# Frequently Asked Security Questions

Last modified 17 January 2020 | For Public Use | security@energage.com

# About Energage

Energage helps you realize your workforce's full potential by building a stronger culture and connections across the organization. With higher employee engagement and intentional cultures, Energage customers are reducing turnover costs, increasing productivity, and improving teamwork.

Energage's CultureTech™ platform combines employee surveys, reliable insights, and expert guidance to transform your culture with an employee-centric approach. We apply our proprietary research, neuroscience, and patented insights to give you clear next steps to develop an employee-centric approach to success.

For more information on how Energage can help you build a winning workplace culture, please contact info@energage.com.

# Information Security at Energage

Energage is committed to protecting the confidentiality, integrity, and availability of your data. With this in mind, Energage has a dedicated Information Security Manager who owns and oversees Information Security at Energage.

Energage aligns its Information Security program with ISO 27001:2015 security best practices and guidelines, specifically:

1. The procurement, provisioning, maintenance, retirement, and reclamation of corporate computing resources,
2. All aspects of service development and operation related to security, privacy, access, reliability, and survivability,
3. Ongoing risk assessment, vulnerability management, incident response, and
4. Security-related human resources controls and personnel training.

## Notice to Massachusetts Residents

According to the 201 CMR 17.00 regulation, a Massachusetts resident's first name and last name or first initial and last name *in combination with* any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued, identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Because we only collect email addresses and demographic information, we are not subject to this set of standards.

For more information, please contact security@energage.com.

# Table of Contents

# 1. Information Privacy

For our full Privacy Policy, please visit https://www.energage.com/privacy.

## 1.1 What information is collected?

Energage customers will only provide, and Energage will only collect - personal information that is necessary for a stated purpose.

For example, certain areas and features of our Services may require you to complete a form or a registration (e.g., signing up to use our survey configuration tool, complete a survey, or using our software products).

- Registration: To register, a designated representative of our business entity customers (“Customers”) must provide us with their first name, last name, company name, email address, phone number, and select a password. We also may collect additional optional information, such as company profile information, employee counts and other information related to our offerings from Customers, however, you are not required to provide us with this information.
- Customers: In addition, if you make a purchase, we will also request that you provide your credit or debit card information and your billing address for credit card purchases or the appropriate billing information for invoicing.
- Use of Services: You may use some Services without registration. In these instances, you may be asked to provide demographic information (e.g., department of employment, status as a full or part-time employee, etc.) and comments which may indirectly identify you.
- Survey Participants: If you participate in a survey, you may be asked to provide certain personal information relating to your employment with a Customer and for certain demographic information. Our standard demographics include Hours (full-time/part-time), Tenure, Job Grade, Salary Band, and Age.  We also capture and report out based on organization structure (departments).

## 1.2 How is this information used?

If you are a Customer, we use any information collected:

- To provide our Services to you, to communicate with you about your use of our Services, to respond to your inquiries, to fulfill your orders, and for other customer service purposes.
- To tailor the content and information that we may send or display to you, to offer customization and personalized help and instructions, and to otherwise personalize your experiences while using our Services and interacting with our team.
- To contact you, including for marketing purposes. For example, we may use your information, such as your email address, to send you newsletters, or to otherwise contact you about products or information we think may interest you.
- To better understand how individuals access and use our Services, including to learn about their engagement levels and navigation paths, as well as user retention and drop-offs in our tools, and for other research and analytical purposes.
- To better understand how individuals use our Websites and tools, to learn how we might improve your experience, and to display ads relevant to you on sites across the Internet.

If you are a Survey Participant, we use this information as follows:

- Survey Completion: To complete surveys.
- Research, Data Analysis, Trending and Benchmarking: To provide aggregate insights to our Customers, to provide Customers with analysis and trending data relating to their peer firms and industries, to conduct research and to for benchmarking purposes.
- Coach Application Usage: To store and make available for retrieval, by managers and employees, information submitted within the applications.

