Privacy & Security Policy

Updated on the 1st of January 2015.

ENGAGE Software BV ("ENGAGE") recognizes that many of our customers are subject to certain privacy-related laws that govern the handling of personal information. We seek to support our customers' compliance to such laws by providing a privacy and security policy.

1. Privacy Statement

- For data on ENGAGE's website, ENGAGE provides assurances around the types of information collected, how that information may be used, and how that information may be shared. This includes security measures.
- ENGAGE offers individuals the opportunity to manage their receipt of marketing and other non-transactional communications.
- ENGAGE offers individuals the opportunity to update or change the information they provide to the company.

2. Responsibilities

- ENGAGE has multiple individuals responsible for security and security-related matters. The CEO is responsible for ENGAGE's security program and personnel, including information, product, and corporate security, enterprise risk management, and technology audit & compliance.
- This Privacy & Security Policy of ENGAGE is part of our personnel handbook. All personnel is required to follow the confidentiality, privacy, and information security policies.
- ENGAGE regularly discusses with its personnel information security awareness issues and the obligation to safeguard confidential information, including customer data and personal information. These discussions take place during regular company team sessions.

3. Contractual Privacy Protection and confidentiality

- Engage will not disclose customer confidential information, including customer data, except under certain narrowly defined circumstances, such as required by law.
- ENGAGE shall not access customer's accounts, including customer data, except to maintain the service, prevent or respond to technical or service problems, at a customer's request in connection with a customer support issue, or when required by law.

4. Customer communications

ENGAGE strongly encourages customers to adopt industry-standard solutions to secure and protect their authentication credentials, networks, servers, and computers from security attacks.

- We communicate with our customers about current issues and trends through our newsletters and websites.
- We email end-users about specific security issues when warranted.
- We publish guidelines to our customers about the implementation of customer-controlled security settings. These guidelines are also part of our product trainings and available through our support desk.
- We offer security-related sessions at our customer conferences and webinars.

5. **Technology**

ENGAGE maintains a comprehensive array of technical measures to protect the ENGAGE service and offers a set of customer-controlled settings to further heighten privacy and security protection.

- When creating a new user account for a new customer, ENGAGE will forward the customer login data to the designated key user of such customer. The key user username preferably is the direct email address of this key user. When ENGAGE or its systems generate a new password, the user is requested to change this temporary password at first log-in. The temporary password will expire after 15 days.
- Customer is the only one who can create additional accounts for a multi-user environment. Every new user will get a temporary password by e-mail with the (enforced) request to change it at first login.
- Customer's passwords are not accessible by ENGAGE personnel.
- Application logs record the creator, last update and timestamps, for every record and transaction completed.
- Access to the customer's User Manager for the software solution is limited to the customer. ENGAGE support staff will access this user manager only after specific approval from the customer to this extend.
- The ENGAGE support desk can only access customer's data by using the login data that is provided by the customer. No customer login data is kept in files or CRM systems by ENGAGE.
- Customers can restrict access to the ENGAGE solutions by defining IP-addresses from which their account may be accessed.
- Customers can restrict access to allow login using HTTPS only.
- Software configurations are designed to provide secure logical separations of customer data that permit each customer to view only its related information.
- Multi-tenant security controls include unique, non-predictable session tokens, configurable session timeout values, password policies, sharing rules, and user profiles.

6. Hosting

- ENGAGE solutions are hosted by Microsoft Azure.
- Microsoft Azure has a strong certification and compliance policy which can be found via http://azure.microsoft.com/en-us/support/trust-center/.
- Network security measures as set by Microsoft Azure apply.
- The ENGAGE service is highly scalable and redundant, allowing for fluctuation in demand and expansion of users while greatly reducing the threat of outages. The production servers of Microsoft Azure are three-fold redundant on basis of mirroring.
- All customer data is stored in secure data centers and is replicated over secure links to a disaster recovery data center. This design provides the ability to rapidly restore the ENGAGE service in the case of a catastrophic loss.
- In addition to our disaster-recovery capabilities, customer data is backed up to disk in a separate data center.
- The database of ENGAGE solutions is only accessible from the ENGAGE offices. The database may only be accessed by the development staff. The database is only accessed to install new releases or to manual create an (extra) backup.
- The production servers are hosted by Microsoft Azure. ENGAGE personnel has no access, directly or indirectly to these servers. The servers are located in North Western Europe; the exact physical location of the servers is not known by ENGAGE personnel.

6. Password policy

- All passwords need to be of a minimum length of 8 characters and should contain at least one digit, one uppercase character and one lowercase character. All temporary password (e.g. after adding accounts, users or resetting password) that are generated will expire after 15 days.
- After 3 invalid login attempts the account will be blocked for 15 minutes.

Change

ENGAGE is entitled to change this Privacy & Security Policy. A New version of this policy will be provided through our website.