

## Privacy statement Safesight

Version July 4th, 2021

Safesight's mission is to create the most practical and easy-to-use platform available, with which we enable organizations to work more safely, more efficiently and better together. To this end, Safesight provides services through a cloud solution with a central logbook system and an app with content and tasks for those involved. Safesight wants to be responsible and compliant with the privacy legislation (General Data Protection Regulation or GDPR) concerning your personal data. This privacy statement explains how Safesight wants to do this.

### **Who is responsible for my personal data?**

Safesight is responsible for ensuring that your personal data is processed in accordance with the GDPR. Safesight b.v. is the so-called controller in accordance with the General Data Protection Regulation (GDPR). This means that Safesight decides which personal data are processed, for what purpose and in which way.

The client who concludes an agreement with Safesight for the purchase of one of its services and for this purpose provides personal data to Safesight to enable the service (s) to function, is itself responsible for processing, providing and keeping the personal data up to date. This also applies in particular to the specific unstructured content that an organization contributes to Safesight that may contain personal data.

### **What is my data used for?**

The basis for processing personal data is being able to comply with the implementation of agreements that Safesight concludes with its clients for the fulfillment of its mission.

Safesight uses personal data to identify the employees of a (safety) organization for its clients (log in) and to recognize the user within the Safesight software. To this end, every user has a user account with a password. This user account allows the employee to perform tasks that are available within Safesight. The user also gets to see specific information based on the organization, event/project and role. The employee details (name, role and telephone number) are also placed in a contact list for an event/project so that employees can easily reach each other.

### **What personal information is processed?**

The primary personal data that Safesight processes are name, e-mail address and telephone number. In addition, the organization to which he/she belongs and the role in the safety organization he/she has stored. This data is required for the operation of the Safesight software. Users are free to make this data as irreducible as possible (such as the use of nicknames) as long as they are unique and usable within Safesight and the relevant organization / client agrees.

The operation of the system is such that as part of the functionality all actions of users during the execution of tasks are recorded and made available through Safesight via monitoring and reporting tools.

No sensitive personal data is processed apart from an optional photograph. Location data can be processed for specific operational purposes. If website statistics are collected, they are anonymous. No tracking technology is used.

# Privacy statement

## **How does Safesight obtain my data?**

Safesight receives the personal data from its clients or directly from the data subject concerned. Safesight does not collect personal data at its own initiative or on its own. Safesight can point out to clients and/or data subjects certain data quality problems that can prevent careful processing.

## **Is my information provided to third parties?**

No. Safesight only processes your personal data within the specified purpose and the agreements with clients. Distribution to third parties only takes place if they are involved in the execution of the agreement. Data is never commercially traded or otherwise made available to third parties outside the agreement without explicit permission. Data is not processed outside the European Union.

## **What are my rights?**

You have the right to view your data, correct and delete your data. In addition, you have the right to limit or obtain the processing of your data yourself. If you want to enforce these rights, you can contact us at the email address below.

Safesight does not apply automated decision-making based on your personal data, nor does it promote profiling.

## **Security**

Safesight takes appropriate security measures, both technical and organizational, to protect your data. Network traffic is based on TLS and hosting takes place on ISO27001 certified data centers in the EU (Germany). In the design and design of the Safesight software, privacy protection (privacy by design) is taken into account and privacy settings are always set at the most restrictive settings (privacy by default).

## **Retention periods**

Safesight keeps your data for as long as necessary to be able to meet the contractual obligations with its clients, but not longer. Then this data is destroyed or made anonymous.

## **Data breaches**

If there is a (suspected) data breach, the privacy officer will immediately start an investigation for further analysis in consultation with the clients and the data subjects concerned and report to the Dutch Data Protection Authority.

## **Where can I go for questions, comments or complaints?**

Safesight does not have a formal data protection officer (DPO) but has a CIPP/E certified privacy officer within its own organization. He can be reached at [privacy@safesightsafety.com](mailto:privacy@safesightsafety.com) or via:

Safesight b.v.

Attn. Privacy Officer

Europalaan 100

3526 KS Utrecht

The Netherlands

More information about the GDPR can be found at the Dutch Data Protection Authority (AP), which supervises privacy legislation (<https://autoriteitpersoonsgegevens.nl/>).

Would you like to receive the privacy statement in Dutch? Please send us a mail at [privacy@safesightsafety.com](mailto:privacy@safesightsafety.com).