GENERAL COMMUNICATION POLICY

of CETIN Bulgaria EAD

for https://cetinbg.bg/

I. GENERAL INFORMATION

At CETIN Bulgaria (hereinafter referred to as the „**Company**“ or „**CETIN**“), the privacy and security of your personal data are of utmost importance to us. This General Communication Policy (hereinafter referred to as the „**Policy**“) provides detailed information on how we collect, process, store, archive, and delete personal data received through our general email address, info@cetinbg.bg, or through the contact phone numbers, which are published on our website www.cetinbg.bg. It also outlines the security measures we implement to ensure that all data processing activities are fully compliant with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and the applicable Bulgarian legislation regarding data collection and protection.

This Policy serves as a legally binding statement of our obligations under GDPR. It is designed to inform individuals who contact us under this Policy about how their personal data will be handled, their legal rights, and our data protection procedures.

By contacting us through phone calls and info@cetinbg.bg, you agree to the terms of this Policy.

II. DATA CONTROLLER

The Company operates as the Data Controller under the meaning of GDPR, which means that we determine the purposes and means of processing personal data received through phone and/or email communications.

As the Data Controller, we are responsible for ensuring that all personal data is processed in accordance with the legal obligations under the GDPR and applicable Bulgarian legislation.

III. CATEGORIES OF PERSONAL DATA COLLECTED

When you communicate with us via phone calls or info@cetinbg.bg, we may collect and process various categories of personal data, including but not limited to the following:

3.1 Personal Identifiable Information (PII):

Name: Full name of the individual initiating the communication.

Contact Details: Email address, phone number, and any additional contact details provided in the correspondence.

Job Title and Organization: If the email relates to professional matters, you may voluntarily provide your job title or the name of your employer.

3.2 Inquiry-Related Data:

Email Content: The information included in the body of the email, may contain details of your inquiry, complaint, request, or feedback. This may include descriptions of issues, personal opinions, or information regarding the subject matter of your correspondence.

Attachments: Any attachments provided (e.g., documents, images, files) that may contain additional personal data or information.

3.3 Special Categories of Personal Data:

In accordance with Article 9 of GDPR, special categories of personal data include sensitive data, such as:

- **a)** Data concerning health;
- **b)** Racial or ethnic origin;
- **c)** Political opinions;
- **d)** Religious or philosophical beliefs;
- **e)** Trade union membership;
- **f)** Genetic and biometric data for identification purposes;
- **g)** Data concerning a natural person's sex life or sexual orientation.

We strongly advise against including any special categories of personal data in your communications. In the event that such data is received inadvertently, we will take immediate steps to delete it, except where we are required by law to retain the data for legal purposes.

IV. PURPOSES FOR PROCESSING PERSONAL DATA

The personal data collected through communications under this Policy will be processed for the following legitimate and specific purposes:

4.1 Responding to Inquiries and Complaints:

We will use your personal data to respond to any questions, complaints, or requests you submit via phone or email. This includes verifying your identity where necessary and ensuring appropriate follow-up actions.

4.2 Service Improvement:

The personal data provided may be used to analyze feedback and inquiries to improve the quality and functionality of the services offered by CETIN Bulgaria.

4.3 Compliance with Legal and Regulatory Obligations:

We may process your personal data to fulfil our legal obligations under Bulgarian and EU laws. This includes responding to requests from public authorities, complying with statutory record-keeping requirements, and facilitating potential investigations or legal proceedings.

4.4 Protection of Legitimate Interests:

Where necessary, we may process personal data to protect our legitimate interests, including preventing fraud, ensuring network security, and defending our legal rights in the event of disputes or claims arising from communications with data subjects.

The purposes outlined above are pursued in strict adherence to the principles of data minimization, meaning that we only process data that is strictly necessary for the intended purpose.

V. LEGAL BASIS FOR PROCESSING

We rely on the following legal bases for the processing of personal data under this Policy, in accordance with Article 6 of GDPR:

5.1 Legitimate Interests (Article 6(1)(f) GDPR):

The primary basis for processing personal data received via phone call or email is the legitimate interest of CETIN Bulgaria in responding to inquiries and handling communications effectively. Our interest in maintaining communication with clients, suppliers, business partners, and other stakeholders justifies the processing of personal data provided voluntarily in such communications.

5.2 Compliance with Legal Obligations (Article 6(1)(c) GDPR):

Certain personal data may need to be processed to comply with applicable legal requirements, such as statutory reporting obligations, responding to regulatory inquiries, or retaining records as required under Bulgarian law.

5.3 Consent (Article 6(1)(a) GDPR):

In cases where you voluntarily provide sensitive or other data for which we do not have legitimate grounds for processing, we will request your explicit consent to process such information unless the processing is justified under another legal ground. You may withdraw your consent at any time by contacting us, though this will not affect the lawfulness of any processing carried out prior to the withdrawal.

VI. DATA RETENTION

We will retain personal data received through communications under this Policy for no longer than is necessary to fulfil the purposes for which the data was collected.

Personal data provided in inquiries will be retained for a maximum of six (6) months from the date of the final correspondence unless a longer retention period is required by law.

In cases where legal obligations or ongoing legal disputes require extended retention, we will securely store the relevant data until the matter is resolved, and any statutory retention periods have been satisfied.

6.1 Special Categories of Personal Data:

If any special categories of personal data are inadvertently collected through communications under this Policy, these will be immediately deleted unless retention is required by law. Our retention policy for such sensitive data is in full compliance with GDPR, specifically Article 9(2), which prohibits the processing of special categories of data unless specific legal conditions are met.

