

## Information on data processing

Magyar Telekom Ltd. as data controller (seat: 1097 Budapest, Könyves Kálmán krt. 36, Hungary; registration no.: 01-10-041928; taxation no.: 10773381-2-44; the „Data Controller”) hereby, in accordance with Regulation (EU) 2016/679 of the European Parliament and the Council (April 27, 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 („General Data Protection Regulation” or „GDPR”), notifies data subjects who submit a report through the Data Controller’s whistleblowing system called “Mondd el!” (“Tell us!”) or any other similar channel for reporting alleged wrongdoings, as well as other data subjects named or referenced in such reports, as follows:

**Reporters (whistleblowers) are requested to provide no more personal data that is necessary for understanding and investigating the reported incident, abuse or wrongdoing.**

In certain cases, for the success of the investigation, data subjects whose activities or omissions are reported by the whistleblower, or about whom the whistleblower otherwise provides information, will only be specifically informed later, within reasonable time (e.g. during an investigative interview, in interview minutes or by e-mail). This general data processing notice also applies to such data subjects.

### 1. The identity and the contact details of the Data Controller:

**Magyar Telekom Ltd.**

Contact person: Magyar Telekom Investor Relations;

Postal address: 1097 Budapest, Könyves Kálmán krt. 36. (registered seat);

Phone number: +36-1-458-0332.

### 2. The name and the contact details of the data protection officer:

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

### 3. The categories of the processed personal data, the purposes of the processing for which the personal data are intended, the legal basis for the processing and the period for which the personal data will be stored:

Purposes of the processing	Legal basis for the processing	Categories of personal data	Period for which the personal data will be stored
----------------------------	--------------------------------	-----------------------------	---

<p>To operate a system for reporting suspected misconducts or wrongdoings involving employees of the Data Controller or its subcontractors, agents or other contractual partners.</p>	<p>Article 6(1)(f) of the General Data Protection Regulation, legitimate interest of the Controller.</p> <p>The information provided by the notifier may include information that falls into a special category of personal data. For these, the legal basis for processing is Article 9(1)(f) of the General Data Protection Regulation.</p>	<ul style="list-style-type: none"> <li>Personal data of the whistleblower (name, e-mail address, telephone number) The whistleblower can opt for anonymity; however it does not mean anonymity as defined in data protection law, since the data subject will</li> </ul>	<p>With regard to the legitimate interest of the Data Controller consisting in the submission, enforcement or defense of legal claims, the personal data will be retained for no longer than 5 years after the completion of the investigation.</p> <p>Manifestly unfounded notifications are deleted by the Data Controller as soon as possible, but no</p>
<p><b>Purposes of the processing</b></p>	<p><b>Legal basis for the processing</b></p>	<p><b>Categories of personal data</b></p>	<p><b>Period for which the personal data will be stored</b></p>

		<p>nevertheless be singled out in the system by a unique technical identifier, although the Data Controller will not know his/her identity.</p> <ul style="list-style-type: none"> <li>• Other information provided by and related to the whistleblower</li> <li>• Personal data provided by the whistleblower in relation to the person in connection with whom an incident or wrongdoing is reported .</li> <li>• Personal data relating to other third parties mentioned in the report (e.g. identification data, contact details, their role in the abuse, their knowledge, etc.)</li> </ul>	<p>later than within 2 working days.</p> <p>Reports assessed on the merits and decided not to be investigated shall be deleted by the Data Controller within 30 days.</p>
<p>Appropriate investigation of suspected wrongdoings, misconducts by employees in the Compliance area of the Data Controller who are responsible for the investigation.</p>	<p>Article 6 (1) (b) of the General Data Protection Regulation, the processing is necessary for the performance of a contract between the Data Controller and the employees in the Compliance area of the Data Controller who are responsible for the investigation.</p>	<p>Employees in the Compliance area of the Data Controller who are responsible for the investigation:</p> <ul style="list-style-type: none"> <li>• name</li> <li>• type of work</li> <li>• e-mail address</li> <li>• password</li> </ul>	<p>With regard to the legitimate interest of the Data Controller consisting in the submission, enforcement or defense of legal claims, the personal data will be retained for no longer than 5 years after the completion of the investigation.</p>

Only those employees who need to have access to the data for performing their tasks shall have access to the personal data. No automated decision-making, including profiling, takes place in connection with the data processing.

