# KOMPaaS data protection guidance

Based on the articles 13 and 14 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Regulation (EC) No 95/46 (GDPR.) **KOMPaaS** compiled a guidanceon handling personal data for persons concerned.

## 1. Data controller

Name: KOMPaaS (MCNtelecom Kft).
Customer care office, address: 1114 Budapest, Kemenes utca 8. félemelet 3.Website: www.kompaas.sk
E-mail address: info@kompaas.tech
Phone: + 421 2 22202 999 (opening hours on weekdays: from 8 am to 5 pm)

## 2. Relevant legislation in force on data controlling

Data controller performs its activities guided by the following regulations:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Regulation (EC) No 95/46 (GDPR.).
- Act CXII of 2011 on the right to information self-determination and freedom of information (Info Act).
- Decree 4/2012. (I. 24.) of the National Media and Info-Communications Authority onthe rules pertaining to data protection and confidentiality obligations related to electronic communications services, special requirements for data processing and confidentiality, for the security and integrity of services, for the management of trafficand billing data, for the display of the caller ID and call forwarding (Akr.); Act C. of 2003 on Electronic Communications (Eht.).
- Act C. of 2003 on Electronic Communications (Eht.).
- Decree 2/2015. (X. 30.) of the National Media and Info-Communications Authority onthe detailed rules of the conclusion of electronic communications subscription contracts (Eszr.)
- Act CLV of 1997 on protection of consumers (Fgytv.)
- Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Services Related to the Information Society (Eker. Act)
- Act VI of 1998 on the protection of individuals with regard to the automated processing of personal data.
- Act CXIX of 1995 on the management of name and address data for the purpose of research and direct marketing (DM. Act).
- Act C. of 2000 on Accountancy (Számviteli tv.)

## 3. Data handled during data controlling

According to GDPR personal data means any information relating to an identified or identifiable natural person (“Subscriber”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier suchas 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.

### 3.1. Legal basis for the processing of personal data:

Data processing can only be performed if the appropriate legal basis is ensured. Inthe absence of an appropriate legal basis, data controlling cannot be lawfully performed.

Such legal basis could be:
that the data controlling was based on the provisions of law, i.e. necessary for the fulfillment of legal obligations concerning KOMPaaS (e.g. fulfillment oftax and accounting obligations, certain mandatory provisions of the Eht.),
that the subscriber has given his or her consent to one or more specific purposes(e.g. direct marketing consent),
that it was based on the legitimate interest of KOMPaaS (e.g. datacontrolling for fraud prevention, profiling),
that the data processing is necessary for the performance of a contract to which thedata subject is a party or it is necessary to take steps upon request of the data subject prior to the conclusion of the contract; (for example to fulfill a subscriptioncontract),
that the data processing is necessary to protect the vital interests of the data subjector another natural person (for example, data processing to search for a missing person)

### 3.2. Whom can be passed over personal data ?

Personal data can be handed over based on the following provisions of law and incase when a subscriber has given his or her consent to the following categories ofaddressees :

**Data processors :**

**a)** that perform billing, collection of debts, and contribute to sales and customercare activities,
**b)** legal representatives and empowered bodies for settling legal disputs concerning billing and sales
**c)** based on the GDPR Article 28 where a data processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract in

particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this Regulation.

**Third parties :**

Based on consent of the Subscriber Data Controller can pass over the personal data to third parties where processing is necessary for archiving purposes in the publicinterest, scientific or historical research purposes or statistical purposes.

Authorities and other bodies:

**a)** Police, public prosecutions, court, national security service

**b)** court executors
**c)** where the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physicallyor legally incapable of giving consent (GDPR Article 49)
**d)** Hungarian National Bank where performs control on national financial transmission system
**e)** Hungarian Competition Authority, where performs investigation on unfair commercial activities
**f)** Consumer Protection Authority
**g)** Administrative infringements related to misuse of emergency telephone numbers

### 3.3. Data transfer to third country or international organization

Data Controller does not transfer any data to third country or international organization.

### 3.4. Security of processing

The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
the pseudonymisation and encryption of personal data;
the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
the ability to restore the availability and access to personal data in a timely mannerin the event of a physical or technical incident;
In assessing the appropriate level of security account shall be taken in particular ofthe risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller.

## 4. Subscribers (Data subjects) rights concerning of handling their personal data

### 4.1 Right of access by the data subject (GDPR Article 15)

The data subject shall have the right to obtain from the controller confirmation as to whetheror not personal data concerning him or her are being processed, and, where that is the case, access to 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 recipient to whom the personal data have been or will be disclosed, in particular 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 existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or 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;

(h) the existence of automated decision-making, including profiling, 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.