- To Otherwise Provide the Services: To facilitate participation in other Energage Services.

We do not use personal information of Survey Participants to contact for marketing purposes. If demographic information is provided by the customer to Energage prior to employees taking the survey, the employees will have the ability to change their information and/or opt out of having their responses included in department level reports. Once the survey is completed, that responder's data becomes locked, however, they could still contact Energage to make changes.

All survey questions are optional, so employees don't have to provide any demographic information they are not comfortable with sharing.

If demographic/department data is provided/uploaded post-survey, then this is not available to be changed by the survey taker.

Employees are able to view a confidentiality statement prior to taking the survey.

## 1.3 With whom is this information shared?

We may share the information that we collect about you, including personal data, as follows:

- Service Providers. We may disclose your information to third-party vendors, service providers, contractors, or agents who perform actions or functions on our behalf. Examples of this include Google Analytics, FullStory, Microsoft Azure, and other tools necessary to carry out our business operations.
- Customers. If you are a Survey Participant, we may disclose your information in aggregate form to Customers for the purpose of providing such Customers with the Services to which your use relates (e.g., aggregate survey results and trending analysis).
- Business Transfers. We may disclose your information to another entity in connection with, including during negotiations of, an acquisition or merger, sale

or transfer of a business unit or assets, a bankruptcy proceeding, or as part of any other similar business transfer.

- In Response to Legal Process. We may disclose your information in order to comply with the law, a judicial proceeding, or court order, such as in response to a court order or a subpoena. In certain situations, Energage may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.
- To Protect Us and Others. We may disclose your information where we believe it is necessary to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety of any person, violations of our Terms of Use or this Policy, or as evidence in litigation in which we are involved.
- Aggregate and De-Identified Information. We may share aggregate or de-identified information about you with third parties for marketing, advertising, research, or any other lawful purposes.

# 2. Data Protection

## 2.1 Who has access to my data?

Sensitive personal information is only disclosed to those with a need-to-know in the performance of their duties. As such, only a small number of our internal staff has access to email addresses and aggregate survey response data in our online results tool/reports.

## 2.2 Is my data shared with any third parties?

Energage does not disclose information to any other party (secondary sharing) without the express permission of the customer. However, we reserve the right to utilize the Collected Information and provide such information to third parties for research and

analytics purposes including, without limitation, benchmarking purposes, provided that Company and its employees are not identifiable.

Aggregate/statistical data is combined with other companies in order to create sector-based benchmarks.

If a company is named a Top Workplace in one of our participating programs, some aggregate information and/or individual comments from engaged employees may be shared with the publishers.

For our full list of subprocessors, please see: https://www.energage.com/trust/subprocessors

## 2.3 Is my data sold to any third parties?

No, Energage never sells data or information about its customers to any third parties.

## 2.4 How long is my data stored?

By default, the information is stored indefinitely. This primarily includes any employee email addresses and/or phone numbers that were provided by the customer, along with employee comments. We cannot delete aggregate information that is used in benchmarking. We keep historical data that is useful for reporting on trends over time. We are not currently subject to any medical (e.g. HIPAA) or financial regulatory policies due to the nature of the information we collect and store; however, we maintain GDPR compliance.

Personally identifiable information can be deleted by our development team upon written request to info@energage.com.

# 3. Account Security

## 3.1 What security controls does an Energage account have?

Survey Tokens

Survey participants are issued a survey token that is active until either they complete their survey or their company's survey is closed (whichever comes first). This token only allows access to their individual survey, and are randomly generated 8-digit alphanumeric values. Survey participants do not create unique Energage accounts.

Account Administrator Access

Account Administrators (typically HR or Marketing teams) are assigned administrator access upon onboarding with Energage. New administrators are emailed a uniquely-generated one-time security token that expires upon initial login. Once they log in with the temporary link, a password must be chosen.

