REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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 repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as the Regulation, and the Personal Data Protection Act, the Data Controller issues the following:

NOTICE ABOUT JOINT CONTROLLERS

Article 1.

These Privacy Rules (hereinafter: "the Rules") set out the rules on the collection, processing and use of personal data, as well as the rules and procedures for the protection of personal data when storing and using databases.

Article 2.

For the purposes of this Policy, the following terms shall have the meanings set out below:

1. "personal data" means all data relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, a network identifier or by means of one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual;

2. 'processing' means any operation or set of operations performed on personal data or on sets of personal data, whether or not automated, such as collection, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, dissemination or otherwise making available, aligning or combining, restricting, erasing or destroying;

3. "pseudonymisation" means the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and rganisational measures so as to ensure

that the personal data cannot be attributed to an identified or identifiable natural person;

4. "controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union law or by the law of a Member State, the controller or the specific criteria for its designation may be laid down in Union law or in the law of a Member State;

5. "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

6. 'recipient' means a natural or legal person, public authority, agency or another body to whom personal data are disclosed, whether or not it is a third party.

7. 'the data subject's consent' means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by means of a statement or a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Article 3.

When processing personal data, the Controller shall comply with the following principles:

(a) lawfulness, fairness and transparency;
(b) purpose limitation;
(c) data minimisation;
(d) accuracy;
(e) storage limitation;
(f) integrity and confidentiality;
(g) reliability.

Article 4.

Processing is lawful only if, and to the extent that, at least one of the following applies:

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
(b) the processing is necessary for the performance of a contract to which the data subject is a party or in order to take pre-contractual steps at the request of the data subject;

(c) the processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.

Article 5.

In accordance with the Regulation, children are entitled to special protection in all respects, including with regard to the protection of personal data.

In accordance with Article 19, paragraph 1 of the Act on the Implementation of the General Data Protection Regulation, children are considered to be all persons under the age of 16, and the Data Controller does not request or collect personal data from or about children without the consent of the holder of parental responsibility.

Therefore, the Data Controller will take all reasonable efforts to process any data obtained from children only with the consent of the holder of parental responsibility.

If the Data Controller becomes aware that personal data of children has been sent to them without the valid consent of the holder of parental responsibility, the Data Controller will, to a reasonable extent, endeavour to do the following:

- delete those personal data from its records as soon as possible; and
- ensure, where deletion is not possible, that such personal data is no longer used for any purpose;
- and in any event will not disclose them to any third party.

Article 6.

Data collected by the Data Controller:

First name, surname
Email address
Telephone number
Job Title
Employer

Article 7.

By this Policy, the Data Subject is informed of the processing of personal data as prescribed by this Policy, including the disclosure to third parties (recipients or processors), and is deemed to be at all times aware of this privacy policy and to fully understand and accept it.

Article 8.

Personal data is collected in one of the following ways:

Directly from the individual – data provided for the purpose of entering into or performing a contract, by creating a user account on the Controller's website, directly, via telephone conversation with the individual.

Indirectly – data that is publicly available on websites not belonging to the Controller (e.g. posts on social media, open forums), data obtained through the use of cookies, links and similar technologies.

Article 9.

The following information is provided to the data subject in accordance with Article 13 of the Regulation:

(a) the identity and contact details of the joint controllers:

1. CROZ d.o.o., Lastovska 23, 10000 Zagreb, Croatia,
croz-info@croz.net, Tel: +385 (0)1 6184831, Fax: +385 (0)1 6184833

2. CROZ DACH GmbH, Aschauer Straße 30, 81549 Munich, Germany,
dach@croz.net, Tel: +49 175 204 8013

3. CROZ DACH GmbH, AUSTRIA, Haus 539, 6236 Alpbach, Austria
austria@croz.net, Tel: +43 676 712 1720, Fax: +43 676 712 1419