The controller shall provide a copy of the personal data undergoing processing. For any furthercopies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unlessotherwise requested by the data subject, the information shall be provided in a commonly usedelectronic form. The right to obtain a copy shall not adversely affect the rights and freedoms ofothers.

### 4.2 Right to rectification (GDPR Article 16)

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

### 4.3 Right to erasure (Article 17)

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the 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 and where 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, or the data subject objects to the processing;

(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 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).

Where the controller has made the personal data public and is obliged pursuant to paragraph 1to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllerswhich are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b)for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defense of legal claims.

**4.4 Right to restriction of processing (GDPR Article 18)**

The data subject shall have the right to obtain from the controller restriction of processing whereone of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the 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 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 defense 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 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 defense of legal claims or for the protection of the rights of another natural or legal person or for reasonsof important public interest of the Union or of a Member State.

**4.5 Right to object (GDPR Article 21)**

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 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 defense of legal claims. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning himor her for such marketing, which includes profiling to the extent that it is related to such directmarketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

### 4.6. Right to data portability (GDPR Article 20)

The data subject shall have the right to receive the personal data concerning him or her, whichhe or she has provided to a 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 controller to which the personal data have been provided, where:

(a) the processing is based on consent of data subject or on a contract with him and

(b) the processing is carried out by automated means.

In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

### 4.7. Right to withdraw consent (GDPR Article 7, paragraph (3))

The data subject shall have the right to withdraw his or her consent at any time. The withdrawalof consent shall not affect the lawfulness of processing based on consent before its withdrawal.Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdrawas to give consent.General rules of exercising rights by the Data Subject

Data controller shall inform the Data Subject on the relevant measures taken as a response to the Data Subject's request without undue delay, but no later than within one month upon receiptof the request. Where necessary and in consideration of the complexity and number of requests,this deadline can be extended with two more months. Data controller shall inform the Data Subject of the extension of the deadline, indicating the reasons for the delay, within one monthfrom the receipt of the request. If the Data Subject files the request electronically the information - insofar as possible - shall be provided electronically, too, unless the Data Subjectrequests otherwise.

Data controller provides the Data Subject with the information and the measure free of charge.If the Data Subject’s request is manifestly unsubstantiated or - in particular due to its repeatedoccurrence - excessive, Data Controller, in respect of the administrative costs arising from theprovision of the requested information:

a) may charge a reasonable fee, or

b) may refuse to take the requested measure.

The burden of proof regarding the unsubstantiated or excessive nature of the request lies with Data controller. If Data controller has reasonable doubts as to the identity of the natural personsubmitting the application, it may request the provision of additional information necessary toconfirm the

identity of the Data Subject.

**5. Enforcement of rights**

If the Data Subject's rights are violated the Data Subject may turn to the competent court and file an official complaint against Data controller. The court shall adopt a decision in priority proceedings. Data controller shall be obliged to prove that the data controlling complies with the provisions of the law. The final decision on the case shall be made by the tribunal, in the capital by the Budapest-Capital Regional Court. The lawsuit can also be initiated before a courtoperating at the Data Subject's permanent address or place of residence.

Data controller shall compensate for damages caused by the unlawful processing of the Data Subject's data or the breach of data security requirements. Data Controller shall be relieved from liability if it is able to provide evidence that the damage is the result of an unavoidable cause beyond the scope of data processing. No compensation shall be paid if the damage was caused by intentional or serious negligent conduct on the part of the aggrieved party. In the event that the Data Subject have complaints on the processing of his or her personal data the complaint can also be filed with the Hungarian National Authority for Data Protection and Freedom of Information, postal address: 1530 Budapest, PO Box: 5., address: 1125 Budapest,Szilágyi Erzsébet fasor 22/c, Telephone: +36 (1) 391-1400; Fax: +36 (1) 391-1410; E-mail: ugyfelszolgalat@naih.hu; website: www.naih.hu).

**6. Terms and definitions**

personal data:

personal data means any information relating to an identified or identifiable natural person (“Subscriber”); 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;

data controlling:

this refers to an operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

data controller:

data controller means the natural or legal person, public authority, agency or other body which,alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Member Statelaw; KOMPaaS (MCNtelecom GmbH) is considered as data controller.

data processor:

data processor means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the Service Provider;

consent:

of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

personal data breach:

means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

profiling:

means any form of automated processing of personal data consisting of the use of personal datato evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

third party:

means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor,are authorized to process personal data;