

PRIVACY NOTICE

1 INTRODUCTION

We, Critical Security, UAB (hereinafter - CS), take care of the security of your personal data (personal data means any information that is related to an identified or identifiable living person, such as name, surname, address, e-mail address, Internet behavior website etc.). The privacy notice below is intended for all persons who contact, work, seek to apply or otherwise cooperate with CS, use CS services or in any other way submit their personal data to CS.

This privacy notice is created based on valid legal acts and recommendations, such as the General Data Protection Regulation (hereinafter - GDPR), the Law on Legal Protection of Personal Data, the guidelines of the State Data Protection Inspectorate (hereinafter - SDPI). The purpose of the privacy notice is to indicate the rights and obligations of the data subjects, as well as other information that must be provided in accordance with the GDPR.

The Company's services are not intended for children (ie, persons under the age of 14).

2 DATA CONTROLLER

Critical Security UAB, legal entity code: 300646885, registered office address: Saulėtekio al. 15-1, LT-10224 Vilnius, Lithuania is the data controller of the personal data indicated in this privacy notice (the concept according to the GDPR).

3 DATA PROTECTION OFFICER

CS does not have the obligation to appoint a data protection officer in accordance with Section 4 Article 37 of the GDPR. Personal data issues can be contacted by e-mail. by mail: dpo@critical.lt.

4 WHEN DO WE PROCESS YOUR DATA?

Data is processed when, for example:

- You provide the data yourself, for example, in order to get a job, browsing the website or social networks, requesting e-mail. by mail, by subscribing to the newsletter;
- The data is provided by the company where you work or to which you otherwise belong and which has a contractual or legal relationship with CS;
- By participating in public tenders;
- Data is generated when you use our services;
- after requests from CS on the basis of legitimate interest from (e.g. social services, credit rating companies, public registers, etc.);
- We receive data from other sources who pass it on following instructions from authorities, etc.;
- We receive data from public sources when you publish it yourself or a company/institution you represent

5 WHAT PRINCIPLES DO WE FOLLOW WHEN PROCESSING YOUR DATA?

The processing shall be carried out on the basis of the following principles specified in Article 5 of the GDPR:

- the principle of lawfulness, fairness and transparency;
- the principle of purpose limitation;
- the principle of data minimization;
- the principle of accuracy;
- the principle of storage limitation;
- the principle of integrity and confidentiality.

The Institution takes appropriate technical and organizational measures in order to ensure that it is able to meet the obligation under the accountability principle.

6 HOW DO WE PROTECT YOUR DATA?

In order to protect your data, we have taken organizational and technical measures that are designed to properly regulate and manage your data. Such measures include, but are not limited to: SDPI guidelines, measures specified in the information protection management standard ISO 27001 / ISO 27002, EDPS (European Data Protection Supervisor) and WP29 (Working Party 29) guidelines and recommendations.

Organizational personal data protection measures include, but are not limited to, the following measures: personal data processing rules, data subject rights implementation procedure, risk assessment, information security incident management procedure, information security documents, register of personal data processing activity records, data processing agreements with data processors, various personnel procedures, continuous employee training, etc.

Technical personal data protection measures are implemented based on information security documents. With the help of data processors, a data processing agreement is always concluded.

7 WHAT DATA DO WE PROCESS ABOUT YOU?

CS processes your personal data as a data controller:

Purpose of processing personal data	Personal data is processed	How long are personal data stored?	Legal basis for processing personal data
Conclusion and execution of CS contracts with legal entities	Legal entity representatives: name, contact information (phone number, e-mail address, etc.), data of the represented legal entity, information on the contract	10 years from the end of the contract	Legal obligation, Article 6(1)(c) GDPR
CS contracts with natural persons	Representatives of a natural person: name, contact information (phone, e-mail address, etc.), individual activity/business license no., date of birth, contract information	10 years from the end of the contract	Legal obligation, Article 6(1)(c) GDPR

Selection for vacancies	Candidate: first name, last name, e-mail address, phone number, salary expectations, when you can start working, resume and other information provided by the candidate, employment agency / partner / job exchange information	Until the end of the selection. With the consent of the data subject - up to 3 years	Consent, Article 6(1)(a) GDPR Conclusion and execution of the contract, Article 6, paragraph 1, subparagraph 2 GDPR
Administration of projects financed under the European Union or similar	Name, surname, position, workplace, e-mail email address, phone number, LinkedIn account link, salary details	10 years from the end of the contract	Legal obligation, Article 6(1)(c) GDPR
Direct marketing	Name, surname, e-mail, statistical information	Until withdrawal of consent	Legitimate interest, Article 6(1)(f) GDPR Consent, Article 6(1)(a) GDPR
Administration of the contact database of potential business partners	Name, surname, contact information, information about the company, other data provided by the potential client/partner	Until objection Until withdrawal of consent	Legitimate interest, Article 6(1)(f) GDPR Consent, Article 6(1)(a) GDPR
Events, seminars, webinars, trainings, hackathons, consultations and etc. organization	Participant: name, surname, phone number, e-mail, address, represented organizations data (name, address, etc.)	2 years after the end of the event/project	Consent, Article 6(1)(a) GDPR
Accountability for Europe Union funded projects	Name, surname, represented organization / company, address of the represented organization / company, contact e-mail address, photo / video material	5 years after the end of the project	Legal obligation, Art. 6 GDPR. 1c
Inquiry handling and communication	Name, surname, telephone, e-mail address, message	10 years after receiving the message	Legitimate interest, Article 6(1)(f) GDPR
Social networks LinkedIn, Github , Twitter	Data specified in the privacy policy of the social network	The terms specified in the privacy policy of the social network	Consent, Article 6(1)(a) GDPR
Publicizing CS activities	Name, surname, position, e-mail e-mail address, phone number, organization name, description	Until withdrawal of consent	Legitimate interest, Art. 6 GDPR Clause 1f Consent, GDPR 6 solution

8 SOCIAL NETWORKS AND WEBSITES

8.1 SOCIAL NETWORKS

CS operates various websites that also process personal data - generated during browsing (such as IP address, page visited, browser data, etc.), collected when ordering specialized information (e.g. market/sector reviews), through contact forms, ordering newsletters, through cookies installed on websites, are also managed in social networks. We provide detailed information about this below.

