

General Terms and Conditions of BUSINESS for the Provision of Fixed-Line Data and Internet Services

Annex 2 DATA PROCESSING NOTICE

Data Protection Guidelines of Vodafone Magyarország Zrt.

How to use this data processing notice

In this data processing notice, we will explain to you how we process and protect your personal data when you are using our products and services.

Who we are

Name of data controller: Vodafone Magyarország Zrt. (hereinafter: “*Service Provider, Vodafone, or Controller*”),
Registered office: H-1096 Budapest, Lechner Ödön fasor 6.
Website: <https://www.vodafone.hu/magyar>
Company registration number: 01-10-044159
Registered by: Court of Registration of the Metropolitan Court of Budapest
Tax number: 11895927-2-44

How to contact us

Your opinion as a subscriber (hereinafter: “*subscriber*”) is important to us, so if you have any questions about our data processing notice, you can contact the data processing officer using one of the following contact methods:

- By e-mail to DPO-HU@vodafone.com OR
- By post to Vodafone Magyarország Zrt. (H-1476 Budapest Pf: 350) OR
- Via the Service Provider’s customer service line, by calling 1788 or +3612881788.

Our principles

Vodafone Magyarország Zrt. is committed to the respect of your personal data. Vodafone Magyarország Zrt. takes data protection, data security and compliance with data protection, the applicable data protection laws and with the legal provisions seriously.

Data Processing Notice of Vodafone Magyarország Zrt.

I. APPLICABLE LAWS

The Data Processing Notice of Vodafone Magyarország Zrt. is based on the following European Union and Hungarian laws:

EU laws:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 Processing Regulation or GDPR)

Hungarian laws:

- Hungary's Fundamental Law, Section VI
- Act V of 2013 on the Civil Code, Book Two, Part Three
- Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereinafter: Info Act)

Hungarian sector laws:

- Act CLV of 1997 on Consumer Protection
- Act C of 2000 on Accounting
- Act CVIII of 2001 on Certain Aspects of Electronic Commerce and Information Society Services
- Act C of 2003 on Electronic Communications (hereinafter: Electronic Communications Act)
- Act CXXXIII of 2005 on the Rules of Personal and Property Protection Activities and Activities of Private Detectives
- Act CXXVII of 2007 on Value Added Tax
- Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions relating to Commercial Advertising Activities
- Act CCXXII of 2015 on the General Rules of Electronic Administration and Trust Services
- Act CL of 2017 on the Rules of Taxation
- Decree 4/2012 (I.24) NMHH of the National Media and Infocommunications Authority on the special conditions of the data protection and privacy obligation associated with public electronic communications services, the special conditions of data processing and confidentiality, safety and integrity of networks and services, the processing of traffic and billing information, and the display of identification data and call diversion (hereinafter: Akr Decree)
- Decree 2/2015 (III. 30.) NMHH of the Hungarian National Media and Infocommunications Authority on the detailed rules of electronic communications subscription contracts (hereinafter: ESzR Decree)
- Government Decree 451/2016 (XII. 19) on the detailed rules of electronic administration

II. TERMS AND BASIC PRINCIPLES

TERMS

Personal data: any information relating to an identified or identifiable natural person (“data subject”); 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. Such specific personal data is in particular: name, address, place and date of birth, mother’s maiden name.

Data processing: any 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.

Controller: 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 Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Recipient: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Third party: 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 authorised to process personal data.

Consent of the data subject: 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: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Consumer: a natural person acting in the interests of objectives falling outside his independent occupation and economic activity, who buys, receives, uses, utilises goods or is the recipient of commercial communications and offers relating to the goods.

PRINCIPLES

In the course of processing personal data, the Service Provider takes into account the following principles; thus, personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (“purpose limitation”);
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (“storage limitation”);
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”).

The controller shall be responsible for, and be able to demonstrate compliance with the above (“accountability”).

LEGAL BASIS OF DATA PROCESSING

The Service Provider shall process personal data to the extent that at least one of the following conditions is met:

- a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

III. LEGAL BASIS, PURPOSE OF DATA PROCESSING PERFORMED BY VODAFONE MAGYARORSZÁG ZRT., CATEGORIES OF PERSONAL DATA AND DURATION OF DATA PROCESSING

1. Required for compliance with the legal obligation applicable to the controller: based on Section 154(1) of Act C of 2003 on electronic communications (Eht Act) and Section 11(1)(a) of Decree 2/2015 (III. 30.) NMHH on the detailed rules of electronic communications Subscription Contracts (ESzR Decree)

Purpose of data processing:

creation of the electronic communications services contract, definition, amendment of its content

Categories of personal data:

a) personal data, if applicable:

- aa) the subscriber's name, residential address, place of abode or registered office,
- ab) the subscriber's billing address, if necessary, his/her/its account number,
- ac) the subscriber's name at birth, place and date of birth, mother's name at birth,
- ad) in the case of a subscriber who is underage or partially restricted in respect of the legal representations relating to the signing of the subscription contract, the data of the legal representative according to aa)-ac) in the subscription contract for post-paid services,
- ae) the subscriber's company registration number or other registration number, if necessary, its bank account number,
- af) contact information.

Duration of the data processing:

Under Section 157(3) of the Electronic Communications Act (Eht.), the Service Provider shall process the personal data for this purpose from the time it is generated until the lapse of claims according to Section 143(2) arising from the subscription contract in connection with the data, i.e. 1 year following occurrence of delay or defective performance or in the event of dispute, until such dispute is closed.

