Data Protection Information of CETIN Hungary Zrt.

Date of the last update of this statement: 9 June 2021

Data protection is of utmost importance to us and we want to ensure transparency regarding how we collect your personal data and how we process it. Please read this information notice and if you have any questions, please contact us using the contact details specified in section 11.

This information notice provides information about your rights concerning your personal data and outlines the principles followed by **CETIN Hungary Zrt.** (hereinafter referred to as the "Data Controller") in the processing of your personal data. The following document contains the general terms and conditions for the processing of personal data, and therefore applies to all services provided by the Data Controller, its website or any of our services provided in cooperation with our partners.

1. Principles of Data Processing

CETIN Hungary Zrt., the Data Controller, is a company registered with the Company Registry Court of the Budapest Environs Regional Court under registration number Cg.13-10-042052, and has its registered office at Pannon út 1, Törökbálint, 2045 Hungary.
Our goal is to handle data in accordance with the regulations and to ensure that all our customers can trust us with their data. To achieve this, we apply the following data protection principles:

1. We handle your personal data in compliance with this Data Protection Information and applicable laws and regulations.
2. We take all reasonable measures to ensure transparency in the processing of your personal data and are always available to address any questions you may have.
3. We process your personal data only for specific, explicit and lawful purposes, in a manner and for a duration necessary to achieve these purposes. We take all reasonable measures to promptly delete or rectify any inaccurate personal data in relation to the purposes of data processing. We also ensure that personal data are stored appropriately, and that the data minimisation principle is respected in all data processing activities.
4. We implement appropriate security measures to safeguard the security of your personal data, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage of data.
5. We design our services with data protection considerations in mind. This means that we give the highest priority to the protection and proper management of your data, and we make every effort to build appropriate data protection safeguards into the services we develop, looking at your specific concerns already at the design stage to ensure that we provide you with the most appropriate service.

2. The Legal Framework for Personal Data Processing

In the processing of personal data, we comply with the aforementioned data protection principles and applicable laws and regulations.

Applicable legal regulations

(a) Act C of 2003 on electronic communications ('Act C of 2003');
(b) Act CXII of 2011 on informational self-determination and freedom of information ('Act CXII of 2011');
(c) Act CVIII of 2001 on certain issues of electronic commerce services and information society services ('Act CVIII of 2001');
(d) Act XLVIII of 2008 on the basic conditions of, and certain restrictions on, economic advertising ('Act XLVIII of 2008');
(e) Act CLXV of 2013 on complaints and notifications of public interest;
(f) Commission Regulation (EU) No 611/2013 of 24 June 2013 on measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector ('611/2013/EU regulation').
(g) 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 ('GDPR').

3. Data Processing in Everyday Life

The collection and usage of personal data depend on the purpose of data processing and align with the services you utilize.

In general, we collect and use your personal data when:

- The data is necessary to provide the service you use,
- The data is essential for handling any complaints or feedback you may have.
- The collection and processing of data are required by law.
- We need the data to enhance your user experience.
- The data is necessary for ensuring and improving the quality of our services, or
- You have given your consent for the collection and use of your data for a specific purpose.

The specific personal data we collect and the manner in which we handle it depend on the particular service you are using.

The Data Controller operates a Compliance function to support its Code of Ethics, internal policies, relevant regulations and other compliance-related matters. This includes translating ethical and compliance principles into daily activities, addressing and managing ethical and compliance issues and situations, monitoring employees' compliance and investigating potential violations. Anyone can make a report to CETIN Compliance by sending an email to cetin.hu.compliance@cetin.hu to raise concerns or report potential violations. We treat all reports confidentially, and no one will face adverse consequences for making good-faith reports of such incidents.

If you browse our websites, you can find additional information in the Cookie Policy alongside this Data Protection Information.

Legal basis for processing your personal data

The legal basis for processing your personal data by the Data Controller may vary depending on the specific processing activities.

In general, the possible legal bases for our data processing are as follows:

- Consent – when you have given your consent for the processing of your personal data for one or more specific purposes.
- Complying with a legal obligation to which the Data Controller is subject;
- Data processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, unless those interests are overridden by your interests or fundamental rights and freedoms which require the protection of your personal data.

