PRIVACY POLICY

Last updated on April 6, 2020

Svort Inc., registered at 1013 Centre Road, Suite 403-B, Wilmington, DE, 19805, USA ("Controller", "We", "Ours") respects your privacy. Please read this Privacy Policy carefully as it describes Our methods of handling your data that are processed and collected when you visit our website www.svort.io, as well as demo.svort.me and onboarding.svort.me, and the use of Our Products (the SDK particularly and the Svort System in general) on other websites where this Privacy Policy is posted.

You agree to the Terms of Use and this Privacy Policy before registering by taking action on our website or starting to use our Product (SDK). Our Privacy Policy may be updated at any time to reflect changes in our practices or the laws that govern it. Therefore, each time you use our Product (SDK), you agree that we collect, use, store, transfer and disclose the information you provide as described in this Policy. Please check this page periodically for the latest updates.

If you do not agree with this Privacy Policy, please do not use the Product (SDK) or take action on our websites.

1. DEFINITIONS

"Svort System" - Identity and Access Management System based on anonymous neural biometrics.

"SDK" (Product) - a set of libraries (modules) that implement various (combined) functionality of Svort System, which itself is an access management system based on biometric parameters of a human face.

"Service" - the final service (functionality SDK), which is accessed, as well as support services.

"Account" - a user account in the Svort system or on a website with a domain belonging to Svort.

"Client" - means any organization that uses the Service.

"User" ("you", "your") - means the end user of the Svort product, a client or an employee of the Svort client.

"End device" - a device (phone, tablet, computer, etc.) on which Svort product is used.

"Identification" - procedure of recognizing a user by his or her identification data (e-mail (login)), or by his or her face in order to grant or restrict access, as well as to collect analytical data.

"Authentication" - procedure of proving a user’s right to get access to his data by checking that he or she is the person he or she pretends to be.

"Verification" - process of verifying user's identity and his\her identity documents. Comparison of facial biometric data that the user presents in front of the camera with identity photos from the documents.

"Personal Data" - means any data, including Confidential Data: about an identified or identifiable person and received by Svort Inc. in connection with the Service.

"Processing of Personal Data" - means any manual or automated action in relation to personal data, including: collection, receipt, recording, systematization, storage, clarification (updating, modification), extraction, use, transfer (distribution, provision, access), depersonalization, blocking, deletion, destruction of personal data.

"Controller" (Svort Inc.) - a person or organization that independently or together with others determines the purposes and means of processing Personal Data.

"Processor" - means any natural or legal person, public authority, institution or other body processing Personal Data on behalf of the Controller.

Unless the context implies otherwise:

- words used in the singular form include the plural form and words used in the plural form include the singular form;
- any words following the terms "including", "include", "in particular", "for example" or any similar expression shall be construed as illustrative and shall not limit the meaning of words, descriptions, definitions, phrases or terms preceding those terms.

2. HOW SVORT SYSTEM WORKS

Svort System is Identity and Access Management System that provides the Clients with proprietary SDK to satisfy all the Clients' necessities with regard to biometric access management and control taking into account all the current challenges about privacy and users' data.

SDK (Product) - is a neural-biometric access management system, that is based on anonymous biometrics algorithms and that does not collect or store any photos and videos references and enables to only store depersonalized code. We process the biometric data of your face and train the neural network to recognize you as a User/Person. In this way we implement the concept "you are the key". The biometric data about our Users is not stored on our resources or on the resources of our Customers.

3. DATA THAT WE MAY COLLECT WITHOUT YOUR CONSENT

We may collect without your consent the following data:

Custom actions about how you interact with us, including the content that you have viewed and interacted with.

We may automatically collect information about your computer or another device, for example:

- your IP-address;
- browser type;
- links/exits pages;
- operating system.

4. DATA THAT WE CAN COLLECT IF YOU PROVIDE IT TO US

We can collect the following data provided that you have given it to us:

- name;
- e-mail address;
- phone number;
- name of your company.

5. WHAT DATA WE KEEP AND FOR HOW LONG

We retain the collected data for the period of time that meets our business and development needs, and only for the purpose of our own ability to perform our services, and as a benchmark to ensure continuous product integrity and improvement.

6. DATA EXCHANGE

We may disclose Personal Information provided by our Customers and Users for our Service to the following persons and in the following cases:

- Business partners and service providers that we use to maintain and improve our Service.

- if required to do so by law or legal process and/or a competent regulatory authority.

