

Humanyze – Privacy Policy (this “policy”)

Last Updated: May 1, 2024

Section 1: Where we are data controller

Sociometric Solutions, Inc., trading as Humanyze, (“Humanyze” or “we” or “us”) are committed to protecting and respecting your privacy. We are registered in the state of Delaware, United States of America under file number 5047652 and have our registered office at 160 Greentree Drive, Suite 101, Dover, Delaware, 19904 USA and our primary business location at PO Box 961740, Boston, MA 02196, USA. If you have any questions regarding this policy, you may contact us at info@humanyze.com.

We are also a participant in the Data Privacy Framework, as operated by the US Department of Commerce. Details of our compliance with the Data Privacy Framework can be found in Section 3 of this policy.

As used in this policy (a) “GDPR” means the General Data Protection Regulation (EU) 2016/679; (b) “UK Data Protection Laws” means the UK GDPR and the UK’s Data Protection Act 2018 (“UK DPA 2018”); (c) “UK GDPR” means the UK equivalent of the GDPR, as defined in section 3(10) (and as supplemented by section 205(4)) of the UK DPA 2018; (d) “European Data Protection Laws” means the GDPR and/or UK Data Protection Laws, in each case to the extent applicable; and (e) “controller” and “processor” shall have the meanings set out in the European Data Protection Laws.

For the purpose of the European Data Protection Laws, we are the data controller of the data set out in this Section 1, and we are data processor of data we receive from your employer as set out in Section 2 below. Please read this policy carefully to understand our practices regarding the processing of your personal data. For the purposes of this policy, “personal data” refers to any information relating to an identified or identifiable natural person.

If an organization with which you are associated, such as your employer, (an “Organization”) signs up to use our services, we may receive information about you in connection with our provision of such services to your Organization including the information set out in Section 2 of this policy. To the extent we process that information solely in order to provide such services to your Organization, we will act as a processor on behalf of your Organization in respect of that information, which means: we will handle that information solely at the direction of your Organization; and your Organization (and not us) is responsible for obtaining all necessary consents and providing you with all requisite information as required by applicable law.

By using our website, services, applications, products and content, and our Humanyze Elements™ software (collectively, the “Platform”), you accept the practices described in this policy.

As used in this policy, the terms “using” and “processing” information include using Cookies (as defined below) on a computer, subjecting the information to statistical or other analysis and using or handling information in any way, including, but not limited to collecting, storing, evaluating, modifying, deleting, using, combining, disclosing and transferring information within Humanyze or among our affiliates within the United States or internationally.

1. The types of personal data we use

We may collect and use the following information about you:

- **Information you give us.** You may give us information about you by using our Platform or by corresponding with us by e-mail or otherwise such as your name, company name, title, country, phone number, number of employees at your company, email address, how you

learned about Humanyze, and other information related to your request or that you choose to share with us. This includes information you provide when you register on the Platform, such as your user profile. Additionally, our service provider that is responsible for billing and payment processing services (the “Payment Services Provider”) may collect your billing and credit card information from you directly.

- **Information we collect about you.** We automatically collect certain data from you when you use the Platform, including IP address or other unique device identifiers, Cookies (as defined below) and information regarding your use of our Platform such as log of site visits and page views.
- **Data provided by your Organization, such as your employer.** Data that we obtain from our customers through use of the services, as more fully set out in Section 2.

2. Cookies

We use cookies and other similar technologies (e.g. web beacons, Flash cookies, etc.) (“Cookies”) to enhance your experience using the Platform. Cookies are small files which, when placed on your device, enable us to provide certain features and functionality.

We use the following Cookies:

- **Strictly necessary Cookies.** These are Cookies that are required for the operation of the Platform. They include, for example, Cookies that enable you to log into secure areas of the Platform.
- **Analytical/performance Cookies.** They allow us to recognise and count the number of visitors and to see how visitors move around the Platform when they are using it. This helps us to improve the way the Platform works, for example, by ensuring that users are finding what they are looking for easily.
- **Functionality Cookies.** These are used to recognise you when you return to the Platform. This enables us to personalise our content for you, greet you by name and remember your preferences (for example, your choice of language or region).

If for any reason you wish to not take advantage of Cookies, you may disable Cookies by changing the settings on your browser. However, if you do so, this may affect your enjoyment of the Platform. Unless you opt out of Cookies, to the extent permitted by applicable law we will assume you consent to the use of Cookies.

For the avoidance of doubt, the Platform uses third-party services (including to help analyze how users use the Platform). These third-party services may place cookies on your computer or mobile device. If you would like to disable "third party" cookies, you may be able to turn them off by going to the third party's website.

Here are links to the main third-party services we use:

Addtoany	BambooHR	Google	Sentry
Amplitude	Calendly	Hotter	Stripe
Automatic	CookiesYes	Marketo	

3. How we use your personal data

We will only use your information to the extent that the law allows us to do so. Legal bases for our processing your information may include (without limitation):

- where you have given consent to the processing, which consent may be withdrawn at any time without affecting the lawfulness of processing based on consent prior to withdrawal;
- where it is necessary to perform the contract we have entered into or are about to enter into with you (whether in relation to the provision of the Platform or otherwise);
- where it is necessary for us to comply with a legal obligation to which we are subject; and/or
- where it is necessary for the purposes of our legitimate interests, including to be responsive to you and to ensure the proper functioning of our Platform and organisation, and your interests or fundamental rights and freedoms do not override those legitimate interests.

