Information security at PRé

Answers to frequently asked questions

SimaPro

Title: Information security at PRé | FAQ

Written by: Phoebe Dennis, Sevrien Arentsen, Steven le Corvaisier, PRé Sustainability

Version: 1.0

Date: October, 2023

About SimaPro

SimaPro was developed by PRé with the goal of making sustainability a fact-based endeavor. PRé has been a leading voice in sustainability metrics and life cycle thinking development for more than 30 years, pioneering the field of environmental and social impact assessment. We develop tools that help you create value and drive sustainable change.

PRé
Fact-based sustainability

SimaPro is distributed through a Global Partner Network. All partners were carefully selected by PRé. A partner in your country will act as your local SimaPro sales and support representative and can show you a personal demo or provide more information.

Find your local partner: simapro.com/global-partner-network

Get in touch

T +31 33 450 40 10

E support@simapro.com

W simapro.com | support.simapro.com | pre-sustainability.com

Contents

1 General security and ISMS

How does PRé keep your information safe and what standards do we comply with?

PRé Sustainability B.V. is ISO/IEC 27001:2013 certified under certificate number ISC 123 for design, build and support of a web-based platform for life cycle assessment and sustainability performance. Every year we continuously revise and improve our processes to comply with the requirements of ISO/IEC 27001:201. We run annual internal audits and are also externally reviewed by an independent auditor, BSI (Lead Auditor changes every three years) annually.

We have dedicated process owners for ISO27001 controls. The overall Information Security organization is managed by the management and the process owners. Information Security Management and Tactical/operational tasks are delegated to process owners. The process owners are responsible for all Information Security aspects of their own process. Each process owner is responsible for the tactical/operational activities of PRé's Information Security policy and Information Security management system within their own process. In addition, we have an IT Security Project Manager.

What aspects of operations and services does PRé's information security and privacy program cover?

Both the processes that directly deal with customer data (such as IT) and the processes that might indirectly affect the security of customer data (such as HR processes) are in the scope of our ISMS.

Do employees of PRé undergo information security and privacy training?

As part of onboarding and our ISO27001 compliancy, all employees (including contracted and temporary hires) receive an information security and privacy (including GDPR) training upon hire. PRé also has a Continuous Awareness Program, where every two months an awareness moment is planned and refresher sessions regularly occur.

Are background checks performed on PRé employees?

PRé performs relevant background checks for personnel who are entrusted with sensitive information or granted access to sensitive systems and/or confidential information. This can include CV checks, criminal record/conviction checks, reference checks, and Certificate of conduct for natural persons (VOG NP) for all employees accessing and handling the organization's data.

Does PRé have controls in place to ensure that data is not transferred outside of the EU?

As agreed in contracts, PRé/SimaPro does not transfer data outside EU.

Does PRé have a written password policy that details the required structure of passwords?

Yes. The system requires new password twice a year. The minimum password length is 8 characters and requires a symbol, number and capital character.

2 Physical security

How does PRé control, manage, and review physical access of office facilities?

PRé is located in a shared office building with a staffed reception desk. We have an entire floor for our own use and share another floor with one other organization. Some facilities are shared with other companies, including the main entrance, lifts, stairwell, and carpark. Access to both floors is only possible via an electronic access pass. Access to spaces is restricted to PRé employees and visitors. Our BHV (Emergency Response Officers) have more access to rooms in the building, special rooms like patch and server rooms.

PRé has a process in place for granting and revoking physical access to office facilities. We regularly review physical entry logs, and retain these logs for at least 6 months. All network equipment is protected and locked away, and only assigned IT employees have physical access to such equipment. The SimaPro platform is a cloud solution, therefore we do not have any data centers to store confidential data onsite.

3 Firewalls, vulnerability scanning, VPN, patches, accessibility, encryption

Are network boundaries protected by firewalls and is there regular network vulnerability scanning?

Yes, we have firewalls for filtering all inbound and outbound traffic and run regular network vulnerability scanning.

Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used?

Yes.

Is antivirus software installed on data processing servers?

Yes.

Are system and security patches applied to servers on a routine basis?

Yes.

Are PRé's client systems configured to log security-relevant events?

We have comprehensive logging enabled on client systems, including security events. We keep these logs in case we need to investigate an incident.

Does PRé have a responsible individual/team to review service providers and subcontractors, to ensure that they sufficiently protect the security and privacy of sensitive information and systems?

Yes, this is part of the role of our process owners for ISO27001 controls. The process owners are responsible for all Information Security aspects of their own process.

Is the management of servers (or parts of) outsourced?

Yes, the SimaPro SaaS platform is hosted in the MS Azure Cloud and is composed of a Single-Page-Application and an API built on .NET stack.

