# PRIVACY POLICY
# of
# STRIGA TECHNOLOGY

Last updated: 4 January 2023

This is the privacy policy (**"Policy"**) of Striga Technology OÜ, a company registered in the Republic of Estonia (Member State of the European Union), registry code: 16298772, address: Sepapaja 6, Lasnamäe linnaosa, 11415 Tallinn (**"Striga"**, **"we"**, **"us"**, and **"our"**).

When we speak of **"you"** and **"your"**, we mean the natural person (data subject) whose personal data we process under this Policy or, where the context so suggests, a person/entity who provides us personal data.

The Policy has been prepared and published in accordance with Articles 12, 13, and 14 of the **"GDPR"**[1]. The Policy includes information on the natural persons whose data we process as well as why and how we collect, store, process, and transfer personal data to third parties. This Policy does not cover the processing of our employees' personal data.

The Policy will also provide information about the data storage periods and your rights concerning your personal data and our data processing activities.

This Policy is published on our website www.striga.com. The Policy is complemented and to be read together with Striga's Cookie Notice, also available on our website.

If you have any additional questions about our data processing practices, or if you wish to exercise your rights under this Policy and/or applicable law, please contact us via legal@striga.com, and we will get in touch with you shortly.

## 1. WHOSE PERSONAL DATA WE PROCESS

1.1. We may process your personal data if you visit our website, write, email, call, or meet (either physically or virtually) us or our employees/representatives, apply to become our customer, cooperation partner, or employee, use our services, offer or sell goods or services to us, or otherwise interact or cooperate with us in the course of our day-to-day operations, or if we offer our services to you.

1.2. We may also process your personal data if another person/entity, in situations referred to in clause 1.1 above, has provided us with your personal data and/or where we have lawful grounds to process your personal data.

*E.g., if a company you work for provides us with your personal data in the course of cooperating with us, we may process your personal data in accordance with this Policy.*

1.3. When we receive your personal data from another person/entity, we presume that the person/entity providing your personal data has a valid legal basis for doing so. However, we exercise care and diligence in processing the personal data received from other persons/entities; and if we have reasonable grounds to believe that another person/entity may

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

have provided us with your personal data in violation of your rights, we will take measures that are appropriate in each particular case in light of our rights and obligations under applicable law. To protect your rights, you must notify us as soon as possible if you believe that a third party has illegally provided us with your personal data, but, just as importantly, you should require the third party to terminate the violation of your rights.

1.4. Whenever you provide us personal data of another person, we presume that you have a valid legal basis to provide us with such data. However, upon our request, you are required to provide proof in a form we accept about your right to provide us personal data of a third party and, where relevant, the third party's acceptance of this Policy. Failure to comply with the above may result in legal action brought against you and potential legal liability to the data subject, the competent authorities, and/or, where relevant, Striga.

## 2. HOW WE COLLECT PERSONAL DATA

2.1. We may collect personal data from you directly, such as when you apply to become our customer, submit a request or an application, use our services, or otherwise interact with us.

2.2. We may collect your personal data through automated means, such as tracking your use of our website, application, and services. Please also refer to the Cookie Notice.

2.3. We also collect your personal data from third parties who are either entitled or required to disclose that information to us under applicable law, such as:

2.3.1. third parties you have a legal or personal relationship with, your transaction partners, and other parties related to you;

2.3.2. our cooperation partners and third-party service providers (*e.g.,* our Co-Brand Partner through whom you access our services, card issuer, vIBAN provider);

2.3.3. financial institutions and other virtual asset service providers;

2.3.4. public and private registers;

2.3.5. other public sources (public blockchain, social media profiles, media articles);

2.3.6. state and local authorities, courts.

## 3. WHICH PERSONAL DATA WE PROCESS

3.1. Generally, we process the following categories of personal data:

| *Categories of personal data* | *Examples* |
|---|---|
| Personal identification information | Name, gender, age, unique ID, identity document details, residence permit data, facial image on photo or video, signature, personal code, place of birth, date of birth, citizenship(s) |
| Contact details | Email address, phone number, home or work address, information on a utility bill, or another document serving as proof of address |
| Professional activity data | Employer's name or place of work, field of activity, educational background, tenure, experience |
| Regulatory status data | PEP status, sanction status, and other relevant information available in open source |
| Tax data | Tax residence and related documentation, tax identification number (TIN), tax declarations and payments, tax arrears |
| Financial data | Inbound and outbound payments forecast, income, expenses, commitments, agreements concluded and terminated, service fees, breach of contract, account |