We may also use the information you give us and other information we collect about you in the following ways:

- notify you about changes to our service;
- provide you with user support;
- enforce our terms, conditions and policies;
- communicate with you;
- improve and administer our services and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
- keep our services safe and secure;
- develop our services and conduct product development; and
- measure and understand the effectiveness of the advertising we serve to you and others.

In addition, it is in our legitimate interest to conduct research and as such we may pseudonymize data and process this pseudonymized data for research purposes.

4. How we share your personal data

We may share your personal data with selected third parties in or outside the European Economic Area (“EEA”) or United Kingdom (“UK”), including:

- our suppliers and subcontractors (including the Payment Services Provider) who help us run the Platform or provide other services related to the Platform, including providing credit card processing and fraud screening; and
- analytics providers that assist us in the improvement and optimisation of the Platform. Please note in particular that the Platform uses Google Analytics, including its data reporting features. Information collected by Google Analytics includes but is not limited to web metrics. For information on how Google Analytics collects and processes data, please see the site “How Google uses data when you use our partners' sites or apps”, currently located at

www.google.com/policies/privacy/partners/. For information on opting out of Google Analytics, we encourage you to visit Google's website, including its list of currently available opt-out options presently located at <https://tools.google.com/dlpage/gaoptout>.

We may share your information with law enforcement agencies, public authorities or other organisations if legally required to do so, or if we have a good faith belief that such use is reasonably necessary to:

- comply with legal obligation, process or request, including lawful requests by public authorities, such as to meet national security or law enforcement requirements;
- enforce our terms of service and other agreements, policies, and standards, including investigation of any potential violation thereof;
- detect, prevent or otherwise address security, fraud or technical issues; or
- protect the rights, property or safety of us, our users, a third party or the public as required or permitted by law (including exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction).

We may also disclose your information to:

- professional advisors, such as lawyers, auditors, bankers and insurers, where necessary in the course of the professional services that they render to us;
- third parties in the event that we sell or buy any business or assets, in which case we may disclose your data to the prospective seller or buyer of such business or assets;
- third parties if we sell, buy, merge or partner with other companies or businesses, or sell some or all of our assets. In such transactions, user information may be among the transferred assets; or
- our Corporate Affiliates. For purposes of this policy: "Corporate Affiliate" means any person or entity which directly or indirectly controls, is controlled by or is under common control with Humanyze, whether by ownership or otherwise; and "control" means possessing, directly or indirectly, the power to direct or cause the direction of the management, policies or operations of an entity, whether through ownership of fifty percent (50%) or more of the voting securities, by contract or otherwise.

5. Where we store your personal data

The information that we collect from you may be transferred to, and stored at, a destination outside of your country and the EEA or UK (as applicable), and particularly to the United States of America. It may also be processed by staff operating outside your country or the EEA or UK (as applicable) who work for us, for one of our suppliers or one of our business partners. By submitting your information, you agree to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your information is treated securely and in accordance with this policy.

Without limitation of the foregoing, you hereby expressly grant consent to Humanyze to: (a) process and disclose your information in accordance with this policy; (b) transfer your information throughout the world, including to the United States or other countries that do not ensure adequate protection for personal data (as determined by the European Commission or the UK Information Commissioner's Office, as applicable, each, an "Inadequate Jurisdiction") and/or countries that may not have laws of

general applicability regulating the use and transfer of such information; and (c) disclose your information to comply with lawful requests by public authorities, including to meet national security or law enforcement requirements. To the extent required by applicable law: whenever we transfer your personal data to third parties (as described in this policy) located in an Inadequate Jurisdiction, we ensure a similar degree of protection is afforded to it; we may use specific contracts approved by the European Commission (accessible at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj) or the UK Information Commissioner's Office (accessible at <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/>), as applicable, which give personal data the same protection it has in the EEA or UK (as applicable); and if we rely on another basis to transfer your personal data to an Inadequate Jurisdiction, we will keep you updated or contact you if required.

For specific information regarding how we handle personal data received from the EEA, Switzerland, or the UK to the United States, please see Section 3 below.

6. The security of your personal data

We want your personal data to remain secure. We strive to provide transmission of your personal data from your computer or mobile device to our servers through techniques that are consistent with commercially reasonable standards and to employ administrative, physical, and electronic measures designed to protect your personal data from unauthorized access.

Notwithstanding the above, you should be aware that there is always some risk involved in transmitting information over the Internet. There is also some risk that others could find a way to thwart our security systems. As a result, while we strive to protect your personal data, we cannot ensure or warrant the security or privacy of any information you transmit to us, and you do so at your own risk.