2. Required for compliance with the legal obligation applicable to the controller: based on Act C of 2003 on electronic communications (Electronic Communications Act) Sections 154(2) and 157(2), and Decree 2/2015 (III. 30.) NMHH on the detailed rules of electronic communications subscription contracts (ESzR Decree), Sections 11(1)(a) and 11(3)

Purpose of data processing:

definition and billing of the fees arising from the electronic communications services contract, collection of the related fees and monitoring of the subscription contracts

Categories of personal data:

- a) the personal data specified in Article III. 1.)
- b) number or other identifier of the subscription station
- c) the subscriber's address and type of station
- d) number of total units chargeable in the settlement period
- e) caller and called subscriber's numbers

- f) type, direction, start time of the call or other service, duration of conversation taken place, size of data transmitted, in the case of a mobile phone service, the network and cell of the service provider network, unique identifier (IMEI) of the device used for using the service, in the case of IP networks, the identifiers used
- g) date of the call or other service
- h) data related to payment of fees and billing debt
- i) if debt is left behind, the events associated with the termination of the subscription contract
- j) in the case of phone services, data relating to other, non-electronic communications services that may be used by subscribers and users, in particular data relating to their billing
- k) data generated in the service provider's electronic communications network with regard to the use or attempted use of subscriber terminals illegally used for utilising the subscription service, in particular those banned by their owners
- l) Section 154(2) of the Electronic Communications Act, every piece of personal data required and sufficient for determining the fee and billing.

Duration of the data processing:

Under Section 157(3) of the Electronic Communications Act, the Service Provider may process the personal data for this purpose from the time it is generated until the lapse of claims according to Section 143(2) arising from the subscription contract in connection with the data, i.e. 1 year following occurrence of delay or defective performance or in the event of dispute, until such dispute is closed.

3. Required for compliance with the legal obligation applicable to the controller: based on Act C of 2003 on electronic communications (Electronic Communications Act) Section 154(3), and Section 11(1)(a) of Decree 2/2015 (III. 30.) NMHH on the detailed rules of electronic communications subscription contracts (ESzR Decree)

Purpose of data processing:

providing the electronic communications service

Categories of personal data:

- a) the personal data specified in Article III. 1.)
- b) the personal data specified in Article III. 2.)
- c) the personal data absolutely necessary from a technical point of view to provide the service

Duration of the data processing:

In respect of Article III.3.a), under Section 157(3) of the Electronic Communications Act, the Service Provider stores the personal data for this purpose from the time it is generated until the lapse of claims according to Section 143(2) arising from the subscription contract in connection with the data, i.e. 1 year following occurrence of delay or defective performance or in the event of dispute, until such dispute is closed.

In respect of Article III.3.b), under Section 157(3) of the Electronic Communications Act, the Service Provider stores the personal data for this purpose from the time it is generated until the lapse according to Section 143(2) of the Electronic Communications Act, i.e. 1 year following occurrence of delay or defective performance or in the event of dispute, until such dispute is closed.

In respect of Article III.3.c), the service provider retains the data solely in the extent that and for the duration which is absolutely necessary for providing the service.

4. Required for compliance with the legal obligation applicable to the controller: based on Act C of 2003 on electronic communications (Electronic Communications Act) Section 142(1) and (2), and Section 21(1) and (3) of Decree 2/2015 (III. 30.) NMHH on the detailed rules of electronic communications subscription contracts (ESzR Decree)

Purpose of data processing:

issuing the bill and itemised bill annex

Categories of personal data:

The mandatory data to be included in the bill is the name and address of the service user.

In the bill annex, the Service Provider is obliged to state the charges payable, broken down by all call directions with different rates, if no call directions are used, by terminating provider, premium-rate calls, remote voting, SMS, MMS, for calls received, by charges payable; it is also obliged to state the fee of non-phone services used via the phone service. In the bill annex, the Service Provider shall separately indicate charges on voice and non-voice calls, as well as the charging periods.

Duration of the data processing:

The data may be processed until the lapse according to Section 143(2) of the Electronic Communications Act, i.e. the Service Provider shall store it for 1 year following occurrence of delay or defective performance or in the event of dispute, until such dispute is closed.

Moreover, the Service Provider advises the subscriber that the bill annex provided by the service provider under Section 142(1) of the Electronic Communications Act cannot contain any data that can be used for clearly identifying the called party.

5. Required for compliance with the legal obligation applicable to the controller: according to Chapter X of Act CXXVII of 2007 on Value-Added Tax.

Purpose of data processing:

issuing the invoice and determining the tax

Categories of personal data:

The mandatory data to be included in the bill is the name and address of the service user.

In the bill annex, the Service Provider is obliged to state the charges payable, broken down by all call directions with different rates, if no call directions are used, by terminating provider, premium-rate calls, remote voting, SMS, MMS, for calls received, by charges payable; it is also obliged to state the fee of non-phone services used via the phone service. In the bill annex, the Service Provider shall separately indicate charges on voice and non-voice calls, as well as the charging periods.

Duration of the data processing:

Based on Chapters IX and XXVI of Act CL of 2017 on the Rules of Taxation: five years from the last day of the calendar year in which the tax return must be filed.

6. Required for compliance with the legal obligation applicable to the controller: based on Act C of 2000 on Accounting

Purpose of data processing:

reporting and following up on accounting documents

Categories of personal data:

The mandatory data to be included in the bill is the name and address of the service user.

In the bill annex, the Service Provider is obliged to state the charges payable, broken down by all call directions with different rates, if no call directions are used, by terminating provider, premium-rate calls, remote voting, SMS, MMS, for calls received, by charges payable; it is also obliged to state the fee of non-phone services used via the phone service. In the bill annex, the Service Provider shall separately indicate charges on voice and non-voice calls, as well as the charging periods.

Duration of the data processing:

Under Section 169 of Act C of 2000 on Accounting, the Service Provider must retain, in a legible form, the accounting document that supports accounting records for at least 8 years from disclosure of the financial statements, taking into account that the disclosure deadline is the last day of the 5th month following the last day of the business year.

