20221003
Version 5.1
Author Ilya Devèrs

REWORC

Technical and Organizational Measures
for a secure environment with respect for privacy

Introduction

Why this document?

The risks associated with IT systems can be mitigated by implementing technical and organizational measures. An IT system containing personal data must therefore meet certain criteria to ensure the security of the data. Technical measures are those that directly involve the IT system. Organizational measures, on the other hand, relate to the system's environment and particularly to the people using it. Only an interplay of both types of measures can prevent data from being destroyed or lost and mistakes, fakes and unauthorized access from occurring. These measures are part of the life cycle of an IT system and must be implemented at every level of the system.

About Reworc Security & Privacy

Security

Preventing unwanted access and malicious use of the components of the Reworc platform.

Why
The Reworc platform is used by organizations around the world to provide insightful information that helps to improve the work environment. It needs to be protected from malicious access and abuse to provide a stable and trustworthy environment.

How
- The components of the Reworc platform use state of the art, enterprise class cloud-based components.
- The teams we employ to build the individual components and maintain the overall platform are experienced in developing and maintaining business critical applications for customers around the world and have a track record of providing high quality, trustworthy and secure systems.

What
The Reworc organization and platform form a robust and secure environment suited to the task of expedient and secure data gathering, information exploration and communication, implementing Information Security best practices (ISO/SEC 27002:2022)

Privacy

Prevent (mis)use of information that is traceable to individuals.

Why
The Reworc platform makes use of employee level information. It could be misused for alternative purposes other than the intended use. We commit to the highest standards of privacy warranting guidelines and comply with individual nations and corporations' guidelines.

How
- Personally identifiable information is only used for data gathering purposes (E-mail, First name).
- The Reworc platform is completely transparent about the types of information that are gathered, and how they can be adjusted or removed.
- Ownership of Personally identifiable information is never transferred to Reworc but remains property of the 'controller'.

What
The Reworc platform provides meaningful and transactional knowledge with respect to international privacy laws.

Security in detail

Reworc implements an Information Security Management System based on the latest best practices and guidelines, including annual audits. The Reworc system is developed and hosted on the Microsoft Azure cloud platform. Microsoft Azure, as a cloud computing platform, provides confidentiality, integrity, and the availability of customer data. It must also provide transparent accountability to allow customers and their agents to track administration of services, by themselves and by Microsoft. Reworc implements and maintains the security control framework that is extended to its sub-processors.

Reworc's sub-processors' cloud infrastructures undergo annual audits for PCI DSS, SOX and HIPAA compliance, as well as internal assessments throughout the year. The main component, that is hosted on the Azure cloud has obtained ISO/IEC 27001:2005 certification and auditing standards attestations.

Reworc secures the data transmission between the browser and the servers by industry standard Secure Sockets Layer, with identity provided by high quality certificate providers.

The teams that provide development work for Reworc are trained and proficient to correctly use the Azure components in the correct way and have ample experience developing business critical applications (OWASP best practices).

Note #1: Reworc's ISMS is based on ISO/IEC 27002:2022, including annual auditing with penetration testing by external auditors.

Note #2: Reworc's platform has configured the cloud systems it uses to only host information in the European Economic Area.

Note #3: ISO/EC 27001:2005 is a standard that specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System. You can find out more about it here.

Specific security measures

Organizational controls

Robust Information Security Management System
- An evolving, risk based, ISMS
- Clear policies for Information Security
- Segregation of environments (dev-ops)
- Suppliers and networks of threat intelligence
- Information security in project management
- Privacy by design
- Information security for use of cloud services
- Independent review of information security

Identity management
- Robust and modern provider of Identity (Azure AD B2C)
- Federated Authentication
- Role-based Authorization

Privacy and protection of PII
- Legal, statutory, regulatory and contractual requirements are embedded
- Response to information security incidents are formalized

People controls

Awareness & Training
- Continuous information security awareness
- Privacy sensitivity training
- Segregation of duties (development, R&D, commercial)
- Personal proficiency with password managers, VPN software

Terms and conditions of employment
- Screening
- Disciplinary process
- Confidentiality and non-disclosure agreements
- Remote working
- Information security event reporting

Reproducibility of the processes
- All staff uses the same procedure when exercising the data subjects' rights
- Well documented procedures
- Only trained and authorized staff execute these procedures

Specific security measures

Physical controls

Security of workplace
- Controlled access to the workplace. The persons who are permitted to access the workplace or Reworc are known
- Regulate access and reception for visitors in such a way that they cannot freely move around the building on their own.
- Use workplaces in secured co-working or dedicated buildings.