Has PRé implemented monitoring and alerting for our network?

Yes. We regularly review these logs and retain them in case we need to investigate a security incident. We retain these logs for at least 6 months.

What safeguards does PRé have in place to maintain the integrity and availability of public, internet-facing endpoints?

Within our infrastructure, all systems connected to the internet are fully stripped of non-essential functionality and have HBP mechanisms in place, ACL, next gen firewalls, IDS's and AV and anti-malware/ransomware software. Azure Firewall Threat intelligence-based filtering can alert and deny traffic to and from known malicious IP addresses and domains. The IP addresses and domains are sourced from the Microsoft Threat Intelligence feed. We also make use of MS Azure frontdoor protection.

How does PRé ensure that our SSL configuration only offers secure protocols and ciphers are offered to clients?

We regularly review the cipher suite advertised by the server and the protocols it uses.

Does the SimaPro SaaS solution contain any hard coded passwords?

All hard coded passwords have been migrated to the MS Vault.

Are any APIs used for the SimaPro SaaS solution, and are any passwords embedded in requests?

API is exposed for direct use or Platform Frontend. Requests requires a valid non-expired authentication token.

What is the use of encryption and cryptography?

We have the latest SSL/TLS internet security controls in place. Data at rest is encrypted, and encryption is always enabled in transit by default. All encryptions provided by MS Azure are in use and applied to data.

Resiliency

SimaPro SaaS solution is a high availability (HA) solution hosted in the Azure cloud. Microsoft guarantees that Azure App Service will be available 99.95% of the time. Further detail can be found here regarding the SLA. https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services?lang=1

4 Authentication

What protocols are being used to connect SimaPro SaaS solution?

Internet HTTPS connections to the SimaPro platform. To make connecting to the platform as safe as possible, we implement security features for a number of connections (eg. Azure managed certificates).

How are the user interface and database layers of the SimaPro SaaS solution segregated?

We have four environments in which we run separate instances of the whole SimaPro platform. All environments live in a separate MS Azure subscription, so we can manage access rights independently. This allows us to test new features during development, do acceptance testing and pilots with new software features, manage the mother database, and have a stable environment for our customers to work with. Every new company has their own database so that data is isolated from other companies, and is able to be restored, backed up, and allow the database to be scaled independently of those of other companies.

What are the available authentication options to access the SimaPro SaaS solution?

Credentials (email and password) submission for each user. The default password strength requirements of SimaPro SaaS are:

- Length: 9
- Lockout window: 90 days (after 90 days, the account is locked)

- Change password window: 90 days (after 90 days, the user must change the password)
- Password history: 4 passwords (the password must be different from those chosen the last four times)
- Number of upper case characters: 1
- Number of upper case characters: 0
- Number of numeric characters: 1
- Number of non-alphanumeric characters: 0
- Lockout duration: The time it takes for an idle session to time out is also configurable per company. The default is 60 minutes.

Where are our servers backed up and what are our protocols for backups?

SimaPro SaaS solution is hosted off-site in the Azure cloud, located in Western Europe. We have a fixed backup cycle. Backups are created daily, and these backups are for disaster recovery of the platform as a whole only. The data is protected with MS Azure backup with geo-redundancy and encryption. We use 35 days retention for all customer databases in our production subscription in Azure. Data is retained for up to 6 months after expiry of a customer account.

Who has access and how do we control and manage this?

We have a formal control of access to System Administrator privileges. MS Azure access logs capture who has accessed the system and what changes were made.

Within PRé, on all relevant database entities, we log who created and last modified them as well as login attempts in an audit log.

5 Third party testing

In addition to ISO27001 certification, how else does PRé test our software?

We have also performed penetration tests, have dynamic application security testing, and static code analysis.

6 Disaster recovery, incident response, change management

How does PRé control and manage disaster recovery and incident responses?

We have a crisis team that has developed a formal written Business Continuity Plan for our entire operations as well as an Incident Response Plan and Change Management Process. Regarding our tools, we periodically carry out tests to try to replicate possible incidents (regarding data availability, integrity and confidentiality) and check the recovery scenarios. PRé has processes in place to ensure that access to data is based on a need-to-know basis, and to revoke access to those who no longer require it as part of their job function.

While PRé has not experienced any information security breach to date, we have controls in place to identify, document, and promptly contact customers if we became aware or suspected any such breach.

Via MS Azure, there is an RTO of at least 12 hours as acceptable and a cross region RPO of 1 hour when a data center goes down.

SimaPro's databases use Zone redundancy. Zone-redundant storage (ZRS) copies your data synchronously across three Azure availability zones in the primary region.