(b) contact details of the Data Protection Officer: dpo@croz.net, at the address CROZ d.o.o., Lastovska 23, 10000 Zagreb, Croatia, Tel: +385 (0)1 6184831
(c) the purpose of the processing for which personal data are used, as well as the legal basis for the processing: protection of the vital interests of the data subject, for the purposes of the legitimate interests of the Controller or a third party, performance of a contract, marketing and sales activities

(d) legitimate interests of the Controller or a third party: analysis, testing, improvement of the service
(e) recipients or categories of recipients of personal data: intermediaries and/or principals and/or end users to whom the Controller provides services or the Controller's processors, as well as other recipients who are in a contractual relationship with the Controller.
(f) The Controller will not transfer personal data to a third country or an international organisation, except with your explicit consent.
(g) the period for which the personal data will be stored/the criteria for determining that period: 8 years from the date of the last contact, and if it relates to the conclusion of a contract and the provision of services within the scope of the Controller's activities – 8 years from the date of completion of the service, whichever date is later.
(h) the data subject has the right to request from the Controller access to personal data and the rectification or erasure of personal data or the restriction of processing relating to the data subject, or the right to object to such processing and the right to data portability;
(i) where the processing is based on the data subject's consent, the data subject has the right to withdraw their consent at any time without affecting the lawfulness of processing based on consent before its withdrawal;
(j) the right of the data subject to lodge a complaint with a supervisory authority;
(e) the provision of personal data does not arise from a legal or contractual obligation of the Data Controller, nor is it a necessary requirement for entering into a contract, and the data subject has no obligation to provide the personal data and there are no consequences if such data are not provided;
(f) there is no automated decision-making
(g) the data subject's data is stored on a single database shared by the joint controllers.

Article 10.

The data subject has the right of access and to obtain from the Controller confirmation as to whether personal data concerning him are being processed, and if such personal data are being processed, access to the personal data and to the prescribed information.

Where personal data are transferred to a third country or an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

Article 11.

The data subject shall have the right to obtain from the Controller the rectification of inaccurate personal data concerning him without undue delay. Taking into account the purposes of the processing, the data subject shall have the right to have

incomplete personal data completed, inter alia by means of a supplementary statement.

Article 12.

The data subject shall have the right to obtain from the Controller the erasure of personal data concerning him without undue delay and the Controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
(c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
(d) the personal data have been unlawfully processed;
(e) the personal data must be erased in order to comply with a legal obligation under Union law or the law of a Member State to which the Controller is subject;
(f) the personal data have been collected in the context of the offer of information society services.

Paragraph 1 of this Article does not apply to the extent that the processing is necessary.

Article 13.

The data subject shall have the right to obtain from the Controller restriction of processing in accordance with the conditions laid down in legislation.

Article 14.

The controller shall communicate any rectification or erasure of personal data or restriction of processing to the recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject of those recipients upon the data subject's request.

Article 15.

The data subject shall have the right to receive the personal data concerning him or her which he or she has provided to the controller in a structured, commonly used and machine-readable format and shall have the right to transmit that data to

another controller without hindrance from the controller to whom the personal data are provided, where:

(a) the processing is based on consent or on a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract
(b) the processing is carried out by automated means.

Article 16.

The data subject shall have the right to object at any time to processing of personal data concerning him or her, including profiling. The Controller shall no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for the purpose of such marketing, including profiling to the extent that it is related to such direct marketing.

Article 17.

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Paragraph 1 shall not apply if the decision:

(a) necessary for the conclusion or performance of a contract between the data subject and the Data Controller;
(b) is permitted by Union law or by law of a Member State to which the Controller is subject, which also lays down appropriate measures to safeguard the rights and freedoms and legitimate interests of the data subject; or
(c) based on the explicit consent of the data subject.

Article 18.

Taking into account the latest state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, The controller implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The Controller shall implement appropriate organisational, technical and personnel measures, depending on the level of security risk:

- minimisation of the processing of personal data
- pseudonymisation and encryption
- monitoring of processing by data subjects
- enhancing IT security
- physical security measures
- staff training on data protection
- human security, etc.

Article 19.