Security of hosting facilities
- Only use certified secure cloud computing providers

Workplace security
- No printed materials are used
- All workstations are locked with strong passwords that are reset frequently

Network security
- Data transfers from between servers is kept to a minimum
- Networks are protected using SSL with certificates from trusted sources
- When network access is required from outside locations to work on the data a Virtual Private Network is applied.

Technological controls

Logging
All used cloud systems log manipulations to the data. Application based logging for traceability and accountability.

Pseudonymization / Anonymization
To limit Personally Identifiable Information on the platform the identifying data will be masked using the SHA hash protocol and deleted when no longer needed. See "Privacy in detail in this document".

Encryption
Strong encryption is used throughout the platform; TLS 1.2 with robust ECDHE_RSA with P-384 and AES_256_GCM for information in transit. Encryption of data at rest with AES_256 based encryption.

Backup
All relevant data for the service delivery is backed up frequently. Old backups are destroyed. Recovery point objective is 10 minutes. Recovery time objective is 1 hour.

Data destruction
Data is physically and irretrievably deleted when no longer needed.

Privacy in detail

General Data Protection Regulation (GDPR)
Because Reworc deals with information gathered at the employee level the protection of privacy is one of our main concerns.

The platform Reworc uses to gather data has the strictest privacy policy in the business. The information that makes the data traceable to an individual (Name, E-Mail) is only used during the information gathering phase, when employees provide information. The information the organization provides us in order to explore and analyze the data is NOT replicated on the data gathering platform, minimizing the propagation of individual information about an employee.

The Reworc system is, and always was, compliant with the European GDPR regulations. The Reworc platform never transfers information to third countries outside the EU.

Following the Schrems II ruling in 2020, we rely even more on its structure when customers request us to move personal data to third countries (outside of the EU). In practice this has never occurred, and we follow the advice of the EDPS to avoid doing so.

When necessary or preferred we enter into specific Data-Processor agreements and can provide Data-Processor contract templates, outside of the standard Data-Processor agreement that is part of our general terms & conditions, that is in effect when Reworc and its clients enter contract.

More information about the warranties the GDPR provides can be found here.

We closely follow the developing regulations by closely monitoring the European Data Protection Supervisor.

Schrems II is the ruling in relation to transfers of personal data to third countries, and in particular, the United States. Based on this ruling, policy such as “EU-US Privacy Shield” became invalid.

Specific privacy measures

The information that the organization provides to analyze and explore the results (FTE, team-names, function descriptions, sites, other required attributes) are NOT combined with the information that allows this information to be traced to an individual.

We can combine these datasets using an industry standard high grade data integrity hashing algorithm called SHA-256. Each e-mail address is translated to a unique code that cannot be used to determine the original e-mail address.

The key between these datasets is not stored on any system outside WPA's own IT infrastructure. No cloud drives, extranets etc.

The individuals' answers, and the information the organization provides, are combined through the SHA hash making the data exploration in the Reworc application completely pseudonymized. This data is not used anywhere outside the organization's dashboard.

Data subject's rights

- Clear information is available for the data subjects, and they are informed of their rights
- The SLA of Reworc provides a clear process for dealing with information requests
- The process to change, correct, block and destroy the data is reliable
- All staff uses the same procedure when exercising the data subjects' rights
- Only trained and authorized staff executes these procedures

About SHA

In cryptography, SHA is a cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States NIST.[2]

Although the SHA-1 hash function is deprecated for Cryptography reasons because a proof of concept in which hash results collide, we continue to use the SHA-256 version of the algorithm.

Reworc does not use this SHA algorithm for cryptography, only for data integrity and pseudonymizing (masking), of Email addresses and thus to individuals.

Specific privacy measures

Using attribute sets to filter to individual results

It is sometimes possible that a combination of several of the provided attributes can, in theory, reveal individual responses. We support our clients to prevent this from occurring by placing emphasis on coarse grained attribute value groups versus fine grained attribute value groups.

As a fail safe we provide a Privacy setting that lets an organization provide a minimum group size and response rate. Below this threshold information about the population is blocked at the server level. If this occurs a ”privacy violation” message is displayed.
This functionality works on pre-defined, ad-hoc and scenario queries.

Since the actual threshold values can be determined on a population-by-population basis we accommodate the common privacy policies.

