

Data Processing Notice for Contracted Partners of the Data Controller

Based on Article 13 of 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 EUROVID LTD. (hereinafter referred to as the **Data Controller**) provides the following data processing information (hereinafter referred to as the **Information Notice**).

1. Data of the Data Controller

Name of the Data Controller:	EUROVID LTD.
Tax number:	24129819-2-03
Registered office of the Data Controller:	6237 Kecel, Mozgó street 61-65.
Person acting on behalf of the Data Controller:	Frida Vida CEO
Electronic contact of the Data Controller:	marketing@eurovid.hu

2. Laws Governing Data Processing

The following laws apply to data processing:

- Regulation (EU) 2016/679 of the European Parliament and of the Council 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) (hereinafter referred to as **GDPR**),
- Act CXII of 2011 on the Right to Informational Self-Determination and on Freedom of Information (hereinafter referred to as **Infotv.**),
- Act V of 2013 on the Civil Code (hereinafter referred to as the **Civil Code**).

Personal data means any information 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, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

3. What contact personal data do we process, for how long, for what purpose, and on what authorization basis?

The legal basis for our data processing is as follows: under Article 6(1)(f) of the **GDPR**, data processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party.

Description of the legitimate interest: The data controller and the contracted partner have a shared legitimate interest in processing contact data, as it is necessary for the fulfillment of the contract between the data controller and the contracted partner, for communication related to the contract, and for sending notifications to the contracted partner regarding the concluded contract. The data controller processes only the strictly necessary data of the contact person, so the fundamental rights and freedoms of the contact person are not violated by the data processing and do not override the legitimate interests of the data controller and the contracted partner.

The scope of processed data, the purpose of data processing, and the legal basis regarding the contact data of contracted partners are as follows:

Category of Processed Data	Source of Data	Purpose of Data Processing	Legal Basis for Data Processing	Data Retention Period, Deletion Date
----------------------------	----------------	----------------------------	---------------------------------	--------------------------------------

Name	Contracted partner	a) Establishing the contract b) Fulfilling the contract c) Claims and legal enforcement d) Identification e) Communication	Article 6(1)(f) of GDPR: Legitimate interest	For enforcing civil claims or fulfilling obligations, the data retention period is 5 years after the end of the civil legal relationship with the data subject, according to Section 6:22(1) of Act V of 2013 on the Civil Code. If data must be retained under Sections 168-169 of Act C of 2000 on Accounting, the data controller will delete the data 8 years after the end of the contractual relationship. Such cases include data in accounting documents, e.g., contract-related documents (including orders) or invoices.
------	--------------------	--	--	--

Email Address	Contracted partner	a) Establishing the contract b) Fulfilling the contract c) Claims and legal enforcement d) Communication	Article 6(1)(f) of GDPR: Legitimate interest	See above
Employer's Name, Address	Contracted partner	a) Establishing the contract b) Fulfilling the contract c) Claims and legal enforcement d) Identification e) Communication	Article 6(1)(f) of GDPR: Legitimate interest	See above
Phone Number	Contracted partner	a) Establishing the contract b) Fulfilling the contract c) Claims and legal enforcement d) Communication	Article 6(1)(f) of GDPR: Legitimate interest	See above
Position	Contracted partner	a) Establishing the contract b) Fulfilling the contract c) Claims and legal enforcement d)	Article 6(1)(f) of GDPR: Legitimate interest	See above

		Communication		
Individual entrepreneur registration number, registered office, tax number	Contracted partner	a) Establishing the contract b) Fulfilling the contract c) Claims and legal enforcement d) Identification e) Communication	For purposes a), b), d), and e): Article 6(1)(b) of GDPR: Establishing and fulfilling the contract; For purpose c): Article 6(1)(f) of GDPR: Legitimate interest	See above

4. Who manages the personal data of contact persons, and who has access to it?

The contact details and company information of the Data Controller can be found in Section 1. Employees of the Data Controller have access to the data only to the extent necessary for performing their work. Access rights to personal data are strictly regulated by an internal policy.

We do not use data processors for the management and storage of contact data.

5. What rights do contacts have regarding the handling of their personal data, and how do we ensure the exercise of these rights?

The data protection rights and remedies of the data subjects are detailed in the relevant provisions of the GDPR (in particular Articles 15, 16, 17, 18, 19, 20, 21, 22, 77, 78, 79, 80, and 82 of the GDPR). The following summary includes the most important provisions, and the Data Controller provides information to the data subjects regarding their rights and remedies related to data processing accordingly.