| | |
|---|---|
| | balance, source of wealth, source of funds on the account, documents about transactions, data on other accounts |
| Payment instrument data | Bank/payment account number, vIBAN, card details (type, term of validity, status, limits, number), virtual asset wallet/account identifier, data about operations with the payment instrument (*e.g.*, suspension, seizure) |
| Transaction data | Type of transaction (fiat currency, virtual asset), currency, time, amount, data on counterparties, data on contested or canceled transactions, blockchain addresses, public keys |
| Customer activity data | Status, the purpose of the business relationship, records of our communications with you, log-in and authentication data, activity in the use of the services, services used, inquiries and complaints |
| Online identifiers | Type of device, device identifier, IP address, location, browser data |
| Data on offenses | Data on committed offenses or suspicion of offenses, punishment |
| Right of representation data | Data on a power of attorney or another authorization document |
| Third-party relationship data | Relationships with parties involved in the provision of services (payment counterparty, company, beneficiary), relationships with politically exposed persons or sanctioned individuals/entities |
| Data on official inquiries | Data related to inquiries of competent state and local authorities, courts |

3.2. We may also process other personal data available on the documentation, communication, or other sources provided to us or collected by us for the purposes set out in this Policy.

## 4. WHY WE PROCESS PERSONAL DATA

4.1. We generally process your personal data based on your consent, the legal relationship between you and us, applicable statutory requirements, and our legitimate interests, as applicable.

4.2. We mainly need to process your personal data to provide our services to you, that is, to enter into a business relationship with you and fulfill the agreement(s) entered into between you and us. Such processing includes the necessary steps we need to take before we decide to enter into an agreement with you (such as identifying you and verifying the accuracy of the data you provide) in accordance with applicable laws and regulations. While in a business relationship, we also process personal data for administering the customer relationship and processing support requests and complaints.

4.3. As a highly regulated entity, we are also required to process personal data to comply with the applicable AML/CFT and sanctions laws and regulations, including the obligations to apply due diligence measures and monitor the business relationship. Furthermore, we process your personal data to comply with our other statutory obligations (*e.g.*, auditing, financial reporting). We may process your personal data for these purposes regardless of your consent, but where we rely solely on statutory obligations as the basis for processing your personal data, we undertake not to process such personal data for other purposes.

4.4. Processing of your data may also be based on our legitimate interests, regardless of your consent. You may contact us if you want more information about our legitimate interests in processing your personal data. For example, we have a legitimate interest in processing your personal data in the following situations:

4.4.1. We process the data received from your use of our services to improve our website and product offering, conduct market analysis and research, education and training programs for our staff, and plan and forecast business activities.

4.4.2. We process personal data for risk management purposes. We have a legitimate interest in and are required by applicable regulatory requirements to hedge and manage the risks we encounter in our day-to-day operations.

4.4.3. If we're being offered to buy products or services or enter into any other sort of cooperation (including if you apply for a job with us), we may process personal data to do our due diligence and take measures to hedge regulatory, reputational, legal, financial, and other risks.

4.4.4. We have a legitimate interest in ensuring protection against legal disputes and exercising and defending our legal rights in court or extra-judicially, and we may process your personal data for that purpose.

4.4.5. We may also process personal data for quality assurance and proper and secure operation of our platform.

4.5. We may use profile analysis and/or automated decision-making if necessary for entering into a business relationship with you or allowed/required by applicable law (*e.g.*, AML/CFT and sanctions laws and regulations).

## 5. TRANSMISSION OF YOUR PERSONAL DATA

5.1. We may forward your personal data to the following categories of third parties:

5.1.1. financial institutions, virtual asset service providers, and other cooperation partners and organizations related to the services we provide or make available (such as our banking partners, the card issuer, vIBAN provider, our Co-Brand Partner through whom you access our services, the virtual asset service provider of a counterparty to a virtual asset transaction, etc.) – to fulfill the agreement we entered into with you and, in some cases, to comply with our legal obligations (such as those arising from applicable AML/CFT and sanctions laws and regulations);

5.1.2. third-party service providers (*e.g.*, server and cloud service providers, website analytics service providers, mail and other communication service providers, other providers of information technology services, identification, screening, monitoring, and accounting service providers, etc.). We transmit your data to these parties to be able to provide our services and fulfill the contract with you, as well as to comply with our legal obligations (such as data retention, AML/CFT, and sanctions laws and regulations);

5.1.3. attorneys, auditors, financial consultants, and other professional consultants and advisors – to pursue our legitimate interests (such as defending our legal rights) as well as to comply with our legal obligations (such as auditing);

5.1.4. other third parties upon your consent (such as your authorized representative, adviser, or another third party you have contacted and involved in the matters between you and us);

5.1.5. competent authorities (such as investigative bodies, the Tax and Customs Board, Financial Intelligence Unit) and courts – to comply with our legal obligations.