**4. Transfer personal data, the recipients or categories of recipients of the personal data:**

The Data Controller uses the following data processors in connection with the processing:

- Whispli, société par actions simplifiée à associé unique (address: 10 rue de la Paix, 75002 Paris, France, contact details: ...); activities in connection with the processing: recording the notifications received and provide the Data Controller with access to them. In the case of anonymous submissions, only transmit the data to the Data Controller with a technical identifier.
- Sub-data 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)

No transfer of data to third countries (i.e. outside the European Union) or to international organizations takes place. (The data processor used by the controller uses sub-processors that are base outside the European Union, but these sub-processors use European infrastructure and therefore no data transfer takes place.)

## **5. The data subject's rights in connection with the processing:**

The data subject may exercise the following rights:

- a) right of access to his/her personal data,
- b) right of rectification of his/her personal data,
- c) right to erasure of his/her personal data or restriction of processing concerning the data subject;
- d) right to data portability (if the additional conditions are met); and
- e) in case of data processing based on the legitimate interest of the Data Controller or a third party, right to object.

### Right of access:

The data subject shall have the right to obtain from the Data Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data. 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. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

### Right to rectification:

The data subject shall have the right to obtain from the Data Controller without undue delay the rectification of inaccurate personal data concerning him or her.

### Right to erasure:

The data subject shall have the right to obtain from the Data Controller the erasure of personal data concerning him or her without undue delay and the Data 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 according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

- (d) the personal data have been unlawfully processed;
- (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Data Controller is subject;
- (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Right to restriction of processing:

The data subject shall have the right to obtain from the Data Controller restriction of processing where one of the following applies:

- (a) the accuracy of the personal data is contested by the data subject, for a period enabling the Data Controller to verify the accuracy of the personal data;
- (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 the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the Data Controller override those of the data subject.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence 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 of a Member State.

Right to data portability:

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Data Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the Data Controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) of the GDPR or on a contract pursuant to point (b) of Article 6(1) of the GDPR; and (b) the processing is carried out by automated means.

Right to object:

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. 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.

General rules regarding the data subjects' rights:

The Data Controller shall provide information on action taken on a request to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Data Controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Information to the data subject and any actions taken shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Data Controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The Data Controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Where the Data Controller has reasonable doubts concerning the identity of the natural person making the request, the Data Controller may request the provision of additional information necessary to confirm the identity of the data subject.

#### **6. Possible legal remedies:**

The data subject may turn to the Data Controller's data protection officer (dr. Adrienn Esztervári; address: 1097 Budapest, Könyves Kálmán krt. 36; E-mail address: [DPO@telekom.hu](mailto:DPO@telekom.hu)) in connection with the processing of his/her personal data at any time.

In case of the infringement of his/her rights, the data subject may submit a claim against the Data Controller to the court. The court shall proceed out of turn. The Data Controller shall prove that the processing is in compliance with the applicable laws. The Court of Appeal (*törvényszék*), in Budapest, the Metropolitan Court of Appeal (*Fővárosi Törvényszék*) is competent. The lawsuit may also be initiated in front of the Court of Appeal that has jurisdiction based on the permanent or temporary address of the data subject.

The Data Controller shall compensate the data subject for the damages caused to the data subject by the unlawful processing of the personal data of the data subject or by the infringement of data security requirements. The Data Controller shall be exempted from liability if it can prove that the damages were unavoidable and the causes were out of the scope of data processing. Damages that were due to the data subject's deliberate or grossly negligent behavior shall not be compensated.

The data subject has the right to lodge a complaint with the National Authority of Data Protection and Freedom of Information (*Nemzeti Adatvédelmi és Információszabadság Hatóság*, Postal address: 1363 Budapest, Pf. 9, Address: 1055 Budapest, Falk Miksa utca 9-11, Phone number: +36 (1) 391-1400; Telefax: +36 (1) 391-1410; Email: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu); website: [www.naih.hu](http://www.naih.hu)).

Dated: Budapest, ....., 2023