Before initiating a specific processing activity, we provide appropriate information about the current legal basis for the data processing.

4. Certain data processing by the Data Controller

The purpose of our data processing through our website is to provide you with the highest quality digital experience possible. We ensure the improvement of online user experience through various digital technologies.

In order to provide our services, it is necessary to process additional data as follows:

While you use our services or browse our website, we may collect other data about you. This data may include:

(a) Data related to your communication with us (e.g., requests you make to us or feedback you send us);
(b) Technical and analytical data generated during your use of various online services, such as when you visit our website and/or use any of our internet services (e.g., browsing activities). Some of this data is stored in the form of cookies and may not necessarily be suitable for your personal identification, but it enables us to improve the quality of our services. The technical data we collect may include:

(i) Network identifiers, such as IP addresses and port numbers;
(ii) Operating system, browser types and their version numbers;
(iii) Type and category of the available internet service, such as, e.g., browsing, social media, Facebook, etc.);
(iv) Time, location and manner of using the service, as well as log data;
(v) Analytical data related to your visit to our website, including the source from which you accessed our website, the pages you visited on our website, the services you viewed, the searches you conducted, furthermore, the duration of your visit and your interactions with us.

The Data Controller does not process the content of available internet services (e.g., article content, emails, images, video content, downloaded file lists, etc.) or search engine results, or precise current and historical GPS locations. This ensures the protection of your privacy and adherence to the data minimization principle.

The data is typically used for the following purposes:

- To fulfil other obligations related to providing the service,
- To use the recorded communication data for quality assurance purposes and to provide feedback management;
- To enhance the customer experience,
- To improve our services by better understanding your behaviour and preferences,
- To analyse the usage of our services in order to identify general trends and develop new services for our customers.

If you wish to object to data processing, you can do so by contacting us at the contact details provided in clause 11. If the legal basis for data processing is your consent, you can withdraw your consent at any time to the effect that withdrawing your consent does not affect the lawfulness of data processing based on your previous consent.

The security of the services we provide to you

We also utilize the available data to maintain the security of our services by:

- Investigating suspicious or unlawful activities that may violate our terms of service or applicable laws, and taking necessary actions against them.
- Sharing your data with competent authorities upon their request, for example, if an authority requests information about you based on legal grounds to fulfil their tasks.

Transmission of your personal data to third parties by the Data Controller during the provision of services

For the complete realization of our services, there may be cases where we need to temporarily transmit certain personal data to third parties for the purpose of data processing. Without such data transmission, it would not be possible to handle your personal data in this manner.
The third parties to whom we transmit your data provide us with guarantees that their data processing is carried out in compliance with data protection principles, as well as with this privacy statement and applicable legal provisions.

We may share your personal data with the following third parties:

(a) Any company operating as part of the CETIN Group or its subsidiaries.
(b) Data processors acting on our behalf, such as providers of mailing services, system operators, etc.
(c) Third parties providing services to which you have given your consent.
(d) Law enforcement agencies and other authorities, if we are required by law to cooperate for the purposes of criminal investigation or other lawful purposes.

Unless otherwise provided by applicable laws, the Data Controller only shares your personal

data with third parties after entering into a contract with the data recipient.

Categories of our partners:

The Data Controller engages data processors to support its services, who may have access to certain personal data stored in the Data Controller's systems in order to perform their activities. For the security of certain facilities operated by the Data Controller, third-party services are employed, and in certain cases, these parties may have access to your personal data to the extent necessary for carrying out their security tasks (e.g., monitoring the recordings stored by security cameras at the facilities).
In order to operate, build, modernize its network, and provide certain services, the Data Controller engages partners who provide operational, information technology (IT) and other services. These partners, acting as data processors, may have access to certain personal data.
The Data Controller engages third-party data processors for logistical and data storage tasks (e.g., document management, storage).

CETIN Hungary Zrt. (registered office: 2045 Törökbálint, Pannónia út 1, Hungary, company registration number: 13-10-042052) cooperates with Telenor Hungary as a data processor in the operation of the network.

