

## **Resume**

We at Skopos Security Labs BV invest in your digital security. In doing so, we collect and process your personal data. We think your privacy is very important. That is why we explain in this privacy statement for what purposes and how we collect and process your data, and what your rights are.

When purchasing our services, your employer is responsible for the personal data that we process in this context. For example, your employer determines which employees have access to our services. In addition, your employer will receive reports and insights about the use of our services within your organization. If you want to know more about the way in which your employer handles your personal data, you can contact your employer. In this privacy statement we provide information about what we do with your personal data.

## **For what purposes do we process your data?**

Skopos provides insight into cyber risks thanks to the combination of powerful technology and ethical hackers. We respect your privacy as a user and ensure that your personal data is treated confidentially.

Processing of personal data only takes place in accordance with the requirements of the General Data Protection Regulation (GDPR). We may process this data insofar as this is necessary for the execution of an agreement with your employer that gives you as a user access to the Skopos platform.

Your personal data will be processed by us within the framework of the following purposes:

1. for the conclusion and execution of an agreement;
2. to offer you the agreed services, products and/or information (digitally) or to deliver them on paper;
3. if it concerns a paid service/product, to invoice;
4. to be able to send you user information, service message or other non-commercial messages;
5. to comply with the laws and regulations resting on us and to have audits performed (by an accountant);

## **What data does Skopos collect?**

### Customers

When we do business with our customers, we collect the personal data relating to our customers and their representatives, contacts and employees such as email address, business telephone number and company address. This personal data is collected when you purchase a service from Skopos, during the sales process, via telephone conversations or via e-mail.

### User platform Skopos

When you access our platform, we never need more than the following personal data from you:

- Name
- E-mail address
- IP address

If Skopos software is installed on your computer or phone, we will also process the following data, depending on your use:

- Which applications are installed on your computer or phone
- What security settings are set on your computer or your phone
- The answers you have given to the questionnaires that have been made available to you.

### **Access to your data**

A limited number of employees within Skopos are authorized to inspect your personal data. Access is based on roles, responsibilities and on a need-to-know basis. These employees are bound by confidentiality. No employee has access to your password. Your employer has access to the Skopos dashboard, which gives your employer insight into the cyber risks. You can ask your employer who has access to the dashboard.

### **Retention periods**

#### Customers

In principle, we maintain a term of two years after the end of the (customer) relationship for the use of data that we process from you. For example, if you receive e-mails because you are or have been a customer, you will continue to receive them until two years after the termination of your customer relationship.

#### User platform Skopos

All your data is kept safe by us. Your personal data will in any case be kept as long as your employer is a customer with us. Unless otherwise agreed with your employer, all personal data known to us will be irrevocably deleted 12 months after the end of the contract.

### **On what grounds do we process your data?**

We process the personal data for two bases from Article 6 of the GDPR, namely necessity for the execution of an agreement or necessity for the representation of a legitimate interest. In addition, we invoke the need to provide personal data if we are legally obliged to do so.

#### Execution agreement:

Using your name, address, and payment details to provide the service, to send you invoices and to collect payments.

#### Legitimate interest:

We want to use our tool to provide our customers with access to usernames/passwords that we can retrieve from public sources. These passwords and usernames have ended up in these public resources after unlawful hacking or data breaches. The purpose of this tool is to provide our customers with the ability to find out if their usernames/passwords can be found on the (dark)web, internet fora and Telegram. In this way, improper use of usernames and passwords can be detected early, and misuse can be prevented.

Skopos uses a narrow definition of the legitimate interest. Before we start processing this data, we have carried out an extensive weighing of interests. This has shown that we have a legitimate business interest in being able to offer customers a service that informs customers (early) about the fact that their passwords and usernames are offered/can be found on the internet. In addition to our customers (and its employees), the general public also has an interest in this processing, as fraudulent activities by criminals (on a large scale) can be prevented.

When offering this service, we cannot avoid temporarily processing passwords and usernames of people who are not employed by one of our customers. That is why we have chosen that everyone can use our tool. This can prevent fraud with passwords and usernames on a large scale. This serves the

general interest/the interest of society. There is no charge for using this tool. Send an e-mail to the e-mail address below.

### **Suppliers**

We place high demands on our suppliers. Of course, we have made agreements about the way in which suppliers should handle your data. They may never use your data for their own purposes. We have marked the suppliers that process your personal data on our behalf as sub-processors. We have concluded processing agreements with these parties. In the context of our general services, we use the following parties that may handle your personal data:

- Our servers are located at Microsoft Azure in Amsterdam. This is a well-secured data center with extensive certifications: ISO 27001, ISO 9001, ISAE3402 Type II and NEN 7510.

### **How can you exercise your privacy rights?**

We think it is important that you can exercise your privacy rights. You can contact us by e-mail, telephone or in writing. You have the following rights:

- The right of access: the right to inspect which personal data we process about you;
- The right of correction: if the personal data we process about you is not (any longer) correct;
- The right to erasure: if we no longer need your personal data for the purpose for which we received it, you have the right to ask us to delete it. There are a number of exceptions to this, such as our obligation to keep certain data for, among others, the tax authorities;
- The right of limitation: during the period that we are in the process of determining whether your data needs to be adjusted, determining the unlawfulness of data processing, determining whether data should be deleted or if you have objected to the processing, you have the right to request restriction of processing;
- The right to data portability: we will transfer all your personal data that we process based on consent or agreement to you, or to an organization of your choice.

We will follow your instructions as soon as possible, unless the law obliges us to keep the relevant personal data or there are (other) urgent reasons that oppose addition, correction, or deletion.

### **Which cookies do we use?**

Skopos only uses technical/functional cookies. A cookie is a small text file that is stored on your computer, tablet, or smartphone when you first visit this website. The cookies we use are necessary for the technical operation of the website and your ease of use. They ensure that the website works properly and, for example, remember your preferred settings and optimize our website. You can opt out of cookies by setting your internet browser so that it no longer stores cookies. In addition, you can also delete all information that has previously been stored via the settings of your browser.

### **How do we protect your personal data?**

We handle your personal data with the utmost care. We have taken various technical and organizational measures to protect your personal data against loss or unlawful use. For example, we secure our systems and applications according to the applicable standards for information security and we have taken technical and organizational measures in the form of encryption of data and physical and logical access control. The number of people who have access to the personal data is limited to a minimum.

### **Do we also process data outside the EU?**

Our starting point is to only process your personal data within the EU. Since the privacy regulation applies within the EU, we can in principle always ensure an appropriate level of protection. If it should be necessary to transfer data outside the EU, then this will only happen

only based on appropriate measures that are reasonably necessary to ensure that your data is protected.

**Finally**

We reserve the right to change this privacy statement. The most recent privacy statement is always made available on our website, which you can find in the footer. The effective date is at the top of this document. If you have a complaint about the way in which we process your personal data, we would like to ask you to contact us ([support@skopos.ai](mailto:support@skopos.ai)), so that we can process your complaint.

