SECFENSE PRIVACY POLICY

Effective date: 06.11.2019

This privacy policy describes our current privacy practices and aims with regard to collecting and protecting personal data. It may be updated from time to time to reflect changes in our privacy practices as well as legal, regulatory, technical or operational requirements.

I. Glossary

1. **Applicable laws**: all the laws and regulations relevant to the collection, processing and storage of data, especially all the data protection laws, including Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46 / EC ("GDPR"), the Act of 10 May 2018 on the protection of personal data (No. 2018.1000, as amended), as well as the Act of 18 July 2002 on the provision of electronic services (consolidated text: Journal of Laws of 2017, item 1219, as amended).
2. **cookies**: small files stored small text files that store data locally on a computer, mobile phone or other device. By storing certain information in a cookie, web browsers, ad servers, and our website are able to remember your preferences and recognize websites visited and/or web browsers used from one visit to another.
3. **Secfense** or **Controller** or **we** or **us** or **our**: Secfense Spółka z ograniczoną odpowiedzialnością with its registered office in Kraków Plac Na Groblach 21, area code 31-101 entered to the Register of Entrepreneurs of the National Court Register, under KRS number: 0000722746, with a NIP number: 6762546545, REGON number: 369676020

II. The scope of collected personal data

1. We may collect information about you through:
   - your communication with us, including the use of our contact, newsletter and registration forms,
   - your use of our website (www.secfense.com).
2. The categories of your personal data may include:
   - first name and last name,
   - company name, address, company position,
   - phone number (company/mobile),
   - Skype ID or other similar communicator ID,
   - tax identification number (e.g. NIP),
   - e-mail address,
   - data collected via social media (LinkedIn, Facebook) and Google, such as your identification data, content of your interaction with us (comments, reactions), information about your telecommunications network or IT system, and the scope of use of the mentioned services.
3. Personal data may be processed in an automated manner (including in the form of profiling) for people who have agreed that we share a newsletter with them. Automated processing consists in profiling subscribers automatically and sending personalized messages on this basis or contacting you by phone.
4. This privacy policy does not cover Secfense products. Due to the sensitive nature of the data flowing through Secfense products (i.e. authorization data) most of our customers prefer on-prem deployments, either as a physical or virtual appliance. As a result, our customers remain data controllers. In order to operate Secfense products do not need to process and store users passwords. As a result, we neither access nor process data flowing through Secfense products, unless we are specifically asked to do so by our customer. In such circumstances, the scope of our actions as a data processor is determined by the agreement between us and the customer.

5. Your personal data will be processed in accordance with Applicable laws, only for the following purposes and legal grounds:

Contract-related data

- conclusion and performance of the contract/contracts (Article 6 (1) (b) of the GDPR),
- legitimate interest of the Controller in examination, investigation and enforcement of claims or defense against claims, including in court proceedings (Article 6 (1) (f) GDPR),
- conducting tax and accounting operations in the ordinary course of our business (Article 6 (1) (c) GDPR).

Communication

- legitimate interest of the Controller in being able to communicate with customers and prospective customers, and handling requests sent through or contact form, and to promote and improve products (Article 6 (1) (f) of the GDPR,
- your consent: with respect to data which are not mandatory to send the contact form and with respect to profiling (Article 6 (1) (a) of the GDPR),
- legitimate interest of the Controller in conducting direct marketing of our services , i.e. promoting the activity conducted by the Controller, and in the cases where you grant appropriate consent – sending commercial information by means of electronic communication, terminal telecommunications equipment and automated calling systems to market our products and services (Article 6 (1) (f) of the GDPR),
- legitimate interest of the Controller in examination, investigation and enforcement of claims or defense against claims, including in court proceedings (Article 6 (1) (f) GDPR).

Other data collected via LinkedIn and Facebook pages and via Google

- legitimate interest of the Controller in being able to communicate with customers and prospective customers, including interaction via social media, for statistical purposes and to promote and improve products (Article 6 (1) (f) of the GDPR).
- legitimate interest of the Controller in examination, investigation and enforcement of claims or defense against claims, including in court proceedings (Article 6 (1) (f) GDPR).

III. Cookies and similar technologies

1. Whenever you interact with our website, some information about your activities may be automatically collected through the use of cookies and similar technologies. We use them for the purposes of traffic analysis and monitoring (e.g. we collect aggregate usage data, such as the overall number of visitors or pages viewed) and to improve the stability and security of our website. The information gathered this way may include:
   - information about your interactions with our website,
   - technical information about your hardware and software, such as cookie data, IP address, the types of devices and web browsers used to access the website, device ID and attributes, network connection type, language, internet service provider, the files you accessed on our website, access times.
2. We collect both “permanent” and “session” cookies. “Permanent” cookies are stored on your device for a long time defined for each cookie, while “session” cookies are deleted automatically when you close the browser window. You may stop delivering this information at any time by deleting the cookies stored on your device. To do this, change the settings of the currently used web browser.
3. We use the following third party technologies:
   - Google Analytics to track and report website traffic. You can learn more here: https://policies.google.com/privacy
   - Woopra to track and report website traffic. You can learn more here: https://www.woopra.com/privacy
   - Cloudflare to maximize network resources, manage traffic, and protect the website from malicious traffic. You can learn more here:

https://support.cloudflare.com/hc/en-us/articles/200170156-Understanding-the-Cloudflare-Cookies