Account Lockout

If a user has five or more invalid access attempts within 5 minutes, they are automatically locked out. Each subsequent invalid attempt will increase the lock time, with the maximum lock being 1 hour.

Password Reset

If a password is forgotten, a user may use the "Reset Password" link. Energage sends an email with a unique reset link to the email address associated with the individual's account. There are no "challenge questions" or other means of identification.

Password Complexity Requirements

Access to our administrative and results applications requires a password that includes a) at least 8 characters, b) at least one lowercase letter, c) at least one capital letter, d)

at least one number, e) at least one symbol/special character. Passwords expire after 6 months.

Data Access Controls

Access to the survey tool and survey results is controlled by the Account Administrator. The Account Administrator controls users' data access permissions. Typically, users are given access to data only within their immediate department or division.

## 3.2 How are accounts provisioned (i.e. created)?

New accounts are created when a new survey is created. Users can be granted access to the Survey Tracker or Survey Results. Administrators can also create sub-accounts and grant access to their team members.

Note that survey participants do not have individual profiles or accounts within the Energage platform; they only have access to their own survey using their assigned survey token.

## 3.3 How are accounts deprovisioned (i.e. deleted)?

Energage follows a templated ticket process that notifies administrators immediately via email to revoke credentials to terminated employees. Account deletions are completed the same day.

## 3.4 How are survey participants added?

The process of uploading employee email addresses and demographic data is done by the surveying company through the Energage platform's "Upload" page. Please contact support@energage.com with any questions.

# 4. System Security

## 4.1 How are systems hardened against security vulnerabilities?

Our applications are hosted on Microsoft Azure Virtual Machines (VMs). By the principle of shared responsibility, Microsoft is responsible for physical security, host infrastructure, and network controls within Azure. Energage is responsible for the security of the virtual machines, the private network, identity and access management, and data hosted within Azure. We rely on automated vulnerability scanning from Qualys to ensure that our operating systems and system software are protected against known security vulnerabilities.

All critical vulnerabilities are remediated as soon as possible.

## 4.2 How are applications hardened against security vulnerabilities?

Applications at Energage are developed in accordance with security best practices to include, but not limited to, authentication and authorization, session timeouts, data validation, output encoding, and error handling. We also use real-time security monitoring and protection from Qualys and Microsoft Azure. Developers are trained in the OWASP Top 10 Most Critical Web Application Security Risks.

## 4.3 What is your Risk Management policy?

Our risk management policy takes into account threats, exposure, likelihood, and harm to Energage and its customers. Energage periodically assesses the risks which include the likelihood and impact of harm from the unapproved use, disclosure, modification or disruption of Energage systems. Risk Assessment results are then shared with relevant persons/teams and addressed as needed based on the likelihood and impact of the risk.

# 5. Data Encryption

## 5.1 How is data protected in transit? At rest?

All data in transit is protected by an encrypted HTTPS connection and support TLS 1.1 and TLS 1.2. Our certificates are signed with the SHA256withRSA algorithm for increased confidentiality.

All data is encrypted at rest using 256-bit AES and is stored in Microsoft Azure, protected by Storage Service Encryption. We use Transparent Data Encryption (TDE) on all of our databases with the AES algorithm and 256-bit key. When TDE is enabled in Azure, the backups are also automatically encrypted. TDE protects data and log files, using AES and 3DES encryption algorithms.

# 6. System Availability

## 6.1 Is this a high-availability system? Is there an uptime guarantee?

Our systems are not mission-critical, therefore, we do not have any uptime guarantees. However, we make every effort to ensure the availability of our systems. We do have maintenance windows on weekends where our systems will be unavailable.

## 6.2 Do you have an incident response plan?

Yes. Our Incident Response Plan is documented to provide a well-defined, organized approach for handling potential threats to systems and data, as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to the Energage, LLC private network. This Incident Response Plan identifies and describes the roles and responsibilities of the Incident Response Team. The Incident

Response Team is responsible for putting the plan into action as well as notifying customers if needed.

