Humanyze - Privacy Policy

Last Updated: December 21, 2017

Section 1: Where we are data controller

Sociometric Solutions, Inc., trading as Humanyze, ("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 18 Tremont Street, Suite 605, Boston, Massachusetts 02108 USA. Our data protection officer can be contacted at info@humanyze.com.

We are also a participant in the EU-US Privacy Shield Framework, as operated by the US Department of Commerce ("Privacy Shield"). Details of our compliance with the Privacy Shield can be found at https://www.privacyshield.gov/.

For the purpose of EU data protection laws, we are the data controller of the data set out in this Section 1, and we are data processor of data from your employer – including the Device data – as set out in Section 2 below. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it.

By using our website, services, applications, products and content, our sensing devices (Sociometric® Badges and Bluetooth Low Energy beacons (together, the "Devices")) and our Humanyze Elements™ software (collectively, the "Platform"), you accept the practices described in this policy.

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. This includes information you provide when you register on the Platform, such as your user profile, name, and email address.

- **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.

- **Device Data and other data provided by your employer.** Data that we obtain from our customers through use of the services, as more fully set out in Section 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, we will assume you consent to the use of Cookies.

How we use your personal data

We will use the information in the following ways:

- As it is in our legitimate interests to be responsive to you and to ensure the proper functioning of our Platform and organisation, we may use information you give us and information we collect about you to:
    - 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;
    - for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
    - keep our services safe and secure;
    - and develop our services and conduct product development;
- It is in our legitimate interest to conduct research and as such we may anonymise Device data and process this anonymised data for research purposes.

How we share your personal data

We may share your personal data with selected third parties in or outside the European Economic Area ("EEA"), including:

- our suppliers and subcontractors who help us run the Platform; and
- analytics providers that assist us in the improvement and optimisation of the Platform.

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;

- 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).

- Humanyze reserves the right to share your Information to respond to authorized information requests of governmental authorities or where required by law. Humanyze reserves the right to use or disclose personal information provided to Humanyze in response to a lawful request by public authorities, including to meet national security or law enforcement requirements, or if Humanyze reasonably believes that use or disclosure is necessary to protect Humanyze's rights and/or to comply with a judicial proceeding, court order, or legal process. In exceptionally rare circumstances where national, state, or company security is at issue, Humanyze reserves the right to share our entire database of visitors and clients with appropriate government authorities.

We may also disclose your information to 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; or

- 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.

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 European Economic Area ("**EEA**"), and particularly to the United States of America. It may also be processed by staff operating outside your country or the EEA 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.

The security of your personal data

Unfortunately, the transmission of information via the internet is not completely secure. Your data is secured during transmission with industry standard encryption techniques (TLS v 1.2 or greater), and it is secured at rest with AES 256 encryption and "least privilege" user access controls. Your data resides in Amazon Elastic Compute Cloud (EC2) servers and is continuously backed up. Only Humanyze authorised personnel can access these servers. Our system is actively monitored for indicators of intrusion or abnormal activity, and all activities are logged. Although we will do our best to protect your personal data, we cannot guarantee the security of your information transmitted through the Platform; any transmission is at your own risk.

Data retention

After you terminate the use of our services, we will retain your information as follows and as required under applicable laws:

- Information you give to us: for up to 30 days.

- Information we collect about you: for up to 30 days.

After you have terminated your use of our services, we may store your information in an aggregated and anonymised format. After the data has been anonymised and aggregated, we may use the data for research purposes.

Your rights

- **Data rights.** You have the right to access personal data we hold about you, to rectify any personal data held about you that is inaccurate and to request the deletion of personal data held about you. You can exercise your rights by contacting us at help@humanyze.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 help@humanyze.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.

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 Privacy Policy, we will post the updated Privacy Policy here and notify our users.

Contact

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

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:

- **Device Data.** The Devices gather the following data: (i) speech characteristics including volume, pitch, and turn-taking; (ii) body movement along x, y, and z coordinates; (iii) and Bluetooth signal strength which helps us understand proximity to others wearing a Device and to other Bluetooth-enabled beacons. The information that each Device collects from another Device is limited to the Device's unique identifier, the approximate distance between the Devices, the length of time during which the Devices were in proximity to one another, and the date and time of the interaction. The Device does not record speech or conversational content.

- **Data Provided by Customer:** In some instances, our customers may share with us additional data such as anonymised email logs (no content is shared with us), anonymised instant messaging logs (no content is shared with us), anonymised calendar events, and limited anonymised 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.

Privacy Shield Statement

Sociometric Solutions, Inc., trading as Humanyze, ("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 18 Tremont Street, Suite 605, Boston, Massachusetts 02108 USA.