The security measures implemented are intended to:

- Prevent unauthorised persons from accessing the data processing system in which personal data are processed;
- Prevent persons entitled to use the data processing system from accessing personal data beyond what is necessary for their tasks and authorisations;
- Ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or transfer;
- Ensure the availability of system records for the purpose of determining who has entered, modified or removed personal data from the data processing system;
- Ensure that where processing is carried out by a processor, the data may only be processed in accordance with the instructions of the Controller;
- Ensure that personal data are protected against accidental destruction or loss;
- Ensure that personal data collected for different purposes can be processed separately;
- Ensure that personal data are not kept for longer than is necessary.

Article 20.

In the event of a personal data breach, the Controller shall without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach, notify the supervisory authority competent for the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification is not made within 72 hours, it must be accompanied by the reasons for the delay.

Article 21.

In the event of a personal data breach likely to result in a high risk to the rights and freedoms of individuals, the Controller shall communicate the personal data breach to the data subject without undue delay.

Notification to the data subject referred to in paragraph 1 is not required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures and those measures have been applied to the personal data affected by the personal data breach, in particular those that make the personal data unintelligible to any person who is not authorised to access it, such as encryption;
(b) the controller has taken subsequent measures to ensure that the high risk referred to in paragraph 1 is no longer likely to occur;
(c) it would require a disproportionate effort. In such a case, there must be public notification or a similar measure whereby the data subjects are informed in an equally effective manner.

Article 22.

Any transfer of personal data that are processed, or are intended for processing after transfer, to a third country or an international organisation shall take place only if the controller acts in accordance with the conditions of Chapter V. Regulation, which also apply to further transfers of personal data from a third country or an international organisation to another third country or an international organisation.

Article 23.

Each data subject shall have the right to lodge a complaint with a supervisory authority if the data subject considers that the processing of personal data concerning him or her infringes this Regulation.
The data subject shall have the right to an effective remedy if he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in breach of this Regulation.

Article 24.

Your personal data is collected and used solely on the basis of information you have voluntarily provided to the Data Controller, whether through established contact or otherwise.

The personal data collected is stored in electronic form, and all appropriate technical and organisational measures are applied to prevent personal data

breaches. Any emails received containing your personal data will be used by the Data Controller solely for the purpose of fulfilling your requests.

Article 25.

When using the official website, the Controller's website saves a certain amount of information, so-called cookies, or other technologies such as pixels, to your computer. Cookies serve to make the website function as effectively as possible and to improve your browsing and usage experience.

A "cookie" is a piece of information stored on a user's computer, mobile phone or tablet (hereinafter "device"), which may be delivered directly by the website you visit (first-party cookies) or in cooperation with and for the purposes of the website by a third party (third-party cookies). Cookies typically store user settings, website preferences and so on. When the user reopens the website, their web browser sends back the cookies belonging to that site. This allows the site to display information tailored to the user's needs. Cookies can contain a wide range of information, including some personal information. Such information can only be stored if the user allows it. The website itself cannot access information that the user does not permit, nor can it access any other files on the user's computer.
Temporary or session cookies are removed from the device when the web browser is closed. They are used to store temporary data.

Persistent or stored cookies remain on the device after closing the web browser. They are used to store permanent data, such as a username and password, so that you do not have to log in each time you visit a particular website.

By using and visiting the Controller's website, you consent to the use of cookies. You can also block the use of cookies, which will not affect your ability to browse the website; however, certain functionalities of the site may not be available as a result.

If you wish to disable the saving of cookies on your device, you can do so yourself, although this may have a negative effect on your use of the website.

To disable cookies, you need to adjust the settings and configurations of your web browser.

Article 26.

The purpose of cookies is, but is not limited to:

To ensure the proper functioning of the website / applications

- Proper display of content;
- Creating and remembering logins/registrations on subscription purchase pages
- Personalising the interface, such as language selection;
- Device parameters;
- Screen resolution and type;
- Website/application improvement

To collect statistical data

We collect statistical data to deliver quality content and improve the quality of our websites/apps and services, to better understand user needs and accordingly enhance the services and functionality of our websites/apps.