# 7. Disaster Recovery and Business Continuity

## 7.1 Describe your backup and disaster recovery strategy

In the event of a disaster which interferes with Energage's ability to conduct business from one of its offices, Energage follows its Business Continuity and Disaster Recovery Plan, used by the responsible individuals to coordinate the business recovery of their respective areas and/or departments. The plan is designed to contain, or provide reference to, all of the information that might be needed at the time of a business recovery.

## 7.2 How often are your disaster recovery plans reviewed and tested?

Our Business Continuity and Disaster Recovery Plan is reviewed annually, and table-top tested bi-annually.

# 8. Physical Security

## 8.1 What physical controls are in place?

The Energage office has badge restricted access with restricted access during non-business hours, visitors are always escorted, badge access is immediately removed upon employee termination, and 24x7/365 alarm monitoring.

Microsoft Azure Data Centers have multiple layers of physical and logical security including high-security perimeter fence, 24x7/365 surveillance, vehicle checkpoints, multi-factor biometric entry points, full-body metal detection, on-site hard-drive destruction, state-of-the-art fire suppression systems, 24x7/365 from Microsoft's cyber

defense operations center.  Learn more here: https://www.microsoft.com/en-us/cloud-platform/global-datacenters

# 9. Compliance

## 8.1 Is Energage GDPR compliant?

Yes. Energage is GDPR compliant. If you would like to exercise your rights as an EU data subject, please contact privacy@energage.com, or visit https://www.energage.com/trust.

## 8.2 Is Energage CCPA compliant?

Yes. Energage is CCPA compliant. If you would like to exercise your rights as an California data subject, please contact privacy@energage.com, or visit https://www.energage.com/trust.

# 10. Common Configuration Questions

## 10.1 What Browser/System specifications are required?

The Energage platform is fully web-accessible and platform agnostic. We recommend using the latest version of Chrome or Microsoft Edge for the best user experience. Our survey application is backward-compatible with all modern browsers. Our survey application uses both cookies and JavaScript.  Survey takers will need to have both enabled in order to complete the online survey.

The application does not require additional software to support its overall functionality (i.e. Java, Adobe Reader, MS Office, etc.).

## 10.2 What are the Spam/Web Filter configuration requirements?

Survey participants are notified through email with a link to their survey. To ensure that everyone at your company is able to receive this email, your spam and web filters need to be configured to allow inbound email from energage.com. These configuration details are below:

### a) Spam filter configuration details

| | |
|---|---|
| SMTP server IP addresses: | 198.2.187.91,<br>98.129.209.146 |
| Email "From:" addresses: | survey@energage.com<br>support@energage.com |
| Email "From:" display names: | Energage Survey<br>Energage Support |
| Email subjects (may be any of these): | Your [COMPANY_NAME] Workplace Survey<br>Your [COMPANY_NAME] Survey Reminder<br>Your [COMPANY_NAME] Workplace Survey FINAL Reminder<br>Your [COMPANY_NAME] Energage Survey<br>Your [COMPANY_NAME] Energage Survey Reminder<br>Your [COMPANY_NAME] Energage Survey FINAL Reminder<br>Our Employee Survey<br>Employee Survey Reminder |
| URLs in emails (part in italics varies): | https://survey.energage.com/***<br>http://responses.energage.com/*** |

## b) Web filter configuration details

| | |
|---|---|
| Domain name: | secure.energage.com<br>survey.energage.com<br>app.energage.com |

## c) Additional non-Energage domains to whitelist (recommended)

| | |
|---|---|
| Domain name: | *.pendo.io<br>*.cloudfront.net<br>*.prodperfect.com<br>*.googleapis.com<br>fonts.gstatic.com<br>fullstory.com<br>*.intercomcdn.com |