7. Required for compliance with the legal obligation applicable to the controller: based on Act C of 2003 on electronic communications (Electronic Communications Act) Section 142(1) and (2), Decree 4/2012 (I.24) NMHH of the National Media and Infocommunications Authority on the special conditions of the data protection and privacy obligation associated with public electronic communications services, the special conditions of data processing and confidentiality, safety and integrity of networks and services, the processing of traffic and billing information, and the display of identification data and call diversion (Akr.), Section 7, and Decree 2/2015 (III.30) NMHH on the detailed rules of electronic communications subscription contracts (ESzR.), Section 21(2)-(4)

Purpose of data processing:

issuing the call detail record for the subscriber, to check the accuracy of the invoice

Categories of personal data:

The call detail record must state, for each service and service provider, the following information:

- a) number called (details below)
- b) start time of call
- c) call duration
- d) price of the call unit
- e) price of the call

In case of non-voice data connections or calls, the call detail record contains the following information, grouped by access type:

- a) time of the non-voice data transmission
- b) volume of data transmission or, in the case of time-based invoicing, duration of data transmission

- c) unit traffic, or, in the case of time-based invoicing, price per unit time
- d) charges of the data transmission

Duration of the data processing:

Under Section 157(3) of the Electronic Communications Act, the Service Provider may process the personal data for this purpose from the time it is generated until their lapse according to Section 143(2), i.e. 1 year following occurrence of delay or defective performance or in the event of dispute, until such dispute is closed.

Moreover, the Service Provider advises the subscriber that:

- The call detail record mentioned in Section 142(2) of the Electronic Communications Act cannot contain any data that can be used for clearly identifying the called party. If the subscriber requests that a call detail record be provided to it under Section 142(2) of the Electronic Communications Act, then prior to complying with such request, the service provider is obliged to advise the subscriber that with the call detail record the user of the electronic communications service may acquire personal data of individuals using the service other than the subscriber, and the subscriber shall only be entitled to access such personal data if the users have their consent thereto.
- The Service Provider is not obliged to check the existence or content of consent, and the subscriber shall bear exclusive liability for such consent.
- In the report, even if the subscriber requests so, the service provider cannot indicate the phone numbers of organisations communicated by the Authority as “unidentifiable numbers” at least five days prior to receipt of the subscriber’s request, where
 - services are provided mostly to anonymous callers, from which sensitive data of the caller can be deduced, in particular calls to church, spiritual or addiction helplines;
 - it is made possible for mostly anonymous callers to report crimes (anonymous witness lines);
 - emergency services are called.

The NMHH keeps an electronic registry of unidentifiable numbers (hereinafter: unidentifiable numbers registry). An application for listing a number as an unidentifiable number must be submitted to the NMHH. The NMHH decides on the application for listing the number indicated by the applicant as an unidentifiable number within fifteen days. The NMHH must ensure that electronic communications service providers can access continuously and electronically, without paying a special fee, the list of numbers included on the unidentifiable numbers registry.

8. Required for compliance with the legal obligation applicable to the controller: based on Act C of 2003 on electronic communications (Electronic Communications Act) Section 129(2) and (2a) and (2b), and Section 32/B(4) of Decree 2/2015 (III. 30.) NMHH on the detailed rules of electronic communications subscription contracts (ESzR Decree)

Purpose of data processing:

Verification of identity

Categories of personal data:

number of the subscriber’s official identity document and personal identification data

Duration of the data processing:

If the contract is made, the Service Provider is obliged to retain the personal data for 1 year following termination of the subscription contract or, in the event of dispute, until such dispute is closed.

In the case of prepaid services, the Service Provider is obliged to verify the authenticity of the identification data on the identity document presented by the subscriber or the subscriber's representative, directly in the official identity documents registry (database of the Deputy State Secretariat of the Ministry of the Interior in charge of Keeping Registries, or any database substituting it). In other cases, the Service Provider is entitled to verify the authenticity of identification data directly/via an intermediary.

9. Required for compliance with the legal obligation applicable to the controller: based on Act C of 2003 on electronic communications (Electronic Communications Act) Section 159/A (1) - (2)

Purpose of data processing:

Compliance with data retention obligations with the purpose of crime-fighting, national security and homeland defence

Categories of personal data:

(1)

(a) in the case of fixed phone or mobile phone services, internet access services, internet phone, internet mailing services or combination thereof, the personal data of the subscriber specified in the individual subscription contract;

(b) in the case of fixed phone or mobile phone services, internet access services, internet phone, internet mailing services or combination thereof, the number of the subscriber's or user's terminal or subscriber access point or other permanent technical IDs necessary for the unique identification of the subscriber or user, specified in the subscription contract or otherwise allocated to the subscriber or user by the electronic communications service provider;

(c) in the case of fixed phone services or fixed internet access services, or combination thereof, address where the subscriber's or user's terminal or subscriber's access point is installed and its type;

(d) in the case of fixed phone or mobile phone services, internet access services, internet phone, internet mailing services or combination thereof, the numbers of subscribers or users participating in the communication, their unique technical IDs, user IDs, type of electronic communications service used, date, start and end time of communication;

(e) in the case of call diversion and call forwarding utilised together with use of fixed phone or mobile phone services or combination thereof, the intermediary subscriber or user numbers participating in the call structure;

(f) in the case of mobile phone services, the device IDs (IMEI) or mobile subscriber ID (IMSI) of the participants to the communication, used when using the service;

(g) in the case of mobile phone services, the network and cell ID of the service provider at the start of communication, and data that permits identification of the actual geographical location of the cell pertaining to the cell ID at the time of providing the service;

(h) in the case of internet-based electronic mailing, internet-based phone services or combination thereof, the data specified in (d) in respect of the communication started towards an intended recipient;

(i) in the case of internet access, internet-based electronic mailing, internet-based phone services or combination thereof, the type of the electronic communications service and the date, start and end time of the subscriber's or user's use of the service, IP address, user ID, number used for using it;

(j) in the case of internet access, internet-based electronic mailing, internet-based phone services or combination thereof, the data necessary for monitoring any conversion by the electronic communications service provider of the unique technical IDs of the subscribers or users (IP address, port number);

(k) in the case of prepaid mobile phone services with anonymous calling card, the date and time of the first use of the service and ID of cell from which it was activated.

(2) The obligation to retain and report data also extends to the data specified in paragraph (1), generated or processed during unsuccessful calls.

Duration of the data processing:

The Service Provider is obliged to retain the data specified in paragraph (1) points (a)-(c) for 1 year following termination of the subscription contract and those in points(d)-(k), for 1 year from when they were generated, and those in paragraph (2) for half a year from when they were generated.

