Privacy Policy

Magyar Telekom Nyrt. as a data controller complies with Regulation (EU) 2016/679 of the European Parliament and of the Council (April 27, 2016) on the protection of natural persons with regard to the processing of personal data and on the free flow of such data, as well as the 95/46/ Based on the repeal of the EC Directive **("General Data Protection Regulation"), the "Tell me!" operated by the Data Controller informs you below. or other stakeholders operated by the Data Controller who make a report through the system for reporting suspected abuses or named or mentioned in this report ("Data Subject")** in relation to the management of their personal data.

The Data Controller asks the Whistleblower to provide only the personal data necessary for the investigation of the given misuse among the information provided in the notification.

To ensure the success of the investigation of the contents of the report, in certain cases, with respect to third party stakeholders, in connection with whose activities or omissions the Whistleblower claims or assumes misuse, or provides information, separate information will only be provided later, but within a reasonable time, e.g. during an investigation interview, in minutes or via e-mail. This general information also applies to this case and to the persons concerned.

1. **Company name and contact details of the data controller:**

Magyar Telekom Nyrt. (Address: 1097 Budapest, Könyves Kálmán krt. 36., company registration number: 01-10-041928, tax number: 10773381-2-44 **„data controller")**

2. **Name and contact details of data protection officer:**

dr. Adrienn Esztervári (address: 1097 Budapest, Könyves Kálmán krt. 36.; email: DPO@telekom.hu)

3. **Scope of processed personal data, the legal basis for data management, the purpose and duration of data management:**

Purpose of data processing	Legal basis for data processing	Scope of processed personal data	Duration of data management or criteria for determining the duration
Operation of a system for reporting suspected abuse involving the employees of the controller, as well as its subcontractors, agents and other contractual partners.	Pursuant to Article 6 (1) point c) of the General Data Protection Regulation, the legal obligation for the Data Controller It is about complaints, reports in the public interest, and rules related to reporting abuse. 2023.CLXV. tv. 18. § (1) .	• Personal data concerning the informant as a data subject (name, e-mail address, telephone number) The Whistleblower can also choose anonymity, but this does not mean anonymity in terms of data protection, because she/he is identified in the system with a unique, technical identifier, but the Data Controller does not know her/his identity. • Additional information about	The Data Controller deletes personal data 5 years after the end of the investigation to submit, enforce and protect legal claims. The Data Controller will delete obviously unfounded reports as soon as possible, but no later than within 2 working days. Reports that have not been examined based on the substantive evaluation will be deleted by the Data Controller within 30 days.

Purpose of data processing	Legal basis for data processing	Scope of processed personal data	Duration of data management or criteria for determining the duration
		herself/himself provided by the Whistleblower in the notification. • Regarding the person notified by the Whistleblower, personal data provided in connection with the reported abuse. • Personal data concerning other third parties mentioned in the report (e.g. identification data, contact information, their role in relation to the abuse, their knowledge, etc.)	
The proper investigation of suspected abuses is in the hands of the employee responsible for investigation working in the Compliance area at the Data Controller.	Article 6 (1) point b) of the General Data Protection Regulation, data management is necessary for the fulfilment of the contract between employees working in the Compliance area of the Data Controller and responsible for investigations and the Data Controller.	Employees working in the compliance area of the Data Controller and responsible for the investigations: • Name • Job title • E-mail address • Password	The Data Controller deletes personal data 5 years after the end of the investigation to submit, enforce and protect legal claims.

4. Automated decision-making (including profiling):

During data management, automated decision-making, including profiling, does not take place.

5. Transmission of personal data, recipients of personal data and categories of recipients:

The Data Controller uses the following data processors in relation to data management:

- Whispli*, société par actions simplifiée à associé unique*company registration number (Paris Commercial and Company Registry) 853 011 278 00019: address: 10 rue de la Paix, 75002 Paris, France, activity related to data management: recording the reports received and providing the Data Controller with access to them. In the case of an anonymous report, the data will only be forwarded to the Data Controller with a technical identifier.

- Sub-processors used by Whispli: Amazon Web Services (52 rue du port, 92000, Nanterre, France), Google (8 Rue de Londres 75009 Paris, France), Zendesk (266 Place Ernest Granier, 34000 Montpellier, France), Dobbytec OÜ (Usetiful) (Sepapaja tn 6 15551 Tallinn Estonia), iSope (Espace Reine 90-92 Route de la Reine Boulogne-Billancourt 92100 France), Twilio (24 Rue Cambacérès, 75008 Paris)

Personal data will not be transferred to a third country (i.e. outside the European Union), or for transmission to an international organization. (The data processor used by the data controller uses sub-data processors based outside the European Union, but these sub-data processors use the European infrastructure, so no data transfer takes place.)

6. Rights of the Data Subject in relation to data management:

The Data Subject is entitled to the following data management rights:

a) the right of access to personal data concerning her/him,

b) the right to correct your personal data,

c) the right to delete or limit the processing of your personal data - apart from mandatory data processing,

d) the right to data portability if the conditions specified in the law exist,

e) in the case of data processing based on legitimate interest, the right to object.

Right of access:

The data subject has the right to receive feedback from the Data Controller as to whether her/his personal data is being processed, and if such data processing is in progress, she/he is entitled to receive access to the personal data. The Data Controller provides a copy of the personal data to the Data Subject. For additional copies requested by the Data Subject, the Data Controller may charge a reasonable fee based on administrative costs. If the Data Subject submitted the request electronically, the information must be provided in a widely used electronic format, unless the Data Subject requests otherwise.