- Calendly to facilitate scheduling meetings and demonstrations. You can learn more here: https://calendly.com/pages/privacy#cookies-and-other-tracking-mechanisms

IV. Data retention and protection

1. Your personal data will be kept for the following periods:
   - if we enter into a contract with you: for its duration and after its completion, in connection with our legal duties resulting from generally applicable legal provisions (e.g. tax),
   - necessary for us to pursue claims in connection with the conducted activity or defending against claims directed against us, on the basis of generally applicable laws, including limitation periods for claims specified in generally applicable laws (including the Polish Civil Code and Tax Ordinance),
   - in the case of processing for marketing purposes – in the case of data processing on the basis of a legitimate purpose – until the opposition to such processing; in the case of data processing on the basis of consent – until its withdrawal,
   - in the case of consent to the processing of data for a given purpose (i.e. newsletter) – until withdrawal of consent,
   - for the purpose of accountability, i.e. to prove compliance with provisions regarding the processing of personal data, they will be kept for the period in which we are obliged to preserve data or documents containing them to prove the fulfillment of legal requirements and enable verification by public authorities.
2. We use various measures technical and organizational measures to ensure the security of personal data being processed, in particular preventing unauthorized third parties from accessing them or processing them in violation of generally applicable laws, preventing personal data loss, damage or destruction. These include: restricting access to data to authorized employees and officers, appointment of a Data Protection Officer, implementing physical, electronic and procedural safeguards and using trusted vendors of third-party services.

V. Transfer of personal data

1. The personal data entrusted to us is made available to entities that provide us with consulting services, legal assistance, tax, accounting, IT and cloud services. These data can also be transferred to state authorities or other authorized entities according to Applicable laws.
2. In some cases, the recipients listed above may reside in a country outside of the European Economic Area (EEA), i.e. in the United States of America. Your data will be transferred to the USA only in accordance with Applicable laws, with appropriate safeguards in place and only to Privacy Shield certified vendors (according to the EU Commission Decision 2016/1250) or by using standard contractual clauses adopted by the European Commission (EU Commission Decision on standard contractual clauses for the transfer of Personal Data to processors established in third countries under Directive 95/46/EC (the “Model Contract Clauses”), or based on other applicable transborder data transfer mechanisms.

If you are located in the EEA, you may contact us if you require a copy of the safeguards which we have put in place to protect your Data transferred outside of the EEA and your privacy rights in these circumstances.

You may also learn more about:

- Privacy Shield Program: https://www.privacyshield.gov/Program-Overview and https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en
- EU Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087 and https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

VI. Your rights

1. You have certain rights relating to your data, subject to local data protection laws. Depending on the applicable laws, these rights may include:

Your right	What we do to protect your legal rights?
The right to be informed	You have the right to request that we disclose certain information about our collection and use of your personal data. After receiving your verifiable request, we will disclose to you in particular the categories of data we collected about you, the categories of sources for the personal data we collected about you, our purpose for processing the data and the categories of third parties with whom we share the data.
The right of access	You can request a copy of your data that we hold about you by contacting us.
The right to rectification	You may contact us if any of your data is not accurate or not complete and request that we update or rectify your data.
The right to erasure	You have the right to the erasure of your data without undue delay (so called 'right to be forgotten') in circumstances described in Applicable laws, including the following: the data is no longer necessary in relation to the purposes for which they were collected or otherwise processed; you withdraw consent to consent-based processing; the processing is for direct marketing purposes; the data has been unlawfully processed. However, there are certain general exclusions of the right to erasure, which include situations where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; or for the establishment, exercise or defense of legal claims.
The right to restriction processing	You have the right to restrict the processing of your data in circumstances described in Applicable laws, including the following: you contest the accuracy of the data; processing is unlawful but you oppose erasure; we no longer need the data for the purposes of our processing, but you require data for the establishment, exercise or defense of legal claims; you have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store your data. However, we will only otherwise process it: with your consent; for the establishment, exercise or defense of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important public interest.
The right to data portability	We are obliged to enable you to obtain and reuse your data for your own purposes in a safe and secure way without it affecting the usability of your data. This right only applies to personal data that you have provided to us as the data controller. The data must be held by us by consent or for the performance of a contract and the processing is carried out by automated means.
The right to object (opt-out right)	In some circumstances, you have the right to object to the processing of your personal data where, for example, your data is being processed on the basis of legitimate interests and there is no overriding legitimate interest for us to continue to process your data, or if your data is being processed for direct marketing purposes.
The right to withdraw consent	If you have given your consent to process your data but changed your mind later, you have the right to withdraw your consent at any time, and we are obliged to stop processing your data unless we have another valid legal ground for further processing. The withdrawal of consent does not affect the compliance of the processing which was made on its basis before the withdrawal of consent.

The right to complain	You have the right to lodge a complaint with the competent supervisory authority. In Poland, the supervisory authority is the President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych).

2. To exercise the rights described above, you may submit a request to us (see point VII). We may check if the person requesting a specific operation on personal data has the right to do so, by requesting additional data allowing to verify the identity of the person who makes the request. The request should be described with sufficient detail to allow us to properly understand, evaluate and respond to it.

VII. Contacting us

1. You may contact our Data Protection Inspector – Mr. Tomasz Kowalski, by phone +48 605 290 285, in writing to the address of the company: Plac Na Groblach 21, 31-101 Kraków, or by sending an e-mail to hello@secfense.com.