10. Required for compliance with a legal obligation referring to the data controller: based on Act CLV of 1997 on consumer protection, Section 17/A (5) and (7) and Section 17/B. (5)

Purpose of data processing:

Investigating subscriber complaints

Categories of personal data:

a) consumer's (subscriber's) name, address,

b) place, time, manner of filing the complaint,

c) detailed description of the consumer's (subscriber's) complaint, list of papers, documents and other evidence presented by the consumer (subscriber),

d) the company's (Service Provider's) statement on its position regarding the consumer's (subscriber's) complaint, if the complaint can be investigated immediately,

e) signature of the person drawing up the report and – except for verbal complaints communicated by phone or using other electronic communications services – the consumer's (subscriber's) signature,

f) place and date of drawing up the report,

g) unique ID of the complaint in the case of verbal complaints communicated by phone or using other electronic communications services,

h) the subscriber's call number or other ID (invoice payer ID) required for clearly identifying the subscriber;

Duration of the data processing:

The Service Provider is obliged to retain the complaint documentation data for 5 years or, in the event of dispute, until such dispute is closed.

11. Required for compliance with the legal obligation applicable to the controller: based on Act C of 2003 on electronic communications (Electronic Communications Act) Section 138(8), and Section 25(1) of Decree 2/2015 (III. 30.) NMHH on the detailed rules of electronic communications subscription contracts (ESzR Decree)

Purpose of data processing:

Examining inquiries

Categories of personal data:

- a) subscriber's name, address,
- b) place, time, manner of submitting the inquiry,
- c) detailed description of the subscriber's inquiry, list of papers, documents and other evidence presented by the subscriber,
- g) unique ID of the complaint in the case of verbal complaints communicated by phone or using other electronic communications services,
- h) the subscriber's call number or other ID (invoice payer ID) required for clearly identifying the subscriber;

Duration of the data processing:

Under Section 138(10) of the Electronic Communications Act, the service provider is obliged to record inquiries or complaints concerning the subscription relationship, received by the service provider's customer service, and any phone communication between the service provider and the subscriber, as specified by specific laws, in a retrievable manner for at least 1 year.

12. Required for compliance with the legal obligation applicable to the controller: based on Act C of 2003 on electronic communications (Electronic Communications Act) Section 141(2), and Section 22(7) of Decree 2/2015 (III. 30.) NMHH on the detailed rules of electronic communications subscription contracts (ESzR Decree)

Purpose of data processing:

Investigating error reports and troubleshooting

Categories of personal data:

- a) notification address or other ID of the subscriber
- b) subscriber's call number or other ID
- c) a description of the error
- d) time and date of the error report (year, month, day, hour)
- e) actions taken to locate the cause of the error and their results
- f) cause of the error
- g) method, time and date when error was eliminated (year, month, day, hour) and the result (no success and cause);
- h) method and time of the notification to the subscriber, in particular, manner and time of the confirmation of the subscriber's report and notifications about the data mentioned in (g).

Duration of the data processing:

Under Section 141(1) of the Electronic Communications Act, the service provider is obliged to record the error reports, the results of the error definition process and troubleshooting measures taken in a retrievable manner, by voice record or by other electronic means, and to retain such records while observing the data processing rules for at least one year or, in the event of dispute, until such dispute is closed.

Under Section 25(1) of the Eszr Decree, the service provider is obliged to make a voice recording of subscriber complaints and error reports received by the phone customer service, and retain it in a retrievable manner for 2 years following the report date or, in the event of dispute, until such dispute is closed.

13. Required for compliance with the legal obligation applicable to the controller: based on Act C of 2003 on electronic communications (Electronic Communications Act) Section 138(10)

Purpose of data processing:

recording inquiries or complaints concerning the subscription relationship and phone communication between the service provider and the subscriber

Categories of personal data:

voice recordings

Duration of the data processing:

Under Section 25(1) of the Eszr Decree, the service provider is obliged to make a voice recording of subscriber complaints and error reports received by the phone customer service, and retain it in a retrievable manner for 2 years following the report date or, in the event of dispute, until such dispute is closed.

14. Required for compliance with the legal obligation applicable to the controller: based on Section 6(1) of Decree 2/2015 (III. 30.) NMHH on the detailed rules of electronic communications Subscription Contracts (ESzR Decree)

Purpose of data processing:

contact, notifications

Categories of personal data:

e-mail address

Duration of the data processing:

The Service Provider processes the personal data for 1 year following termination of the subscription contract or, in the event of dispute, until such dispute is closed.

15. The legal basis is that processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Purpose of data processing:

verification of the purchasing limit specified in Article 3.1 of the GTC, prior to entering into a pre-paid subscription contract

Categories of personal data:

- a) number of and data contained in the subscriber's or his/her legal representative's official identity document
- b) number of prior purchases

Duration of the data processing:

The Service Provider processes the personal data for 1 year following termination of the subscription contract or, in the event of dispute, until such dispute is closed.

16. The legal basis is that processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Purpose of data processing:

assessment of the contracting party's creditworthiness prior to entering into a post-paid subscription contract

Categories of personal data:

- a) other phone numbers of the subscriber
- b) number of and data contained in the subscriber's or his/her legal representative's official identity document
- c) the following data entered on the so-called information data form:
 - ca) subscriber's name
 - cb) marital status
 - cc) apartment/house data
 - cd) highest educational attainment
 - ce) type of bankcard owned
 - cf) workplace data
 - cg) total net monthly income of the household
 - ch) type of employment
 - ci) duration of employment at current employer
 - cj) economic sector of employment
 - ck) type and number of current mobile phone subscriptions
- d) data of the proof of employment
- e) data of the proof of retirement
- f) data of bank account statement proof
- g) invoice data from other mobile service provider

Duration of the data processing:

The Service Provider processes the personal data for 1 year following termination of the subscription contract or, in the event of dispute, until such dispute is closed.

17. The legal basis is that processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Purpose of data processing:

Fulfilment of the conditions required for providing the Vodafone Family (Vodafone Kid) and Vodafone You Promotion Services

Categories of personal data:

- a) serial number of official address card of relatives younger than 18
- b) date of birth of relative under 18
- c) date of birth of User entitled to the discount
- d) number of identity card of the User entitled to the discount.