5.2. Whenever a recipient is not a separate data controller but our data processor, the processor shall not have an independent right or legal basis for processing personal data, and your data is processed on behalf of and under the responsibility of Striga. We exercise diligence and care in selecting our data processors and ensure that they process personal data in accordance with our instructions, generally recognized security standards, and applicable requirements of the data protection legislation. However, when we transmit your data to data controllers (*i.e.*, persons or organizations who themselves decide what data to process and why), they are processing your data on behalf of and under the responsibility of themselves.

5.3. Generally, we process your personal data within the European Economic Area (**"EEA"**) and do not transfer your data outside of the EEA. We may transfer your data outside of the EEA if the European Commission has determined through an adequacy decision that the country in question offers an adequate level of data protection.

5.4. In some limited instances, we may need to transfer your personal data to countries outside of the EEA or not covered by the European Commission's adequacy decisions. Whenever we transfer your personal data to these countries, we rely on an appropriate legal basis and/or apply additional safeguards, such as concluding an agreement with the recipient, which includes the Standard Contractual Clauses regarding the transfer of data to third countries as adopted/approved by the European Commission.

## 6. SECURITY AND DATA RETENTION

6.1. We take commercially reasonable technical and organizational precautions to prevent the loss, misuse, or alteration of your personal information. Accordingly, we store all the personal information you provide on secure servers.

6.2. We also use suitable legal, technical, and organizational security measures to protect your data against accidental or intentional manipulation, partial or complete loss, destruction, or unauthorized access by third parties. Our security measures are continuously improved in line with technological developments.

6.3. Please note that no transmission of information via email or other telecommunication channels or your access to our platform and services through the internet could be fully secured. Therefore, you should take due care when you are accessing our platform and services via internet or sharing confidential information via e-mail or other telecommunication channels.

6.4. We do not retain personal data for longer than necessary to achieve the processing objectives, including, as applicable, to provide the services to you, comply with our legal obligations, and maintain the protection of our legal rights and legitimate interests.

6.5. Generally, we retain personal data for the following periods:

6.5.1. data relating to legal agreements and legal relationships – 10 years after the due date of the latest event potentially giving rise to a legal claim;

6.5.2. billing information – 7 years;

6.5.3. CVs and other information provided by job applicants – 1 year;

6.5.4. other information – 5 years as of collecting the data or 5 years after the termination of the business relationship, as relevant.

6.6. Where the law prescribes specific limitation periods or data retention terms, we may retain personal data for a different time than set out above.

6.7. Upon the expiry of the retention period, we will erase your personal data or anonymize it irreversibly.

## 7. YOUR RIGHTS

7.1. You have the right to know whether we process your personal data, receive a copy of your personal data, and demand corrections to your personal data due to inaccuracies or changes in your personal data. Your personal data is available to you through our platform, but you also have the right to contact us to access the personal data we process. However, please note that your right to access the personal data we process may be limited by legal acts, others' privacy rights, and our rights and other obligations (such as protection of business secrets, confidentiality obligations).

7.2. You may also demand the deletion of your personal data if we lack the right to process such data or if we process the data solely based on your consent and you withdraw your consent. Note that this right may be overridden by our right or legal obligation to process such data (compliance with laws and regulations, performing a contract, pursuing our legitimate interests).

7.3. You can withdraw your consent for the processing of your personal data. After you have withdrawn your consent, we shall no longer process your data for the purpose you consented to.

7.4. You may object to the processing of your personal data, including the performance of profile analysis, and if we process the data based on our legitimate interest. Upon receiving your objection, we shall not process your data unless our interests outweigh the potential effect on your rights (*e.g.*, compliance with legal obligations).

7.5. You may require that we terminate the processing of your personal data if we don't have a legal basis to process your data.

7.6. To exercise your rights, please contact us via the contact details provided in this Policy. In certain instances, determined in applicable legislation, we may require a fee before processing your application for exercising your rights as a data subject, which we will notify you before processing your application.

## 8. PROTECTION OF YOUR RIGHTS

8.1. You may contact us in connection with queries and withdrawal of consent, as well as to exercise your rights and lodge complaints relating to processing your data.

8.2. Striga's contact details: address Sepapaja 6, Lasnamäe linnaosa, 11415 Tallinn, email legal@striga.com.

8.3. In the event of a violation of your rights, you also have the right to lodge a complaint with the Estonian Data Protection Inspectorate (www.aki.ee, info@aki.ee, Tatari 39, 10134 Tallinn) or a court of your jurisdiction.

## 9. FINAL PROVISIONS

9.1. We reserve the right to amend this Policy at any time unilaterally. We will notify you of amendments to the Policy on our website and/or, at our discretion, through a communication channel you have provided us.

9.2. This Policy applies to all personal data we process (except for our employees' personal data), including personal data collected before the entry into force of the Policy.

9.3. This Policy does not extend to any external links that lead to services or websites of third parties. These third-party websites and services are subject to the terms and conditions and the privacy policy of the respective provider.