transferred to the United States or other locations where privacy laws may not be as protective as those in your state, province, or country.

Users in Europe should read the important information provided below about transfer of personal information outside of Europe.

Children

The Services are not intended for use by anyone under 18 years of age. If you are a parent or guardian of a child from whom you believe we have collected personal information in a manner prohibited by law, please [contact us](#). If we learn that we have collected personal information through the Services from a child without the consent of the child's parent or guardian as required by law, we will comply with applicable legal requirements to delete the information.

Changes to this Privacy Policy

We reserve the right to modify this Privacy Policy at any time. If we make material changes to this Privacy Policy, we will notify you by updating the date of this Privacy Policy and posting it on the Services or other appropriate means. Any modifications to this Privacy Policy will be effective upon our posting the modified version (or as otherwise indicated at the time of posting). In all cases, your use of the Services after the effective date of any modified Privacy Policy indicates your acknowledging that the modified Privacy Policy applies to your interactions with the Services and our business.

How to contact us

- **Email:** Contact@Verified.Inc
- **Phone:** +1 (202) 831-7415

Notice to European users

Where this Notice to European users applies. The information provided in this “Notice to European users” section applies only to individuals in the United Kingdom and the European Economic Area (i.e., “Europe” as defined at the top of this Privacy Policy).

Personal information. References to “personal information” in this Privacy Policy should be understood to include a reference to “personal data” (as defined in the GDPR).

Controller. Verified is the controller in respect of the processing of your personal information covered by this Privacy Policy for purposes of European data protection legislation (i.e., the EU GDPR and the so-called ‘UK GDPR’ (collectively, the “GDPR”). See the ‘How to contact us’ section above for our contact details.

Our GDPR Representatives. We have appointed the following representatives in Europe as required by the GDPR – you can also contact them directly should you wish:

Our Representative in the EU. Our EU representative appointed under the EU GDPR is Aidan McCarty. You can contact them:

- By email to: Contact@Verified.Inc

Our Representative in the UK. Our UK representative appointed under the UK GDPR is Aidan McCarty. You can contact them:

- By email to: Contact@Verified.Inc

Our legal bases for processing. The legal bases of our processing of your personal information as described in this Privacy Policy will depend on the type of personal information and the specific context in which we process it. However, the legal bases we typically rely on are set out in the table below. If you have questions about the legal basis of how we process your personal information, contact us at Contact@Verified.Inc.

Processing purpose	Categories of personal information involved	Legal basis
<i>Details regarding each processing purpose listed below are provided in the section above titled “How we use your personal information”</i>		

<ul style="list-style-type: none"> • For Service delivery: We need to process your personal information to operate the Service, including managing your account or transactions, responding to your requests or inquiries, providing you with access to content or information you requested, etc. 	<ul style="list-style-type: none"> • Contact data • Credentials • Identity data • Communications data • Transactional data • User-generated content data • Data from Third Party Services • Online activity data • Device data • Information we obtain from users of Verified Email Service • Email Data 	<p>Processing is necessary to perform the contract governing our provision of our Service or to take steps that you request prior to signing up for the Service.</p>
<ul style="list-style-type: none"> • For research and development: We may use your personal information for research and development purposes, including to analyze and improve the Service and our business. 	<ul style="list-style-type: none"> • Any and all data types relevant in the circumstances 	<p>These activities constitute our legitimate interests. We do not use your personal information for these activities where our interests are overridden by the impact on you.</p>

<p>We may need to process your personal information for additional purposes, such as:</p> <ul style="list-style-type: none"> • To ensure access and maintenance of the Service, and to ensure their proper functioning • For compliance, fraud prevention and safety • For sharing your personal information with third parties as described in this Privacy Policy • To disclose your personal information to a prospective or actual purchaser or seller in the context of a merger, acquisition or other reorganization or sale of our business or assets • For the collection of statistical information about the use of the Service • To protect our interests as a company, for different purposes, such as: <ul style="list-style-type: none"> ○ Enforcement of the Terms of Service ○ Assess claims that any content violates the rights of third parties 	<ul style="list-style-type: none"> • Contact data • Credentials • Identity data • Communications data • Transactional data • User-generated content data • Data from Third Party Services • Online activity data • Device data 	<p>We rely on our legitimate interests to process your personal information when performing these processing activities. We do not use your personal information for these purposes where our interests are overridden by the impact on you.</p>
---	---	--