We currently have the following social media accounts:

Account	Account link	Soc . network privacy notice
CS LinkedIn account	https://www.linkedin.com/company/jsc-critical-security/	https://www.linkedin.com/legal/privacy-policy
CS Twitter account	https://twitter.com/criticalsec	https://twitter.com/en/privacy
CS Github account	https://github.com/CriticalSecurity	https://twitter.com/en/privacy

The information you provide via social media is controlled by the operator of the particular social network. CS, having access to this data, uses it only for the purpose of administering its social network accounts.

9 WHAT RIGHTS AND RESPONSIBILITIES DO YOU HAVE?

- The right to be transparently informed, as well as what rights you have. We inform you in this privacy notice.
- The right to be informed about your data being processed, as well as to find out what specific data we are processing.
- The right to data rectification and erasure. If you notice that the data is incomplete or inaccurate, you can contact us and we will examine your case. You can also request the removal of your data. We will be able to perform this action if there are no other legal acts that oblige us to store data.
- You have the right to request the restriction of data processing. For example, until we clear up the inaccuracies.
- You have the right to request data transfer.
- You have the right not to consent to us processing your data, as well as to revoke the given consents at any time.
- You have the right to object to automatic decision-making, including profiling, which has significant consequences for you. CS does not currently apply such decision-making.

Please note that in order to exercise your rights , we will have to establish your identity. Also, if the volume of the request will be large, we may request a fee for the implementation of the request.

When CS acts as a data processor, we act according to the instructions of the data controller and the provisions of the data processing agreement.

You are responsible for ensuring that the data you provide to us is accurate, correct and complete. If the data provided by you changes, you must immediately inform us about it by e-mail. In no case will we be responsible for any damage caused to you due to the fact that you have provided incorrect or incomplete personal data or have not informed us when they have changed.

Information published on CS websites, its copying, reproduction, links to it are allowed only with the written permission of CS. It can be obtained by contacting info@critical.it. This release will not constitute a transfer of any rights in the material.

10 TO WHOM AND WHEN CAN WE TRANSFER YOUR DATA?

We may transfer your personal data when:

- You have consented to the transfer;
- We must do this in accordance with the procedure provided by law, when required by the government / law enforcement institution / pre-trial investigation institution, court or their representatives, in case of suspicion of a criminal act, in the event of a dispute, e.g. tax inspectorate, registry center, financial crime investigation agency, police, competition council, criminal intelligence institutions, others;
- We use a data processor or partners for certain data processing operations:
 - o audit companies;
 - o operations, security, processes, etc. for consultants;
 - o insurance companies;
 - o for companies providing information technology services;
 - o for companies providing publicity and media services;
 - o for archiving service entities;
 - o accounting service entities;
 - o for communication service entities;
 - o entities providing physical security services;
 - o CS reorganizing or otherwise reorganizing - to interested parties;
 - o For travel organizing companies, hotels, etc.
 - o and similar operations
- And in other cases when the data recipient has a legitimate reason to process your personal data.

All your data is processed within the borders of the European Economic Community, without being transferred to third countries. If there is a need to transfer to other countries, we can rely on the decision of the European Commission on adequacy (if, based on the decision of the European Commission, an adequate level of data protection is ensured in the specific country where the data recipient is established and/or operates). Other mechanisms that ensure adequate data protection may also be used, such as standard contractual clauses enshrined in personal data protection legislation.

11 HOW CAN YOU CONTACT US WITH QUESTIONS OR TO EXERCISE YOUR RIGHTS?

If you have any questions or want to exercise your rights, you can apply in a convenient way:

- Email: dpo@critical.lt
- Postal mail to: Critical Security, UAB, Saulėtekio al. 15-1, LT-10224 Vilnius
- Visiting our headquarters at: Critical Security, UAB, Saulėtekio al. 15-1, LT-10224 Vilnius

Please note that in order to exercise your rights, we will need to identify you. If the scope of the request is unreasonable or repetitive, we may request a fee for the fulfillment of the request. Possible authentication methods:

- By presenting the document directly upon arrival at the CS and presenting the identity document to the CS employee;

- When submitting an application by post or through persons providing postal or other parcel delivery services: a copy of the document confirming the identity of the person must be submitted together with the application, certified by a notary public or in another manner established by legal acts;
- When applying by e-mail: the application must be signed with a qualified electronic signature. Signing the request with a qualified electronic signature allows the CS to properly identify the sender and ensure that the requested information or information about the execution of the requested actions (refusal to execute) is disclosed only to the person to whom it is intended

We will always try to find a solution suitable for both parties, but if our actions or inactions raise questions for you, you can contact the State Data Protection Inspectorate (more information at <https://vdai.lrv.lt>).

12 VALIDITY AND REVIEW OF PRIVACY NOTICE

We regularly review whether this Privacy Notice complies with the law and the personal data processed by CS.

We may update or change this Privacy Notice at any time. Such updated or modified Privacy Notice will be effective upon its posting on our Website or Software.

This privacy notice was last edited on 03/19/2024.