For advertising

We sometimes use cookies to show you adverts online for products and services that may interest you, based on your previous behaviour. Using cookies, we learn which topics interest you most and, based on this knowledge, serve you adverts. Likewise, our partners (third parties) sometimes use this information to serve you an advert that may be of interest.

All ad placements are delivered via the Google DFP advertising system. In addition to displaying ads through our own system, we also display ads through third-party systems. This is described in more detail further down in this document.

To customise services

Cookies also help us to customise our services by identifying potential issues with the website/apps and by optimising and improving features such as remembering your basket, login details or language, customising the user interface and so on.

Article 27.

The Controller's websites use Google Analytics, a web analytics service provided by Google ("Google"). Google Analytics uses a specific type of cookie, which is stored on your computer and enables the analysis of your use of our websites. The information generated by the cookie about your use of this website is generally transmitted to and stored on a Google server in the United States.

We would like to point out that on these websites, Google Analytics has been extended to include the code 'gat._anonymizeIp();' to ensure the anonymous recording of IP addresses (so-called IP masking). Due to the anonymisation of the IP address on these websites, your IP address is shortened by Google within the

territory of the European Union and the European Economic Area. Only in exceptional cases is the full IP address transmitted to a Google server in the United States and shortened there. Google has subscribed to the EU-US Privacy Shield (https://www.privacyshield.gov/EU-US-Framework)

Google uses this information on behalf of the Controller to analyse your use of these websites with the aim of compiling web activity and providing additional services related to the use of websites and the internet. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf. The IP address your browser transmits in the context of Google Analytics is not combined with other data held by Google.

You can prevent Google from recording the data generated by the cookie about your use of the website (including your IP address) and from processing this data by downloading and installing the browser add-on available at https://tools.google.com/dlpage/gaoptout?hl=en.

Third-party information: Google Dublin, Google Ireland Ltd, Gordon House, Barrow Street, Dublin 4, Ireland, Fax: +353 (1) 436 1001. Google Analytics Terms of Service: https://www.google.com/analytics/terms/gb.html, Google Analytics Overview of Security and Privacy Principles: https://support.google.com/analytics/answer/6004245?hl=en, as well as Google's Privacy Policy: https://policies.google.com/privacy?hl=en.

These websites use Google Analytics to analyse visitor traffic across devices, based on a user ID. You can opt out of cross-device tracking in your Google Account under "My information" ("My information"), "Personal information".

This website also uses Google Analytics for cross-device visitor analysis, which is carried out via user identification. You can disable cross-device tracking in your Google Account under "My data", "Personal information".
Cookies used: type B. For further information, please see the Cookies section.

Cookie duration: up to 12 months (this only applies to cookies set on this website)

Maximum data retention period: up to 26 months.

For more information on the purpose and scope of data collection and processing by the plugin provider, please refer to the privacy statements of these providers listed below.

a) Facebook Inc., 1601 S California Ave, Palo Alto, California 94304, USA; http://www.facebook.com/policy.php for more information on data collection:

http://www.facebook.com/help/186325668085084, http://www.facebook.com/about/privacy/your-info-on-other#applications as well as http://www.facebook.com/about/privacy/your-info#everyoneinfo Facebook has registered for the EU-US Privacy Shield, https://www.privacyshield.gov/EU-US-Framework.

b) Google Inc., 1600 Amphitheatre Parkway, Mountain View, California 94043, USA; https://www.google.com/policies/privacy/partners/?hl=de. Google has registered itself with the EU-US Privacy Shield, https://www.privacyshield.gov/EU-US-Framework.

Article 28.

Read more about how to manage cookies at the linked pages.

- Google Chrome
- Internet Explorer
- Mozilla Firefox
- Safari (Desktop)
- Safari (Mobile)
- Android Browser
- Opera
- Opera Mobile

Zagreb, 09.06.2026

Vjekoslav Jadrešić

President of the Management Board