<ul style="list-style-type: none"> • For marketing and advertising purposes: We and our third-party advertising partners may collect and use your personal information for marketing and advertising purposes. 	<ul style="list-style-type: none"> • Contact data • Marketing data • Communication interaction data • Device data • Online activity data 	<p>Processing is based on your consent where that consent is required by applicable law. Where such consent is not required by applicable law, we process your personal information for these purposes based on our legitimate interests in promoting our business.</p>
<ul style="list-style-type: none"> • Compliance with legal obligations and protection purposes: We are subject to certain legal obligations that may oblige us to disclose your personal information to courts, law enforcement or regulatory authorities. 	<ul style="list-style-type: none"> • Any and all data types relevant in the circumstances 	<p>Processing is necessary to comply with our legal obligations.</p>
<p>Actions we take with your consent:</p> <ul style="list-style-type: none"> • Allowing third party ad partners and advertisers to use tracking technologies while you use the Service. 	<ul style="list-style-type: none"> • Any and all data types relevant in the circumstances 	<p>In these scenarios, the processing of the personal information you voluntarily provide to us is based on your consent. Where we rely on your consent you have the right to withdraw it any time in the manner indicated when you consent or in the services.</p>

Use for new purposes. We may use your personal information for reasons not described in this Privacy Policy where permitted by law and the reason is compatible with the purpose for which we collected it. If we need to use your personal information for an unrelated purpose, we will notify you and explain the applicable legal basis.

Retention. We apply a general rule of keeping personal information only for so long as is required to fulfill the purpose for which it was collected. However, in some circumstances, we will retain your personal information for longer periods of time. We will retain personal information for the following purposes: (i) as long as it is necessary and relevant for our operations, business needs and to provide the Service, e.g. so that we have an accurate record of your dealings with us in the event of any complaints or challenge; and (ii) in relation to personal information from closed Accounts to comply with applicable laws, prevent fraud, collect any fees owed, resolve disputes, troubleshoot problems, assist with any investigation, enforce the Service terms and take other actions as permitted by law.

No special categories of data. We ask that you not provide us with any sensitive personal information (e.g., information related to racial or ethnic origin, political opinions, religion or other beliefs, health, biometrics or genetic characteristics, criminal background or trade union membership) on or through the Service, or otherwise to us.

No Automated Decision-Making and Profiling. As part of the Services, we do not engage in automated decision-making and/or profiling, which produces legal or similarly significant effects.

Your rights. European data protection laws give you certain rights regarding your personal information. If you are located in Europe, you may ask us to take the following actions in relation to your personal information that we hold:

- Right of information – You have the right to obtain information about how and on what basis your personal information is processed and a copy of these information.
- Your right of access - You have the right to ask us for copies of your personal Information.
- Your right to rectification - You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
- Your right to erasure - You have the right to ask us to erase your personal Information in certain circumstances.
- Your right to restriction of processing - You have the right to ask us to restrict the processing of your information in certain circumstances.
- Your right to object to processing - You have the right to object to the processing of your personal information in certain circumstances. For example, you have the right to object to our reliance on our legitimate interests as the basis of our processing of your personal information in certain circumstances.
- Your right to data portability - You have the right to ask that we transfer the information you gave us to another organisation, or to you, in certain circumstances.
- Your right to withdraw consent - You have the right to withdraw your consent at any time where we rely on your consent to process your personal information.
- Cross-Border Data Transfer - You can obtain a copy of or access safeguards under which your personal information is transferred outside of Europe.
- Direct marketing - If your personal information is processed for direct marketing purposes, you have the right to object at any time to the processing of personal information concerning you for such marketing. In this case your personal information will no longer be processed for such purposes by us.

Exercising These Rights. You may submit these requests by email to Contact@Verified.Inc or our postal address provided above. We reserve the right to charge a fee where permitted by law. We may request specific information from you to help us confirm your identity and process your request. Whether or not we are required to fulfill any request you make will depend on a number of factors (e.g., why and how we are processing your personal information), if we reject any request you may make (whether in whole or in part) we will let you know our grounds for doing so at the time, subject to any legal restrictions.

Your Right to Lodge a Complaint with your Supervisory Authority. In addition to your rights outlined above, if you are not satisfied with our response to a request you make, or how we process your personal information, you can make a complaint to the data protection regulator in your habitual place of residence.

- For users in the European Economic Area – the contact information for the data protection regulator in your place of residence can be found here: https://edpb.europa.eu/about-edpb/board/members_en
- For users in the UK – the contact information for the UK data protection regulator is below:

The Information Commissioner's Office
Water Lane, Wycliffe House
Wilmslow - Cheshire SK9 5AF
Tel. +44 303 123 1113
Website: <https://ico.org.uk/make-a-complaint/>

Data Processing outside Europe. We are a U.S.-based company and many of our service providers, advisers, partners or other recipients of data are also based in the U.S. We may share your personal information with these third parties who may be based outside of Europe. In such circumstances, those parties' processing of your personal information will involve a transfer of your personal information outside of Europe where privacy laws may not be as protective as those in your state, province, or country.

You may contact us if you want further information on the specific mechanism used by us when transferring your personal information out of Europe. You may have the right to receive a copy of the appropriate safeguards under which your personal information is transferred by contacting us at Contact@Verified.Inc.