Duration of the data processing:

The Service Provider processes the personal data for 1 year following termination of the subscription contract or, in the event of dispute, until such dispute is closed.

18. The legal basis is that processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Purpose of data processing:

checking the conformity and quality of the service

Categories of personal data:

- a) the personal data specified in Article III. 1.)
- b) the personal data specified in Article III. 2.)
- c) the personal data specified in Article III. 11.c.)
- a) the personal data specified in Article III. 13.)

Duration of the data processing:

- Personal data specified in Article III.18.a) is processed for the data processing duration specified in Article III.1.
- Personal data specified in Article III.18.b) is processed for the data processing duration specified in Article III.2.
- Personal data specified in Article III.18.c) is processed for the data processing duration specified in Article III.11.
- Personal data specified in Article III.18.d) is processed for the data processing duration specified in Article III.13.

19. Based on the subscriber's consent

Purpose of data processing:

personal and property protection at the shops of Vodafone Magyarország Zrt. and its reseller network

Categories of personal data:

- a) video recordings

Duration of the data processing:

Under Section 31(2) of Act CXXXIII of 2005 on the Rules of Personal and Property Protection Activities and Activities of Private Detectives, the video recordings, voice recordings and video and voice recordings, unless they are used, must be destroyed and erased no later than when 3 working days have passed from the recording.

The Service Provider uses the recordings made solely for the subsequent investigation of the circumstances of crimes committed or other extraordinary events – falling within the scope of surveillance – in the monitored area.

20. Based on the subscriber's consent

Purpose of data processing:

processing of the list of names of subscribers

Categories of personal data:

- a) name
- d) address (registered office)
- e) subscriber's phone number
- e) manner of use of the terminal (upon request) (phone/fax)

Duration of the data processing:

The service provider processes the personal data for this purpose until the consent is withdrawn or in absence of this, until termination of the subscription contract or, in the event of dispute, until such dispute is closed.

The Service Provider shall process the subscriber's data in the directory database in accordance with the subscriber's statement made when signing the subscription contract. Should the subscriber intend to modify his/her/its previous statement regarding the data processing, the Service Provider shall arrange for the appropriate procedure free of charge.

21. Based on the subscriber's consent

Purpose of data processing:

providing or transmitting location services outside the traffic data, by phone or other means of electronic communications (e.g. sms, mms, e-mail), via automated calling systems and internet-based customer service systems or by post.

Categories of personal data:

- a) address of base station or
- b) geo-coordinates

Duration of the data processing:

The service provider processes the personal data for this purpose until the consent is withdrawn; in other cases, the electronic communications service provider is obliged to retain the personal data for 1 year following their generation or, in the event of dispute, until such dispute is closed.

22. Based on the subscriber's consent

Purpose of data processing:

transmission of customised offers for direct marketing purposes, by phone or other means of electronic communications (e.g. sms, mms, e-mail), via automated calling systems and internet-based customer service systems or by post.

Categories of personal data:

- a) the personal data specified in Article III. 1.)
- b) the personal data specified in Article III. 2.)
- c) the personal data specified in Article III. 4.)
- d) the personal data specified in Article III. 7.)
- e) browsing history, visit and purchase data (when using the websites and Online Shop or mobile applications operated by Vodafone Magyarország Zrt.)

Duration of the data processing:

The service provider processes the personal data for this purpose until the consent is withdrawn or in absence of this, and in other cases:

Personal data specified in Article III.22.a) is processed for the data processing duration specified in Article III.1.

Personal data specified in Article III.22.b) is processed for the data processing duration specified in Article III.2.

Personal data specified in Article III.22.c) is processed for the data processing duration specified in Article III.4.

Personal data specified in Article III.22.d) is processed for the data processing duration specified in Article III.7.

Personal data specified in Article III.22.e) is processed until termination of the subscription contract or, in the event of dispute relating to payment of charges or legal dispute, until such dispute is closed.

23. Based on the subscriber's consent

Purpose of data processing:

market research by phone or via other means of electronic communications (e.g. sms, mms, e-mail), via automated calling systems and internet-based customer service systems, or by post

Categories of personal data:

- a) the personal data specified in Article III. 1.)
- b) the personal data specified in Article III. 2.)
- c) the personal data specified in Article III. 4.)
- d) the personal data specified in Article III. 7.)
- e) browsing history, visit and purchase data (when using the websites and Online Shop or mobile applications operated by Vodafone Magyarország Zrt.)

Duration of the data processing:

The service provider processes the personal data for this purpose until the consent is withdrawn or in absence of this, and in other cases:

Personal data specified in Article III.23.a) is processed for the data processing duration specified in Article III.1.

Personal data specified in Article III.23.b) is processed for the data processing duration specified in Article III.2.

Personal data specified in Article III.23.c) is processed for the data processing duration specified in Article III.4.

Personal data specified in Article III.23.d) is processed for the data processing duration specified in Article III.7.

Personal data specified in Article III.23.e) is processed until termination of the subscription contract or, in the event of dispute relating to payment of charges or legal dispute, until such dispute is closed.

24. Based on the subscriber's consent

Purpose of data processing:

providing value-added services (e.g. device insurance, travel insurance) by phone or via other means of electronic communications (e.g. sms, mms, e-mail), via automated calling systems and internet-based customer service systems, or by post

Categories of personal data:

- a) the personal data specified in Article III. 1.)
- b) the personal data specified in Article III. 2.)
- c) the personal data specified in Article III. 4.)
- d) the personal data specified in Article III. 7.)
- e) browsing history, visit and purchase data (when using the websites and Online Shop or mobile applications operated by Vodafone Magyarország Zrt.)

Duration of the data processing:

The service provider processes the personal data for this purpose until the consent is withdrawn or in absence of this, and in other cases:

Personal data specified in Article III.24.a) is processed for the data processing duration specified in Article III.1.

Personal data specified in Article III.24.b) is processed for the data processing duration specified in Article III.2.