Right to rectification:

The Data Subject has the right to have inaccurate personal data corrected without undue delay upon request by the Data Controller.

Right to erasure:

The Data Subject has the right to have inaccurate personal data corrected without undue delay upon request by the Data Controller, and the Data Controller is obliged to delete the personal data concerning the data subject without undue delay if one of the following reasons exists:

- the personal data are no longer needed for the purpose for which they were collected or otherwise processed.
- the data subject withdraws the consent that forms the basis of the data management pursuant to point a) of Article 6 (1) or point a) of Article 9 (2) of the General Data Protection Regulation, and there is no other legal basis for the data management.
- the Data Subject objects to the data processing based on Article 21 (1) of the General Data Protection Regulation and there is no overriding legitimate reason for the data management, or the Data Subject objects to the data management based on Article 21 (2) of the General Data Protection Regulation.
- personal data were handled illegally.
- personal data must be deleted to fulfil the legal obligation prescribed by EU or member state law applicable to the Data Controller.
- personal data was collected in connection with the provision of information society-related services referred to in Article 8 (1) of the General Data Protection Regulation (conditions for child consent).

Right to restrict data processing:

The Data Subject has the right to request that the Data Controller restrict data processing if one of the following conditions is met:

a) the data subject disputes the accuracy of the personal data, in which case the limitation applies to the period that allows the Data Controller to check the accuracy of the personal data;

b) the data processing is illegal, and the data subject opposes the deletion of the data and instead requests the restriction of its use.

c) The Data Controller no longer needs the personal data for the purpose of data management, but the data subject requires them to present, enforce or defend legal claims; or

d) the data subject has objected to data processing in accordance with Article 21 (1) of the General Data Protection Regulation; in this case, the restriction applies to the period until it is determined whether the Data Controller's legitimate reasons take precedence over the data subject's legitimate reasons.

If data management is subject to restrictions, such personal data may only be processed with the consent of the Data Subject, except for storage, or to submit, enforce or defend legal claims, or to protect the rights of another natural or legal person, or in the important public interest of the Union or a member state.

Right to data portability:

The Data Subject is also entitled to receive the personal data relating to him/her provided to the Data Controller in a segmented, widely used, machine-readable format, furthermore, she/he is entitled to transfer these data to another data manager without being hindered by the Data Manager to whom she/he made the personal data available, if: (i) the data processing is based on the consent of Article 6 (1) point a) or Article 9 (2) point a) of the General Data Protection Regulation, or Article 6 (1) point b) of the General Data Protection Regulation is based on a contract according to point; and (ii) data management is performed in an automated manner.

Right to protest:

The Data Subject has the right to object at any time to the processing of his personal data based on points e) or f) of Article 6 (1), including profiling based on the provisions, at any time for reasons related to his own situation. In this case, the Data Controller may no longer process the personal data, unless the Data Controller proves that the data processing is justified by compelling legitimate reasons that take precedence over the interests, rights and freedoms of the data subject, or which are related to the presentation, enforcement or defence of legal claims.

If personal data is processed for direct business acquisition, the data subject has the right to object at any time to the processing of her/him personal data for this purpose, including profiling, if it is related to direct business acquisition. If the data subject objects to the processing of personal data for the purpose of direct business acquisition, then the personal data may no longer be processed for this purpose.

General rules for the exercise of the rights of the affected parties:

The Data Controller shall inform the Data Subject without undue delay, but no later than one month from the receipt of the request, of the measures taken because of the request. If necessary, considering the complexity of the application and the number of applications, this deadline can be extended by another two months. The Data Controller shall inform the Data Subject of the extension of the deadline, indicating the reasons for the delay, within one month of receiving the request. The Data Controller shall inform the Data Subject of the extension of the deadline, indicating the reasons for the delay, within one month of receiving the request.

The Data Controller provides the Data Subject with information and measures free of charge. If the Data Subject's request is clearly unfounded or excessive, the Data Controller, for the administrative costs associated with providing the requested information or information or taking the requested action:

a) may charge a reasonable fee, or

b) can refuse to act based on the request.

It is the responsibility of the Data Controller to prove that the request is clearly unfounded or exaggerated.

If the Data Controller has reasonable doubts about the identity of the natural person who submitted the request, it may request the information necessary to confirm the Data Subject's identity.

7. Legal enforcement options:

The Data Subject may contact the data protection officer of the Data Controller at any time regarding the management of her/him personal data (dr. Adrienn Esztervári; address: 1097 Budapest, Könyves Kálmán krt. 36.; email: DPO@telekom.hu).

In the event of a complaint regarding the handling of personal data, the Data Subject may also contact the National Data Protection and Freedom of Information Authority (postal address: 1363 Budapest, Pf. 9., address: 1055 Budapest, Falk Miksa street 9-11., Phone: +36 (1) 391-1400; Fax: +36 (1) 391-1410; E-mail: ugyfelszolgalat@naih.hu; web: www.naih.hu).

In the event of a violation of their rights, the Data Subject may apply to court against the Data Controller. The court acts out of sequence in the case. The Data Controller is obliged to prove that the data management complies with the provisions of the law. The adjudication of the lawsuit falls within the jurisdiction of the court, in the capital, the Capital Court. The lawsuit can also be initiated before the court of residence or place of residence of the Data Subject.

The Data Controller is obliged to compensate the damage caused to others by the illegal handling of the Data Subject's data or by violating the requirements of data security. The Data Controller is released from liability if it proves that the damage was caused by an unavoidable cause outside the scope of data management. There is no need to compensate the damage if it resulted from the intentional or grossly negligent behaviour of the injured party.

Dated: Budapest, 2024.05.15.