Information must be provided in writing or by other means, including, where appropriate, electronic means. Upon the request of the data subject, information may also be provided orally, provided that the identity of the data subject has been verified by other means.

The Data Controller shall inform the data subject without undue delay, but in any case, within one month from the receipt of the data subject's request to exercise their rights (see GDPR Articles 15-22), about the action taken based on their request. If necessary, considering the complexity of the request and the number of requests, this deadline may be extended by an additional two months. The Data Controller shall inform the data subject of the extension and the reasons for the delay within one month of receiving the request. If the data subject submitted the request electronically, the response should preferably be provided by electronic means, unless the data subject requests otherwise.

If the Data Controller does not take action upon the data subject's request, they shall inform the data subject without delay, and at the latest within one month from the receipt of the request, of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

Right of access by the data subject

- (1) The data subject has the right to obtain confirmation from the Data Controller as to whether or not personal data concerning them is being processed. If such processing is taking place, the data subject has the right to access the personal data and the following information:
 - a) the purposes of the processing;
 - b) the categories of personal data concerned;
 - c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, particularly in the case of recipients in third countries or international organizations;
 - d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - e) the right of the data subject to request rectification, erasure, or restriction of processing of personal data concerning them, and to object to such processing;
 - f) the right to lodge a complaint with a supervisory authority;
 - g) where the personal data are not collected from the data subject, any available information as to their source; and
 - h) the existence of automated decision-making, including profiling, as referred to in Article 22(1) and (4) of the GDPR, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- (2) If personal data are transferred to a third country, the data subject has the right to be informed of the appropriate safeguards relating to the transfer.

(3) The Data Controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Data Controller may charge a reasonable fee based on administrative costs. If the data subject submits the request electronically, the information shall be provided in a commonly used electronic form unless otherwise requested.

Right to rectification

The data subject has the right to obtain from the Data Controller, without undue delay, the rectification of inaccurate personal data concerning them. Considering the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure (“right to be forgotten”)

(1) The data subject has the right to obtain from the Data Controller the erasure of personal data concerning them 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 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 have to be erased to comply with a legal obligation; or
- f) the personal data have been collected in relation to the offer of information society services.

(2) If the Data Controller has made the personal data public and is obliged to erase them, the Data Controller, taking available technology and implementation costs into account, shall take reasonable steps, including technical measures, to inform other controllers processing the personal data that the data subject has requested the erasure of any links to, or copies or replications of, those personal data.

(3) The above provisions do not apply to the extent that processing is necessary, among others:

- a) for exercising the right of freedom of expression and information;
- b) for compliance with a legal obligation;
- c) for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes; or
- d) for the establishment, exercise, or defense of legal claims.

Right to restriction of processing

(1) The data subject has the right to obtain from the Data Controller the restriction of processing where one of the following applies: a) the accuracy of the personal data is contested by the data subject; b) the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; c) the Data Controller no longer needs the personal data for processing purposes, but the data subject requires them for legal claims; or d) the data subject has objected to processing, pending verification of whether the legitimate grounds of the Data Controller override those of the data subject.

(2) If processing has been restricted, such personal data shall only be processed with the data subject's consent, for legal claims, for protecting the rights of others, or for reasons of substantial public interest.

(3) The Data Controller shall inform the data subject before lifting the restriction on processing.

Notification Obligation Regarding the Rectification or Erasure of Personal Data or Restriction of Processing

The Data Controller informs all recipients with whom the personal data has been shared of any rectification, erasure, or restriction of processing, except where this proves impossible or requires a disproportionately large effort. Upon request, the Data Controller provides the data subject with information about these recipients.

Right to Data Portability

(1) The data subject has the right to receive the personal data concerning them, which they have provided to the Data Controller, in a structured, commonly used, and machine-readable format, and has the right to transmit those data to another data controller without hindrance from the Data Controller, if: a) the processing is based on consent or a contract; and b) the processing is carried out by automated means.

(2) In exercising the right to data portability as per section (1), the data subject has the right to request the direct transfer of personal data between data controllers (such as between the Data Controller and another data controller), where technically feasible.

(3) Exercising this right must not infringe upon the right to erasure (the "right to be forgotten") and must not adversely affect the rights and freedoms of others.

Right to Object

(1) The data subject has the right to object at any time, on grounds relating to their particular situation, to the processing of their personal data based on legitimate interests. In this case, the Data Controller shall no longer process the personal data unless the Data Controller

demonstrates compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject, or for the establishment, exercise, or defense of legal claims.