7. Data retention

We will only retain your personal data for as long as necessary to fulfill the purposes for which we collected it or as otherwise permitted by applicable law.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of that personal data, the potential risk of harm from unauthorized use or disclosure, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

8. Your rights

- **Data rights.** Under certain circumstances and in compliance with applicable laws: you may have the right to access personal data we hold about you, to rectify any personal data held about you that is inaccurate, to request the deletion of personal data held about you, to request the restriction of processing of your personal data, object to the processing of your personal data, or lodge a complaint with your relevant supervisory authority. If applicable, you can exercise your rights by contacting us at info@humanalyze.com.
- **Complaints.** In the event that you wish to make a complaint about how we process your personal data, please contact us in the first instance at info@humanalyze.com and we will endeavour to deal with your request as soon as possible. This is without prejudice to your right to launch a claim with your data protection authority (if applicable).
- **Do Not Track.** We take no action in response to automated Do Not Track requests. However,

if you wish to stop such tracking, please contact us with your request at info@humanyze.com.

9. Changes

Any changes we may make to this policy in the future will be posted on this page. Please check back frequently to see any updates or changes to this policy. If we make any material changes to this policy, we will post the updated policy here and notify our users by posting the updated policy at humanyze.com.

10. Contact

Questions, comments and requests regarding this policy are welcomed and should be addressed to info@humanyze.com.

11. Children

We are committed to protecting the privacy of children. The Platform is not designed for or directed to children under the age of 13. We do not collect information from any person we actually know is under the age of 13.

Section 2: Where we are data processor

Our customers, usually your employer, engage Humanyze to provide individual-level and management-level feedback to better understand the interactions and communications of their workforce. As part of our contract with our customers, we may process data on their behalf such as pseudonymous email logs (no content is shared with us), pseudonymized instant messaging logs (no content is shared with us), pseudonymized calendar events, and limited pseudonymized HR data such as gender and organisational role or job title.

Our customers are the data controller of this data and questions about their data handling processes should in the first instance be addressed to them. At all times, we act as a service provider to our customers, and process data on their behalf.

Section 3: Data Privacy Framework (DPF)

Humanyze complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Humanyze has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Humanyze has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. The EU-U.S. DPF Principles and Swiss-U.S. DPF Principles shall be referred to collectively herein as the "Principles".

If there is any conflict between the terms in this policy and the Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/> and <https://www.dataprivacyframework.gov/list>. Humanyze commits to subject all personal data received from the European Union, the United Kingdom (and Gibraltar), and Switzerland under the DPF to the Principles.

For the categories of personal data collected by Humanyze, please see Section 1, Subsections 1 and 2 and Section 2 of this policy; for the purposes for which Humanyze collects and uses personal data, please see Section 1, Subsections 2 and 3 and Section 2 of this policy; for the categories of third parties to which Humanyze discloses personal data and our purposes for doing so, please see Section 1, Subsections 3 and 4 of this policy; and for more information regarding your right to access your personal data and your choices and the means Humanyze offers you for limiting the use and disclosure of your personal data, please see Section 1, Subsection 8 of this policy.

With respect to the categories of data set out in Section 2 of this policy that Humanyze receives under this Section 3: Humanyze collects and uses such data only on the instructions of the applicable third-party controller and will work with the applicable third-party controller to facilitate your data subject rights. Notwithstanding any other provision of this policy, and for the avoidance of doubt, with respect to personal data processed by Humanyze solely on behalf of a third-party controller, the provisions of this policy specific to such data, including Section 2, continue to apply in accordance with the DPF, but may be limited to working with the respective controller, given our role as a processor.

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, Humanyze commits to resolve complaints about our collection or use of your personal data transferred to the U.S. pursuant to the EU-U.S. DPF and the UK extension to the EU-U.S. DPF, and the Swiss-U.S. DPF. EU, UK, and Swiss individuals with inquiries or complaints should first contact Humanyze at info@humanyze.com.

Humanyze has further committed to refer unresolved DPF Principles-related complaints to a U.S.-based independent dispute resolution mechanism, BBB NATIONAL PROGRAMS. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit www.bbbprograms.org/dpf-complaints for more information and to file a complaint. This service is provided free of charge to you.

If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See <https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf>.

Before Humanyze discloses your personal data to a third party, we will require that such third party provide the same level of privacy protection as is required by the Data Privacy Framework. Humanyze remains liable under the Data Privacy Framework if third-party agents that it retains to process your personal data on our behalf process your personal data in a manner inconsistent with the Data Privacy Framework, unless Humanyze can prove that it is not responsible for the event giving rise to the damage. For more information regarding Humanyze's disclosure of personal data to third parties, please see Section 1, Subsection 4 of this policy.

Adherence by Humanyze to the Principles and the provisions set forth in this Section 3 may be limited (a) to the extent necessary to comply with a court order or meet public interest, law enforcement, or national security requirements, including where statute or government regulation create conflicting obligations; (b) by statute, court order, or government regulation that creates explicit authorizations; or (c) if the effect of the European Data Protection Laws, to the extent applicable, is to allow exceptions or derogations, under the conditions set out therein, provided that such exceptions or derogations are applied in comparable contexts.

In certain circumstances, Humanyze may be required to disclose your personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. Finally, note that the Federal Trade Commission has jurisdiction over Humanyze's compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.