Personal data specified in Article III.24.c) is processed for the data processing duration specified in Article III.4.

Personal data specified in Article III.24.d) is processed for the data processing duration specified in Article III.7.

Personal data specified in Article III.24.e) is processed until termination of the subscription contract or, in the event of dispute relating to payment of charges or legal dispute, until such dispute is closed.

25. The legal basis is that processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Purpose of data processing:

entering into pre-paid subscription contracts for minors aged 14-18

Categories of personal data:

- a) the subscriber's name, residential address, place of abode or registered office,
- b) the subscriber's name at birth, place and date of birth, mother's name at birth,
- c) contact information.

Duration of the data processing:

Under Section 157(3) of the Electronic Communications Act (Eht.), the Service Provider shall process the personal data for this purpose from the time it is generated until the lapse of claims according to Section 143(2) arising from the subscription contract in connection with the data, i.e. 1 year following occurrence of delay or defective performance or in the event of dispute, until such dispute is closed.

26. The legal basis is that processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Purpose of data processing:

performance of preliminary data processing

Categories of personal data:

- a) the personal data specified in Article III. 1.)
- b) the personal data specified in Article III. 2.)
- c) the personal data specified in Article III. 4.)
- d) the personal data specified in Article III. 7.)
- e) the personal data specified in Article III. 11.c.)
- f) the personal data specified in Article III. 13.)
- g) data relating to mobile number porting (ported number, recipient service provider, donor service provider, time to port)
- h) all the data processed in the Service Provider's network which is suitable for determining the geographical location of the terminal using the service

i) browsing history, visit and purchase data (when using the websites and Online Shop or mobile applications operated by Vodafone Magyarország Zrt.)

Duration of the data processing:

Personal data specified in Article III.26.a) is processed for the data processing duration specified in Article III.1.

Personal data specified in Article III.26.b) is processed for the data processing duration specified in Article III.2.

Personal data specified in Article III.26.c) is processed for the data processing duration specified in Article III.4.

Personal data specified in Article III.26.d) is processed for the data processing duration specified in Article III.7.

Personal data specified in Article III.26.e) is processed for the data processing duration specified in Article III.11.

Personal data specified in Article III.26.f) is processed for the data processing duration specified in Article III.13.

The Service Provider processes the personal data specified in Article III.26.g) for 1 year following termination of the subscription contract or, in the event of dispute, until such dispute is closed.

The Service Provider is obliged to retain the personal data specified in Article III.26.h) and i) for 1 year following its generation, or, in the event of dispute, until such dispute is closed.

27. Data processing of natural and legal persons relating to business subscriptions

The legal basis is that processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Purpose of data processing:

Identification of natural and legal persons as business subscribers, contact with them and attaining the purposes specified in the previous points

Scope of data processed:

a) name of company as Subscriber, mailing address, phone number, e-mail address, company name, address of headquarters, registered office and local office, status of registered office, legal status of the company, its company registration number, trader licence number, tax number, bank account number, date of foundation, size of share capital

b) name of invoice payer, mother's name, identity document number, registered office, place and date of birth, permanent and mailing address, tax number, company registration number

c) contact person's or representative's name, address, phone number, e-mail address, fax number, position, place and date of birth, mother's name, citizenship, type and number of identity document

Duration of the data processing:

The Service Provider erases the personal data after the data processing purpose has ceased.

IV. CONDITIONS AND MANNER OF TRANSMITTING PERSONAL DATA TO THIRD PARTIES

According to the effective data protection regulations, the Service Provider uses the services of data processors and third parties if the data processing is required for compliance with a legal obligation referring to the data controller, i.e. if permitted by legal provisions, or if it is required for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

1.) Under Section 145 of the Electronic Communications Act

(1) The electronic communications service provider that provides domestic call origination services is obliged to ensure for all of its end users, free of charge – in the case of public phone stations, without use of a payment instrument – access to emergency services and emergency service stations via the statutory numbers, including the single European emergency number “112”.

(2) In order to answer emergency calls, the phone provider is obliged to make available – in the manner specified in specific laws – the caller’s identification and position data to the emergency services and emergency service stations, even in absence or withdrawal of the caller’s consent to the blocking of caller ID display and to the processing of location data.

2.) Under Section 157 (5) of the Electronic Communications Act, the investigating authorities and internal crime prevention and crime investigation, as well as counter-terrorism units and national security services specified in the act on the police, as specified by the law, and the Authority – during exercise of its powers stipulated by Section 11(3) – may monitor, intercept or store the communications, or intervene otherwise in the message or communication for the purpose of their monitoring.

3.) Under Section 157 (8) of the Electronic Communications Act, the Service Provider is authorised to hand over the following data to the National Bank of Hungary acting within the scope of its duties relating to the supervision of the financial intermediation system, as part of a procedure initiated in matters of insider trading, market manipulation, performance of unlicensed services, failure to comply with the reporting and disclosure obligation relating to net short positions, restrictions on short transactions and inspection of compliance with rules of company acquisitions:

- a) the subscriber’s last name and first name;
- b) the subscriber’s name at birth;
- c) the subscriber’s place of residence, information about his/her place of abode;
- d) number or other identifier of the subscription station;
- e) subscriber numbers calling subscriber and called by the subscriber,
- f) date and start time of the call or other service.

4.) Under Section 157 (9) of the Electronic Communications Act, the Service Provider may hand over from the data specified in Section 157 (2) that which is required for the purpose of data processing, within the data retention time stipulated by Section 157 (3):

- a) to those who perform, based on the electronic communications service provider’s orders, billing, debt management, sales management and customer information;
- b) to authorities authorised by law to settle billing and sales disputes;
- c) to the bailiff, according to provisions of the Act on Judicial Execution;
- d) if the data subject is unable to give his/her consent, for inevitable causes, to the authorised authority, based on the request of the authority authorised by specific laws to access the data, in order to prevent the data subject’s or another person’s vital interests, or to eliminate or prevent danger threatening the lives, physical integrity or assets of people;
- e) to the consumer protection authority, according to the provisions of the Consumer Protection Act;

5.) Under Section 157 (10) of the Electronic Communications Act, the Service Provider – to ensure the discharge of the statutory duties of investigating authorities, prosecution office, court and national security service authorised to request data under special laws – is obliged

to hand over or make available, upon request, the data available at the electronic communications service provider under Section 157(2) of the Electronic Communications Act.