(2) If personal data is processed for scientific or historical research purposes or statistical purposes, the data subject has the right to object to the processing of personal data concerning them on grounds relating to their particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Right to Lodge a Complaint with a Supervisory Authority

The data subject has the right to lodge a complaint with a supervisory authority, in particular in the member state of their habitual residence, place of work, or place of the alleged infringement, if the data subject considers that the processing of personal data relating to them infringes the GDPR. In Hungary, the competent supervisory authority is the Hungarian National Authority for Data Protection and Freedom of Information (website: <http://naih.hu/>; address: 1055 Budapest, Falk Miksa Street 9-11; postal address: 1363 Budapest, Pf.: 9.; phone: +36-1-391-1400; fax: +36-1-391-1410; email: ugyfelszolgalat@naih.hu).

Right to an Effective Judicial Remedy against a Supervisory Authority

- (1) The data subject has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.
- (2) The data subject also has the right to an effective judicial remedy if the competent supervisory authority does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint.
- (3) Proceedings against a supervisory authority shall be brought before the courts of the member state where the supervisory authority is established.

Right to an Effective Judicial Remedy against the Data Controller or Processor

- (1) The data subject has the right to an effective judicial remedy against the Data Controller or processor if they consider that their GDPR rights have been infringed as a result of the non-compliant processing of their personal data, without prejudice to available administrative or non-judicial remedies, including the right to lodge a complaint with a supervisory authority.
- (2) Proceedings against the Data Controller or processor shall be brought before the courts of the member state where the Data Controller or processor is established. Such proceedings may also be brought in the courts of the member state where the data subject has their habitual residence. In Hungary, the regional court has jurisdiction over these cases. The data subject may bring the case before the regional court competent for their place of residence or habitual residence. Information on court jurisdiction and contact details can be found at: www.birosag.hu.

6. How Do We Ensure the Security of Your Data?

- We have a comprehensive data management policy to ensure the security of the data and information we handle, which applies to all employees and subcontractors and is known and followed by all our employees and subcontractors.
- Our employees receive regular training on data and information security requirements.

IT Infrastructure Data Security

- Personal data is stored on our central server, which can only be accessed by our employees and subcontractors according to strict access control rules. We periodically and regularly test and monitor our IT systems to ensure and maintain data and IT security.
- Office workstations are password-protected, and external storage devices can only be used after automatic virus and malware scanning.
- Comprehensive, continuous malware protection is provided for all systems and system elements.
- During the design, development, testing, and operation of programs, applications, and tools, security functions are prioritized and managed separately.
- Access keys (e.g., passwords) for information systems are stored encrypted, and access rights (e.g., passwords, permissions, logs) are protected when assigning access privileges.

Data Security in Communication

- We use SSL / TLS encryption for electronic messages and files. To meet the secure data exchange requirements, we ensure the integrity of both control and user data. Error-detection and correction procedures are applied to prevent data loss and damage.
- Our protection system detects unauthorized intrusion, modification, and interception. We prevent data loss and damage using error-detection and correction procedures and ensure non-repudiation.
- For networks used in data transmission, we prevent illegal access and eavesdropping in a manner that meets the security level requirements.

Physical Data Security

- To ensure physical data security, we maintain secure doors and windows and apply strict visitor and entry rules for guests. The office is under surveillance with a camera system, backed by a rapid response team.
- Paper-based documents containing personal data are stored in secure, lockable cabinets, accessible only to authorized personnel with access control.
- Rooms used for storing data carriers are designed to provide adequate protection against unauthorized access, forced entry, fire, or natural disasters. Data carriers used for transmission, backup, and archiving are stored in reliably closed locations only.

7. What Do We Do in Case of a Data Protection Incident?

In compliance with legal requirements, we report data protection incidents to the supervisory authority within 72 hours of becoming aware of the incident, and we keep a record of data protection incidents. In cases defined by law, we also inform the data subjects.

8. When and How Do We Amend This Privacy Notice?

If the scope of processed data or other aspects of data processing change, we will amend this Privacy Notice in accordance with GDPR regulations and notify you accordingly. Please review the amendments to the Privacy Notice carefully, as they contain important information regarding the processing of your personal data. The Data Controller has conducted a legitimate interest assessment for all personal data processing based on legitimate interest, and an aggregated notice is available without restriction at the current office manager of the Data Controller.

Date: Kecel, September 1, 2024.

Frida Vida CEO of EUROVID Ltd.