5. International Data Transfers:

Taking advantage of our strong international presence and operations, we occasionally engage partners, service providers and technical infrastructure (such as servers) that are not located in the country where you live and use the service.

6. How We Protect Your Personal Data

We are aware that transferring data from your country of residence to another country may involve data protection and security risks. Therefore, we only transfer your data to a recipient that implements appropriate security measures, considering the valid legal basis for data transfer. The Data Controller commits to applying EU model contractual clauses (Standard Contractual Clauses, SCCs) for international data transfers, as required for these data transfers. In the judgment C-311/18 (Schrems II), the Court of Justice of the European Union established that, in addition to the measures provided for in these model conditions, further measures may be necessary to ensure compliance with the level of protection required by EU law. We continuously monitor recommendations and guidelines related to this matter and make the necessary additions to the model conditions we use.

Taking into account the risks of varying likelihood and severity, the Data Controller will in any case implement appropriate technical and organisational measures to ensure that your personal data is adequately protected.

If the Data Controller processes your data based on its own legitimate interests or the legitimate interests of a third party, you have the right to object to the processing of your data.

We take the following measures to ensure the security of your personal data:
a) When handling your personal data through service providers or other data processors, we always ensure that these providers and data processors implement appropriate technical and organizational measures to maintain data security. Such control mechanisms include, *inter alia*,

control of access to the data and the infrastructure storing it, as well as agreements with third parties that impose obligations to comply with relevant regulations. We prioritize the incorporation and design of appropriate data protection safeguards already when elaborating our services.
b) If necessary, we conduct data protection impact assessments to evaluate how a specific activity would affect the security of your personal data.

7. How Long Do We Store Your Personal Data?

We only keep your personal data for as long as necessary to fulfil lawful purposes. If we no longer need your personal data for any further purposes, we will delete it.
The data retention periods can vary significantly. For example, in the case of video recordings kept for security purposes, the retention period may vary between 3 and 30 days. According to the Accounting Act of 2000, accounting documents and their attachments that directly and indirectly support accounting records must be retained for 8 years. In addition, there may be various retention periods aligned with specific data processing purposes.

8. Your Rights and How to Exercise Them

It is important to us that you are aware of your rights regarding your personal data.
According to Articles 15-20 of 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 ('GDPR'), you are entitled to exercise the following rights regarding your personal data processed by the Data Controller:
a) access to your personal data;
b) request the correction of your personal data;
c) request the deletion of your personal data;
d) request the restriction of the processing of your personal data;
e) object to the processing of your personal data;
f) receive your personal data and transmit it to another data controller, provided that the legal preconditions for this are met (right to data portability);
g) if the processing of your personal data is based on your consent, you have the right to withdraw your consent at any time.

You may send your request to exercise your rights to the contact details indicated in clause 11. The Data Controller will provide information on the actions taken in response to your request without undue delay and in any event within 30 days from the receipt of the request.
If the Data Controller does not take any action, it will provide information on the reasons for not taking action without undue delay and within 30 days from the receipt of the request. If you do not agree with the response or action taken by the Controller, you have the right to a judicial remedy. The Data Controller will inform all recipients to whom the personal data has been disclosed about any rectification, erasure or restriction of processing, unless it proves impossible or involves disproportionate effort. Upon request, the Data Controller will provide information about these recipients.
If you believe that your rights have been violated, you can file a complaint with the court or with the National Data Protection and Freedom of Information Authority (details can be found in Chapter 11).

Description of Data Subjects' Rights

Right of Access
You have the right to obtain from the Data Controller confirmation as to whether or not personal data concerning you is being processed, and if such processing is taking place, you have the right to access the personal data and receive information regarding the circumstances of processing. The requested information may include, among other things, the purposes of the processing, the categories of personal data, the recipients or categories of recipients to whom the personal data have been or will be disclosed by the Data Controller, the planned duration of storage of the personal data, and, if the data were not collected directly from you, any available information about their source.

Rectification
You have the right to request the Data Controller to rectify inaccurate personal data concerning you without undue delay, as well as the right to have incomplete personal data completed upon request.