6.) Under Section 157 (11) of the Electronic Communications Act, the electronic communications service provider, if such data is available to it, must hand over upon request of the authority competent in offence matters, in order to identify the person committing an offence by misusing the emergency numbers, the following data in respect of the phone number that called the emergency number

- a) the subscriber's last and first name, place and date of birth, mother's name at birth and last name, address and notification address, or
- b) in the case of a non-natural person subscriber, its company name, registered office, local office, representative's last name and first name.

7.) Under Section 156 (16) and (17) of the Electronic Communications Act, the electronic communications service provider – to ensure the discharge of the statutory duties of investigating authorities, prosecution office, court and national security service authorised to request data under special laws – is obliged to determine and transfer to them, upon their request, location data outside the traffic data relating to the user and the subscriber. The electronic communications service provider, upon request for data by an authority conducting an arrest warrant procedure, in order to conduct an arrest warrant procedure, is obliged to determine and transfer to it the location data outside the traffic data relating to the user and the subscriber.

8.) Under Section 158 of the Electronic Communications Act, electronic communications service providers are entitled, for the purpose of preventing the circumvention of obligations to pay fees and other contractual obligations and refusal to sign a contract, to take the subscriber identification data from the scope of data legitimately processed under Section 157, and create a common database. The subscriber's data may be transferred or included in the common database if

- a) because of bill debt, the service provider has terminated the contract or partially or fully restricted the subscriber's possibility to use the service, or
- b) because of bill debt, the service provider has taken court or official action against the subscriber or the subscriber's place of abode is unknown, or
- c) the applicant or the subscriber, to cause damage, has mislead or attempts to mislead the service provider (in particular if a document provided for identification is obviously false, falsified or invalid).

The service provider is obliged to inform the subscriber immediately about the transfer of data.

Data may be requested from the database by

- a) the electronic communications service provider
- b) the body or authority indicated in Section 157(8)-(10)
- c) any consumer in respect of what data the records contain about him/her.

9.) Under Section 47 (9a) of the Consumer Protection Act, the electronic communications service provider from whose network the call was initiated, upon the instruction of the consumer protection authority, is obliged to communicate the call start time and duration data it is processing.

If the Service Provider engages an external partner to process certain elements of the personal data that is processed by it, the confidential and secret processing of your personal data, identical to the data processing practice of our company, is guaranteed in the private contracts concluded by the Service Provider, the Hungarian legislation and compliance with the legal regulations and requirements of the European Union.

Certain agents and subcontractors of Vodafone and subsidiaries of the Vodafone Group may cooperate as processors in the provision of Vodafone Hungary's services, thus in particular in the performance of technical operations. Due to the Service Provider's business decision, both third-party data processors and data controllers may be subject to change. The Service Provider shall inform the subscriber about any such changes. The updated list of the current data controller and data processor companies is available at <http://www.vodafone.hu/vodafonerol/aszf> and in Vodafone's customer service centres.

Depending on the Service Provider's business decision, the person of the data processors and data controllers may change in the future. We announce these changes in our bill letters and attachments thereto. In order to be able to assert your rights to informational self-determination and the protection of your personal data, please monitor this information continuously.

V. RIGHTS OF THE DATA SUBJECT

Your rights relating to the Service Provider's data processing are:

1. Information
2. Access
3. Rectification
4. Erasure
5. Restriction
6. Data portability
7. Objection

1. Information - Information to be provided

Where personal data relating to you is collected from you, the Service Provider shall, at the time when personal data is obtained, provide you with all of the following information:

- a) the identity and the contact details of the controller;
- b) the contact details of the data protection officer;
- c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- d) where the processing is based on a legitimate interest, the legitimate interests pursued by the controller or by a third party;
- e) the recipients or categories of recipients of the personal data, if any;
- f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the European Commission.
- g) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- h) your right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning you or to object to processing as well as the right to data portability;
- i) where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- j) the right to lodge a complaint with a supervisory authority;
- k) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

2. Right of access by the data subject

You shall have the right to obtain from the controller confirmation as to whether or not personal data concerning you is being processed, and, where that is the case, access to the personal data and the following information:

- a) purposes of the data 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 organisations;
- 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;
- e) the right to lodge a complaint with a supervisory authority;
- g) where the personal data is not collected from the data subject, any available information as to their source;
- h) the existence of automated decision-making, including profiling, and, 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.

3. Right to rectification

You shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning you. Taking into account the purposes of the processing, you shall have the right to have incomplete personal data completed.

The subscriber shall forthwith notify the Service Provider about any changes in its data recorded in the subscription contract. The Service Provider shall not be liable for damages arising from the subscriber's failure to immediately notify the Service Provider about such changes; however, the Service Provider may claim indemnification from the subscriber for the damages that have occurred with regard to the subscriber's breach of contract.

The subscriber may at any time request the Service Provider to correct its personal data managed by the Service Provider.

4. Right to erasure ("right to be forgotten")

You shall have the right to obtain from the controller the erasure of personal data concerning you 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) you withdraw your consent on which the processing is based, and there is no other legal ground for the processing;
- c) you object to the processing of your data
- 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.

5. Right to restriction of processing

You shall have the right to obtain from the Service Provider restriction of processing where one of the following applies:

- a) you contest the accuracy of the personal data, for a period enabling the Service Provider to verify the accuracy of the personal data;
- b) the processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;
- c) the Service Provider no longer needs the personal data for the purposes of the processing, but they are required by you for the establishment, exercise or defence of legal claims;
- d) you have objected to processing; in this case, the restriction applies to the period during which it is established whether the legitimate grounds of the controller override yours.

6. Right to data portability

You have the right to receive the personal data concerning you, which you have 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) processing is based on consent or contract; and
- b) the processing is carried out by automated means.