6.2 Archiving:

Personal data will not be archived in long-term storage unless required for compliance with legal obligations, such as but not limited to financial record-keeping, legal claims, or auditing purposes. Any archived data will be securely stored with access restricted to authorized personnel only.

Upon expiration of the retention period, all personal data will be securely and permanently deleted from our systems or anonymized to ensure that individuals cannot be identified from the data.

VII. DATA SECURITY MEASURES

We have implemented the necessary data security measures and employ a variety of technical and organizational measures to safeguard personal data against unauthorized access, alteration, disclosure, or destruction. These include, but are not limited to:

7.1 Encryption:

All communications under this Policy containing personal data sent to info@cetinbg.bg are encrypted both in transit and at rest using secure encryption protocols. This ensures that data is protected from interception during transmission and while stored on our servers.

7.2 Access Control:

Access to the general email inbox and any personal data stored within is restricted to authorized personnel only. The same principle is applied to personal data collected through phone calls. These individuals are granted access based on the principle of least privilege, ensuring that only those who require access for legitimate purposes are granted permission.

All employees with access to personal data are subject to confidentiality agreements and are regularly trained on GDPR compliance and data protection practices.

7.3 Anonymization and Pseudonymization:

Where possible, personal data will be anonymized or pseudonymized to reduce the risk of identification in the event of unauthorized access.

7.4 System Security:

The systems used to manage call logs, recordings (if applicable), and related data are protected to prevent unauthorized access at all times. We utilize secure IT systems with up-to-date firewalls, intrusion detection systems, and anti-virus software to protect against cyber-attacks.

Regular security audits and vulnerability assessments are conducted to ensure our systems are protected from potential threats.

7.5 Incident Response and Breach Notification:

In the event of a data breach that affects personal data, we have implemented an incident response plan that complies with the GDPR's breach notification requirements.

If a breach is likely to result in a high risk to the rights and freedoms of data subjects, we will notify the affected individuals and the relevant supervisory authority, the Bulgarian Commission for Personal Data Protection (CPDP), within 72 hours of becoming aware of the breach.

7.6 Email protection:

We employ standard email protection applications and protocols to ensure a secure and robust email environment such as antivirus software, antispam filtering, antiphishing, data loss prevention and malware detection.

VIII. DATA SHARING AND THIRD-PARTY PROCESSING

CETIN Bulgaria does not share personal data received via communications under this Policy with third parties except in the following circumstances:

8.1 Service Providers:

We may engage third-party service providers to assist with the processing and storage of call logs, and emails or to provide IT infrastructure support. These providers act as Data Processors on our behalf and are contractually bound to adhere to GDPR-compliant data processing agreements.

These agreements ensure that:

a) Personal data is processed only according to our documented instructions.

b) Sufficient security measures are in place to protect personal data.

c) No unauthorized transfers or access occur outside the scope of the agreement.

8.2 Legal Requirements:

We may disclose personal data where required by law, in response to requests from public authorities, or in connection with legal proceedings.

8.3 International Transfers:

As a rule, we strive not to transfer personal data outside of the European Economic Area (EEA). If such a transfer becomes necessary, we will ensure that appropriate safeguards are implemented in line with GDPR, such as Standard Contractual Clauses (SCCs) or other approved mechanisms for international data transfers.

IX. DATA SUBJECT RIGHTS

Under GDPR, you have specific rights with respect to your personal data. These rights are outlined below, and you may exercise them at any time by contacting us.

9.1 Right to Access:

You have the right to request a copy of the personal data we hold about you, along with information about how and why it is being processed.

9.2 Right to Rectification:

If any of the personal data we hold about you is inaccurate or incomplete, you have the right to request that we correct or update it without undue delay.

9.3 Right to Erasure (Right to be Forgotten):

In certain circumstances, you may request that we delete your personal data, for example, if the data is no longer necessary for the purposes for which it was collected or if you withdraw your consent (where consent was the legal basis for processing).

9.4 Right to Restrict Processing:

You have the right to request that we limit the processing of your personal data in specific situations, such as when you contest its accuracy or object to the processing based on our legitimate interests.

9.5 Right to Data Portability:

You may request that we provide you with your personal data in a structured, commonly used, and machine-readable format and transfer that data to another controller where feasible.

9.6 Right to Object:

You may object to the processing of your personal data where the processing is based on our legitimate interests, including profiling. We will cease processing unless we demonstrate that the processing is based on compelling legitimate grounds that override your interests, rights, and freedoms.

9.7 Right to Withdraw Consent:

Where processing is based on your consent, you may withdraw your consent at any time. This will not affect the lawfulness of any processing carried out before the withdrawal of consent.

9.8 Right to Lodge a Complaint:

If you believe that your personal data has been processed in violation of GDPR, you have the right to lodge a complaint with the Bulgarian Commission for Personal Data Protection (CPDP) or the data protection authority in your country of residence.

X. CHANGES TO THE POLICY

We reserve the right to update or modify this Policy at any time to reflect changes in data protection laws or our data processing practices. Any updates will be posted on our website (www.cetinbg.bg/privacy), and significant changes can be communicated to you directly via email or other appropriate means.

This Policy is valid as of 20.09.2024.

All future changes shall take effect immediately.

XI. ADDITIONAL INFORMATION

If you have any questions about this Policy and how we handle personal data, please do not hesitate to contact us.