We recognise that Europe has established strict protections for the processing of European personal data, including the requirements to provide adequate protection for such data when transferred outside the European Economic Area ("EEA"). To provide adequate protection for all personal data received from the EEA, we have elected to self-certify to the EU-US Privacy Shield Framework, as operated by the US Department of Commerce ("Privacy Shield").

Humanyze complies with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union members countries. Humanyze has certified that it adheres to the Privacy Shield Principles. If there is any conflict between the policies in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/

A full list of companies who have self-certified with the Privacy Shield is available at https://www.privacyshield.gov/.

1. **Our commitment to the Principles**

We commit to comply with the EU-US Privacy Shield Principles (the "Principles") with respect to all personal data that we receive from the EEA. Individuals whose personal data is received by us from other non-EEA jurisdictions do not have the rights set out in this statement.

2. **Types of personal data collected**

The types of personal data collected are set out in the section titled "*The types of personal data we use*" in the Privacy Policy:

- **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. This includes information you provide when you register on the Platform, such as your user profile, name, and email address.

- **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.

- **Device Data and other data provided by your employer.** Data that we obtain from our customers through use of the services, as more fully set out in Section 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).

3. **The purposes for collection and use**

The purposes for collection and use are set out in the section titled "*How we use your personal data*" in the Privacy Policy:

- As it is in our legitimate interests to be responsive to you and to ensure the proper functioning of our Platform and organisation, we may use information you give us and information we collect about you to:
    - 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;
    - for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
    - keep our services safe and secure;
    - and develop our services and conduct product development;
- It is in our legitimate interest to conduct research and as such we may anonymise Device data and process this anonymised data for research purposes.

4. **Types of third parties to whom we disclose personal data and purposes for disclosure**

The types of third parties to whom we may disclose personal data is set out in the section titled "*How we share your personal data*" in the Privacy Policy:

We may share your personal data with selected third parties in or outside the European Economic Area ("EEA"), including:

- our suppliers and subcontractors who help us run the Platform; and
- analytics providers that assist us in the improvement and optimisation of the Platform.

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;
- 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).
- Humanyze reserves the right to share your Information to respond to authorized information requests of governmental authorities or where required by law. Humanyze reserves the right to use or disclose personal information provided to Humanyze in response to a lawful request by public authorities, including to meet national security or law enforcement requirements, or if Humanyze reasonably believes that use or disclosure is necessary to protect Humanyze's rights and/or to comply with a judicial proceeding, court order, or legal process. In exceptionally rare circumstances where national, state, or company security is at issue, Humanyze reserves the right to share our entire database of visitors and clients with appropriate government authorities.

We may also disclose your information to 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; or
- 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.

5. **Choice**

If you do not wish us to pass your personal data to a third party who subsequently uses your data for its own purposes or if you wish to opt out from using our services, you may contact us via the details set out at "*Contact us"* section below.

6. **Accountability for onward transfer**

Where required by the Principles, we will enter into written agreements with third parties requiring them to provide the same level of protection that the Privacy Shield required and limiting their use of the data to the specified services provided on our behalf.

Under certain circumstances, we may remain liable for the acts of our third party agents or service providers who perform services on our behalf for their handling of EU personal data that we transfer to them.

7. **Security**

We maintain reasonable and appropriate measures to protect personal data from loss, misuse and unauthorised access, disclosure, alteration and destruction, taking into due account the risks involved in processing and the nature of the personal data.

8. **Data Integrity and Purpose Limitation**

We limit the collection, usage and retention of information to that which is relevant for the intended purposes for which it was collected, and takes reasonable steps to ensure that all data are reliable, accurate, complete and current.

9. **Access**

You have certain rights under the Principles to access the personal data about you that we process. To access such personal data, please make a request in writing to the contact details set out in "*Contact Us"* below. We will responds to your request in accordance with the Principles.

10. **FTC's investigatory and enforcement powers**

Our commitments under the Privacy Shield, and compliance with the Principles, are subject to the investigatory and enforcement powers of the US Federal Trade Commission.

11. **Complaints**

If you have any complaint regarding our compliance with the Principles, please contact us using the details set out at "*Contact Us"* below. We will respond to your complaint within 45 days.

12. **Independent dispute resolution body**

In compliance with the Privacy Shield Principles, Humanyze commits to resolve complaints about your privacy and our collection or use of your personal information. European Union individuals with inquiries or complaints regarding this privacy policy should first contact Humanyze at: help@humanyze.com.

Humanyze has further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit http://www.bbb.org/EU-privacy-shield/for-eu-consumers for more information and to file a complaint.

Under certain limited conditions you may invoke binding arbitration before the Privacy Shield Panel to be created by the U.S. Department of Commerce and the European Commission.

13. **Document revisions**

This Statement may be revised from time to time to reflect changes in data privacy laws, regulations and requirements. All revised Statements will be published here.

14. **Contact us**

If you have any questions about our adherence to the Principles or our participation in the Privacy Shield, please contact us at help@humanyze.com.