- in response to legitimate requests from government authorities, including national security, public interest or law enforcement requirements.

- when we believe in good faith that disclosure is necessary to protect our rights, your safety or the safety of others, to investigate fraud or to respond to a government request.

- to another third party with your explicit, prior consent.

In such circumstances, we will inform the recipient directly that the data transferred is confidential.

We will not share your data with third parties who are deemed unable to protect the information they receive from customers and potential customers.

Svort Inc. also reserves the right to transfer or disclose Personal Data in case of an audit or if the company sells or transfers all or part of its business or assets (including in the event of a merger, acquisition, joint venture, reorganization, dissolution or liquidation) and in case the Personal Data we have on Our Customers will be among the assets transferred to the buyer or acquirer.

We can not provide all services on our own. We must therefore share the information collected with third parties for the purposes described in this Privacy Policy.

Our third party providers to whom we provide your data may be located in countries where data protection and privacy policies may differ from those of your country and provide even lower levels of protection. You acknowledge such transfer and processing of your data outside of the country where our data protection and privacy practices may differ from the laws of your country and offer even lower levels of protection. In order to protect your interests when transferring your personal data outside the country, we will make data protection agreements with all data recipients

outside the country, which are necessary to ensure at least the same level of security as set out in this Policy.

All third parties who are provided with your data by us will receive only the minimum amount of data reasonably necessary to enable them to provide us and therefore you with their services. The use of the information provided by such third parties is strictly limited to the processing purposes set out in this Policy and will not be permitted for any other purposes. All third parties with whom we share your data are required to protect such data in accordance with all applicable laws and regulations and in the same way as we protect them.

Upon your request, we may transfer the data processed in respect of you to the email address you provide us with within 30 calendar days.

7. TRACKING SITE ACTIVITY AND SDK

We may use cookies, pixels, beacons, scripts and other similar technologies (collectively referred to as "cookies") to recognize your browser, operating system or device, to learn more about your interests and intentions, to provide you with features and services, or for additional purposes including:

- repeat visitor recognition;
- tracking certain preferences, such as language and country of origin;
- conducting research and diagnostics to improve our offerings;
- preventing fraudulent activity;
- improving security;
- delivery of relevant content;
- reporting, measuring and analyzing our sites and resources.

If you block or reject our cookies, you may not be able to receive certain content or use certain features of the site.

Third parties may also set cookies when interacting with our products if they receive approval, or if they have entered into an agreement with the Controller or your consent. Third parties include search engines, measurement and analysis service providers, social media and advertising companies.

You can manage cookies in your browser through your browser or device settings.

8. LEGAL BASIS FOR PROCESSING YOUR DATA

You expressly consent to the processing of your personal data for the specific purpose of identifying you as a proper user and to the fact that you are alive and present in reality when you register or log in and test our product.

The processing of your data is necessary to protect your vital interests. Our Policy and work processes are designed to ensure that no other person has unauthorised access to your confidential information.

The processing of your data is a necessary part of the services provided by the organization to you or to the Client to whom we provide our services.

Svort inc., complies with the EU GDPR and U.S. D.O.C. Privacy Shield Policy with respect to personal data that the company receives from its customers or their users in connection with the use of the Svort System and the SDK, without excluding any of the other provisions of this Privacy Policy.

9. COMPLIANCE WITH GDPR

We collect the following data:

Your IP (Internet Protocol) address, which is a set of numbers that determine the location of hardware connected to a network, including the Internet. An IP address allows a device to communicate with other devices over an IP network, such as the Internet. By itself, it cannot provide user identification. It is important to us because it indicates where our software is used in the world, which helps us better prepare the product for distribution and daily use.

E-mail address (login): We collect emails in case we need to contact you, and to identify and verify that you are a registered user.

9.1 OBJECTIVES OF POSSIBLE USE OF DATA

To determine which products or services are most relevant to you.
To respond to requests for services or product information.
To better focus the marketing efforts.
To help with market research.

9.2 ENSURING ACCESS AND MANAGEMENT OF YOUR DATA

You control your data. You may do the following at your discretion:
- request the deletion of your data ("Right to be forgotten");
- request a copy of what data is being collected;
- revoke your consent to data processing at any time;
- make a complaint to the authority in your area.

For this purpose, please notify founders@svort.io by email, which you specified during registration in the system and we will reply to you within 10 working days.