7. Right to object

You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you which is based on point (e) or (f) of Article 6(1) of the General Data Processing Regulation, including profiling based on those provisions. In this case, the Service Provider shall no longer process the personal data unless the Service Provider 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.

You can exercise your above rights as a data subject as follows:

- By post to the Customer Service Centre of Vodafone Magyarország Zrt. (H-1476 Budapest Pf: 350.),
- by e-mail to the Service Provider's e-mail address corporate.hu@vodafone.com
- via the Service Provider's customer service line, by calling 1788 or +3612881788.
- at the Service Provider's shops and in its reseller network

Withdrawal of consents given in the Data Protection statements:

The subscriber may at any time withdraw his/her consent given in the data protection statements at the postal address of Vodafone Magyarország Zrt. Customer Service H-1476 Budapest, Pf.: 350. or by e-mail to corporate.hu@vodafone.com or request that they be amended.

You can address your complaints about the processing of your personal data to the following:

- Data protection officer of Vodafone Magyarország Zrt.
 - By e-mail DPO-HU@vodafone.com OR
 - by post to Vodafone Magyarország Zrt. (H-1476 Budapest Pf: 350) OR
- the National Media and Infocommunications Authority (NMHH, H-1015 Budapest, Ostrom u. 23-25., H-1525 Budapest Pf. 75.) OR

- Hungarian National Authority for Data Protection and Freedom of Information (NAIH, H-1125 Budapest, Szilágyi Erzsébet fasor 22/C. H-1530 Budapest, Pf.: 5.).

Upon infringement of its rights by the Service Provider related to the processing and protection of his/her personal data, the subscriber or user may refer to the court with jurisdiction and competence (birosag.hu) and claim indemnification.

VI. DATA SECURITY REQUIREMENTS

1. The Service Provider protects the confidentiality of the personal data of subscribers and users that has come into its possession and is processed by it in connection with the service and operation of its network, in compliance with the General Data Processing Regulation, the Information Act, the Electronic Communications Act, the EszR Decree, and the Akr. Decree; the Service Provider enforces these protection measures in the course of processing personal data and the personal data processing activities of data processors or third parties.
2. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Service Provider 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:
 - a) the pseudonymisation and encryption of personal data;
 - b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical and technical incident;
 - d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised 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, unless he or she is required to do so by Union or Member State law.

The Service Provider – if necessary, together with other service providers – is obliged to ensure through technical and organisational measures the protection of the security of the service and the subscribers' personal data processed in the course of providing the electronic communications service.

3. Violation of the subscribers' personal data shall mean the accidental or illegal processing by controller or processor of the personal data transferred, stored or otherwise processed by controller or processor in connection with the provision of the publicly available electronic communications services, in particular its destruction, loss, modification, unauthorised disclosure, public disclosure or unauthorised access thereto.

When noticing a violation of the personal data, the electronic communications service provider is obliged to immediately report this to the National Media and Infocommunications Authority (hereinafter: NMHH).

The electronic communications service providers are obliged to keep a register about the events of violation of personal data, and such register shall contain material circumstances, effects of such events and corrective measures taken by the electronic communications service provider. The register shall include all facts and circumstances based on which the NMHH is able to check whether or not the Service Provider is in compliance with the regulations. The register shall only contain information necessary to reach the above-mentioned objectives.

If the violation of personal data is anticipated to prejudice the personal data or privacy of the subscriber or any other individual, the Service Provider is obliged to notify the subscriber or the individual about this without undue delay. The Subscriber or the individual does not need to be informed about the misuse of their personal data if electronic communications service provider can prove with satisfactory evidence to the NMHH that it has taken appropriate technical protective measures, or that such measures have been taken with regard to the data whose security was affected. Such technical protective measures must make the data impossible to interpret by persons not authorised to access them.

Without prejudice to the service provider's obligation to notify the affected subscribers or individuals, in case the service provider has not informed the subscriber or individual about the violation of personal data, the NMHH (after requesting the opinion of the National Authority of Data Protection and Freedom of Information) may oblige the service provider to do so, after taking into account possible disadvantageous consequences of the security breach.

The notification to the subscriber or individual must contain at least the nature of the violation of personal data, and the information points where the subscriber may receive further information, and proposes measures to mitigate the potential disadvantageous consequences of the violation of personal data. Moreover, the notification addressed to the NMHH shall describe the consequences of violation of personal data, as well as measures taken or suggested by the electronic communications service provider for the remedy thereof.

The NMHH may issue recommendations on how to comply with the reporting and notification obligation and best practices for the security level to be achieved in the processing of personal data by public available electronic communications service providers.

The technical and organisational measures – taking into account the best practices and costs of the measures to be taken – shall ensure adequate level of security according to the risks arising at the Service Provider in connection with the unity of the network and providing the service.

The Service Provider informs the subscriber about known risks that remain in spite the technical and organisational measures taken by the service provider, that pose risk to the unity of the network and security of the service, and about the protection measures that may be taken by the subscriber.

Should a formerly unknown, new safety risk emerge due to an event affecting or jeopardising the unity of the network or safety of the service, then the Service Provider shall at least via its customer service and Internet site immediately inform the subscriber about the previously unknown new safety risk and protective measures that may be taken by the subscriber, as well as the anticipated costs thereof. The Service Provider shall not charge the subscriber any additional fees for the

information it has provided. The information provided by the Service Provider shall not exempt the Service Provider from taking the protective measures necessary for restoring the unity of the network and usual security level of the service.

The Service Provider shall have its systems and data processing procedures regularly checked and audited both for data security and quality assurance.

4. In the case of a personal data breach, the Service Provider shall without undue delay and, where feasible, no later than 72 hours from learning of the personal data breach, report the personal data breach to the Hungarian National Authority for Data Protection and Freedom of Information, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The service provider shall document any personal data breaches, indicating the facts relating to the personal data breach, its effects and the remedial action taken.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Service Provider shall communicate the personal data breach to the customers without undue delay. Information to the customers shall not be required if any of the following conditions are met:

- a) the Service Provider has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- b) the Service Provider has taken measures following the personal data breach which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- c) the information would involve disproportionate effort.