Right to erasure ("the right to be forgotten")
You have the right to request the erasure of personal data concerning you without undue delay if one of the following grounds applies:

a) the personal data are no longer necessary;
b) you have withdrawn your consent on which the processing is based, and there is no other legal ground for the processing;
c) you object to the processing, and there are no overriding legitimate grounds for the processing;
d) the personal data has been unlawfully processed by the Data Controller;
e) the personal data must be erased for compliance with a legal obligation.

The Data Controller will not erase the data if processing is necessary for one of the following reasons: (i) for the exercise of the right to freedom of expression and information; (ii) for compliance with a legal obligation that requires the processing of personal data; (iii) or for the establishment, exercise or defence of legal claims.

Right to restrict data processing
You have the right to obtain, at your request, the restriction of processing by the Data Controller if one of the following conditions is met:
a) you dispute the accuracy of your personal information, in which case the restriction applies to the period of time that allows the Data Controller to verify the accuracy of your personal information;
b) the processing is unlawful and you object to the deletion of the data and instead request a restriction on their use;
c) the Data Controller no longer needs your personal data for data processing purposes, but you need the data to make, enforce or protect legal claims, or
d) you objected to the data processing; in this case, the restriction applies for the period until it is determined whether the legitimate reasons of the Data Controller take precedence over the legitimate reasons of the data subject.
In case of restriction of processing, the personal data affected by the restriction will, with the exception of storage, only be processed with your consent or for the establishment, exercise or defense of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or a Member State. The Data Controller

will inform you in advance about the lifting of the restriction.

Right to object
You have the right to object, on grounds relating to your particular situation, at any time to the processing of your personal data based on the legitimate interests pursued by the Data Controller. In such a case, the Data Controller may no longer process the personal data unless the the Data Controller can demonstrate compelling legitimate grounds for the processing which override your interests, rights, and freedoms, or for the establishment, exercise, or defense of legal claims.

The right to data portability
If it does not adversely affect the rights and freedoms of others, you have the right to receive your personal data in a structured, commonly used, and machine-readable format. You are also entitled to have these data transmitted directly by Telenor to another data controller, if:
a) the processing is based on your consent or is necessary for the performance of a contract to which you are a party, or for taking steps at your request prior to entering into a contract; and
b) the processing is carried out by automated means, i.e., the personal data is processed by computer systems and not on paper-based records.

9. Processing of Children's Data

The general rule is that we do not process the data of children under 16 years of age without the consent of their legal representative. If we become aware that we have collected data from a child under 16 years of age without obtaining proper consent, we will take steps to notify their legal representative, request their consent, and if it is not provided, we will delete the data. For services specifically targeted at children under 16 years of age, in addition to providing information about data protection rights, we will also seek the consent of their legal representative.

10. Review of This Data Management Information

The content of this Data Management Information will be reviewed as necessary. If there are significant changes to the content of this Information, we will inform you in an appropriate manner, such as through a notice posted on our website. When determining how to notify, we take into account factors such as the significance of the change, the services affected by the change and the range of customers that can be reached in this way.

11. Questions About the Data Protection Information

The Data Controller is responsible for the processing of your personal data. If you have any questions, concerns or complaints about this Data Protection Information or our processing of your data, please contact us using the following contact details:

CETIN Hungary Zrt.
Address: 2045 Törökbálint, Pannon út 1.
E-mail: cetin.hu.adatvedelem@cetin.hu
We will respond to your enquiry as quickly as possible, but within 30 days at the latest, and will do our best to answer your questions. If you have made a complaint and you are not satisfied with our response, you can lodge a complaint with the National Authority for Data Protection and Freedom of Information (NAIH, www.naih.hu, registered office: 1055 Budapest, Falk

Miksa utca 9-11; phone number: +36 1 391 1400; fax: +36 1 391 1410; e-mail: ugyfelszolgalat@naih.hu).
If you think your rights have been violated, you can also go to court. You may bring the action, at your choice, before the Budapest Environs Regional Court of the place where the Data Controller has its registered office, or before the competent court of law of the place where you reside or stay. A list of courts and their jurisdiction can be found at https://birosag.hu/birosag-kereso.