10. U.S. D.O.C. Privacy Shield Policy

The policy of Svort Inc. complies with the requirements of EU-US privacy protection, within the limits established by the U.S. Department of Commerce regarding the collection, use and storage of Personal Data transferred from the European Union and the United Kingdom, as further described in the "Scope of Application" section below. This Privacy Policy describes our commitment to the Privacy Principles ("Principles") and our practices in implementing them. If there is any inconsistency between this Privacy Policy and the Privacy Principles, the Privacy Principles will apply. To learn more about the Privacy Principles, please visit the Department of Commerce Privacy Protection website.

10.1 TYPES OF PERSONAL DATA COLLECTED

Svort Inc. places and processes customer data, including any personal data contained therein, as directed and in accordance with the instructions of the customers. We also collect several types of information from our Clients, including:

Information and correspondence that our Clients and Users send us through our Service.

Information that we receive from our business partners through the use of the Service by our Clients and Users or through services provided by our business partners on their behalf, including configuration of the Service.

Information related to Users' use of the SDK, including geographic location data and information about Users' Devices and operating system identification, login credentials, language and time zone.

In addition, Svort Inc. may collect general information about its customers, including the name and address of a customer company, credit card information and contact information of a customer representative ("General Information") for billing and contracting purposes.

10.2 PURPOSES OF COLLECTION AND USE

Svort Inc. may use personal data provided by our customers and users as necessary to provide the Services and the Service, including updating, expansion, security and maintenance of the Services, and fulfill contractual obligations of Svort Inc. for its customers and users. Controller also receives general information in connection with the provision of Services and maintenance of relations with his or her customers and users.

10.3 RIGHT OF CHOICE

In accordance with the Principles, Svort Inc. (i) discloses your personal data to third party operators, or (ii) uses your personal data for purposes that are substantially different from those for which the personal data were originally collected or subsequently authorized for transmission by the client or user. To the extent required by the Principles, Svort Inc. will also obtain consent to participate in certain uses or disclosures of Confidential Data. Unless we offer our customers and users an appropriate choice, we will only use Personal Data for purposes that are substantially the same as those specified in this Policy.

Svort Inc. may disclose personal data of customers and users without offering an opportunity to opt-out of their use, and may be required to disclose personal data in accordance with Sections 9 and 10 of this Privacy Policy.

11. RESPONSIBILITY FOR DATA TRANSFER

Svort Inc. is in compliance with the Privacy Principles regarding liability for subsequent data transfers. We remain responsible in accordance with the Principles if

the recipients of the data in their further transmission/receipt process Personal Data in a manner inconsistent with the Principles or this Policy, unless the company proves that it was not responsible for the event that caused the damage.

12. DISPUTE RESOLUTION RULES, QUESTIONS AND COMPLAINTS

If you have any inquiries regarding your personal information or any inquiries in connection with this Privacy Policy, please contact us at founders@svort.io.

If you believe that our collection, use, disclosure and/or storage of your personal information violates any applicable data protection legislation that we are required to comply with, please contact founders@svort.io. We will consider your request within 30 business days and provide you with a response.

If you contact us or complain to us, you agree to the negotiation procedure. If you do not reach a compromise or if your appeal is not satisfied within the prescribed period of time, you have the right to appeal to the competent state authority with such a complaint or demand, in accordance with applicable law.

The intermediary, or Customer, or User, may also contact the U.S. Federal Trade Commission, which has investigative and enforcement powers with respect to Svort Inc. Under certain circumstances, Clients and Users may refer to binding arbitration to address complaints about our compliance with the law in accordance with the Principles.

13. CHILD PRIVACY PROTECTION

We deliberately do not collect or process personal data from children under the age of 13, and you must be 13 years or older to use the Product.

If you are a parent or legal guardian and believe that your child under the age of 13 has provided his or her personal data or other data without your consent, authorization or permission, please notify us immediately by email: founders@svort.io and we will take immediate steps to remove the data processed in relation to your child from our servers, cease the use of such data and inform any other party who may have access to such data.

14. ENSURING SECURITY

We provide access to the information we have about you to employees who in our opinion should come into contact with that information in order to provide the Services to you for the purpose of performing their official duties. These employees are bound by confidentiality obligations and may be prosecuted if they fail to comply with these obligations.

We will take all reasonably necessary steps to ensure that your information is processed securely in accordance with this Privacy Policy.

We will retain and use information that is necessary to comply with our legal obligations, resolve disputes and enforce our agreements. If you have any specific security questions or for more information, please contact us at founders@svort.io