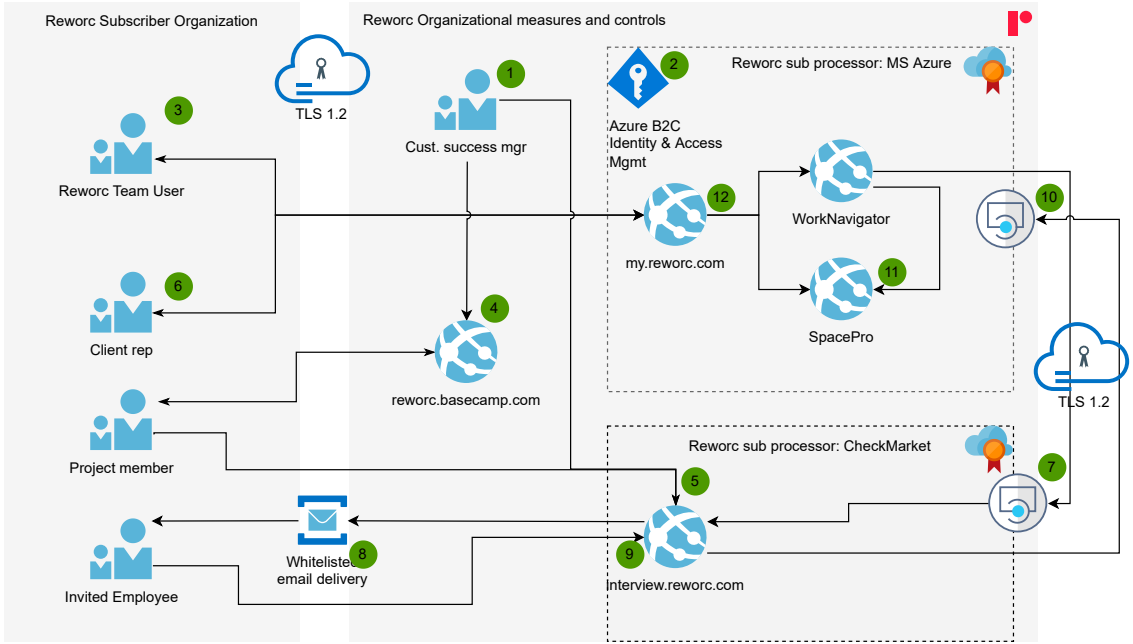
Coarse grained versus fine grained:

Fine grained attribute sets are for example individual functions:

Principal Sr. Sales executive, Manager mid-market segments east-coast. Lead user-experience engineer.

Coarse grained attribute sets are for example: Senior management. Design professionals.

Reworc system description



1. Reworc creates the Reworc organization that subscribes to Reworc and invites authorized Users to become "Team users" for the subscriber.
2. All users of the Reworc platform are identified, authenticated and authorized using Azure B2C Active Directory.
3. Using the my.reworc.com portal, Team User configures the Digital Interview Workstyle Assessment, including the modules and configuration of the questions and answers. Team User creates the Client on the Reworc platform that will assess its workstyles and creates a "Client Rep" for that client. A Client Rep is typically an HR employee for the Client organization.
4. ***Optionally***: Reworc's Customer success manager creates a project site for the Digital Interview project on the Basecamp project management website, and invites client stakeholders involved (Communication specialists, Project managers, etc.). **No Personally Identifiable Information is processed on this application.**
5. Reworc's Customer success manager instantiates a D.I. template on the interview.reworc.com application, provisioned by Reworc's sub-processor CheckMarket.com. The project members perform Q&A on the preview version of the digital workstyle assessment (interactive questionnaire).
6. Once the participating employees, and their attributes, are defined, the Client Rep exports the population from the HR system and imports it directly into the WorkNavigator application. Team User and Customer success mgr will review and process it on the platform.
7. When the invited population is finalized, the Reworc platform sends a subset of the Personally Identifiable Information to the Checkmarket platform via a secured API call (email address, first name, reworc id)
8. When the Digital Interview goes live, the employees of the Client Organization are emailed invitations and reminders via the whitelisted email address of Reworc. This occurs in batches so as not to overload any mail servers and ensure deliverability.
9. Invited employees click on a personalized link that will take them to their personal version of the D.I. This allows them to answer fewer questions and follow different branches.
10. When an individual employee finishes their Digital Interview, their answers are sent to the Reworc platform via a secured API call, at which point the Personal Identifier is pseudonymized. At the closure of the D.I. the respondents who did not answer all answers are also processed via a batch process. At this time, all remaining employees are also pseudonymized. Team User can now use the WN Dashboard to analyze work styles.
11. After the workstyles of the employees are analyzed (at sufficient large group sizes to ensure privacy), they are grouped in scenarios and groups and their anonymized work behaviors are used for behavior-based dynamic space programming.
12. At the end of the subscription, or at a time specified by the data controller, Reworc removes all (pseudonymized) identifiers so that data is no longer Personally Identifiable Information. Reworc masks organization information with generic values and holds the information for learning and calibration purposes.


Business software to understand how work is done.

Make work work

www.reworc.com
info@reworc.com