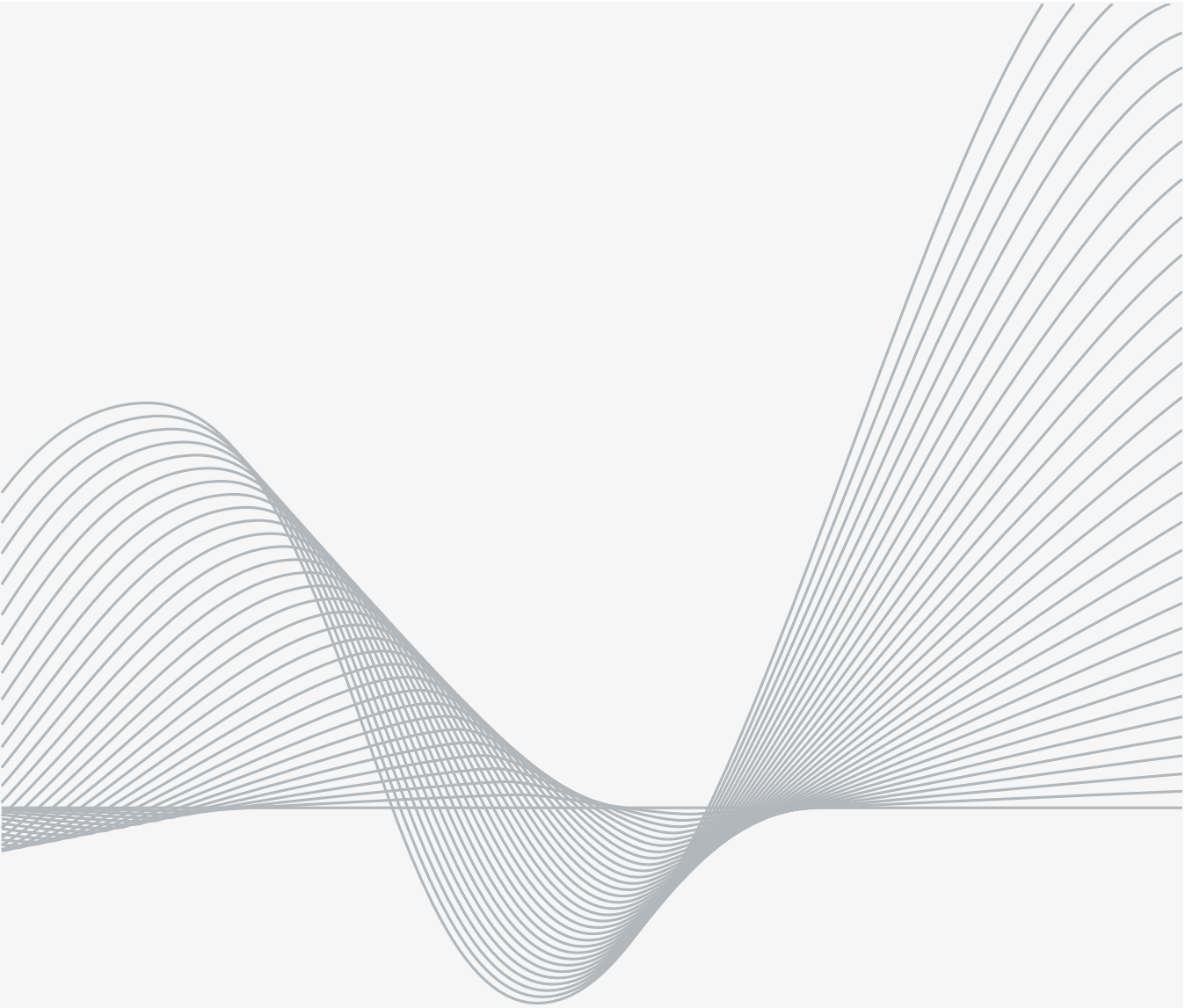
SIMAC

Privacy statement IT environments

Version: August 2025
Scope: (guest) users in Simac's IT environments



Simac

De Run 4256
5503 LL Veldhoven

Postbus 340
5500 AH Veldhoven

T: +31 (0)40 258 29 11
E: info@simac.com

KvK-nummer: 17162224
BTW-nummer: NL8128.78.139.B01

SIMAC.COM

1. Purpose of this Declaration

This privacy statement informs (guest) users of Simac about the way in which we handle personal data within our IT environment.

2. Responsibility

Simac Techniek NV and its affiliates (hereinafter: Simac/we/our) is responsible for the processing of personal data within its IT environments. Simac monitors compliance with laws and regulations and internal codes of conduct on privacy. The processing of personal data is always done with respect for fundamental values such as integrity, transparency, fairness and respect for everyone's privacy. Personal data is processed and stored in a secure manner.
If you have any questions or reports, please contact our Privacy Officer via privacy.officer@simac.com.

3. Data processed

When using Simac's IT environments, the following data can be processed:

- Name and email address
- Organization details
- IP address and device information
- Activities within Simac's IT environments

3.a. Monitoring and Detection

To proactively identify suspicious activity and movements within our network, we use Security Information and Event Management (SIEM) / Managed Detection and Response (MDR). These systems allow us to gain real-time insight into network traffic, user behavior and potential threats. Through advanced correlation and continuous monitoring, we can respond quickly to incidents and strengthen the overall security posture.
This monitoring is performed based on our legitimate interest in ensuring the security and integrity of our IT systems (Article 6(1)(f) GDPR).

3.b. Internet traffic monitoring

In addition to internal network monitoring, traffic to and from the internet is also actively monitored. This includes inspecting inbound and outbound data streams for suspicious patterns, applying firewall rules, and using threat intelligence to detect and block potential risks early.

4. Purposes of processing

The data is processed for:

- Authentication and Authorization
- Security of systems and data
- Access logging and monitoring
- Compliance with legal and/or contractual obligations

5. Legal basis

The processing is based on:

- Performance of an agreement (access to Simac and/or customer systems)
- Legitimate interest (security and control)
- Legal obligations (such as GDPR)

6. Retention periods

Data will not be kept longer than necessary. Logging data is periodically deleted in accordance with internal policies. Retention periods depend on the nature of the data unless longer retention is required in case of an incident or legal obligation.
Processed data is not shared with third parties, unless legally required (e.g. regulatory authorities).

7. Data breaches and incidents

Incidents are reported to the Service Desk and the Privacy Officer. If legally required by the GDPR, data breaches will be reported to the regulatory authority and affected individuals.

8. Rights of data subjects

Guest users have the right to access, correct, delete and restrict their data. Requests can be submitted through privacy.officer@simac.com. You also have the right to object to certain processing, and to file a complaint with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

9. Obligations of (guest)users of Simac's IT environments

The use of the Simac environment is only permitted for business purposes that are directly related to work for or within Simac. Private use or activities without a clear relationship to Simac are not allowed.
We refer to our ‘code of conduct’, ‘protocol ICT use’ and ‘Security & Privacy brochure’. These are available on our Intranet or can be obtained via privacy.officer@simac.com.

10. Changes to this privacy statement

We reserve the right to change this privacy statement at any time in order to comply with legal requirements or to reflect changes in our processing activities or IT environment. Where appropriate, we will actively inform users of material changes.