DATA MANAGEMENT POLICY ABRIDGEMENT

1. Name and contact details of the Data Controller:

Name: **Ace Telecom Kft.**
Registered office: 1037 Budapest, Zay u. 3.
Branch offices: 2600 Vác, Dr. Csányi László krt. 24., 2040 Budaörs, Szabadság út 133.
Company registration number: Cg. 12255726-2-41
Court of registration: Municipal Court of Budapest as Court of Registration
E-mail address: office@acetelecom.hu
Homepage: http://acetelecom.hu/
Tax number: 12255726-2-41
(hereinafter referred to as the Data Controller)

The Service Provider is responsible for hosting.

2. The content and purpose of the policy

The present data management policy and guide (hereinafter referred to as **Data Management Policy**) summarises how and for what purpose the Data Controller collects, uses and protects the personal data of the users of the https://acetelecom.hu/ website (hereinafter referred to as the **Website**), which is operated by the Data Controller, and the personal data of those who are in contractual relationship with the Data Controller (hereinafter referred to as the **User**, **Subscriber** or **you**). This Data Management Policy covers only the management of the personal data of **natural persons**.

The Data Management Policy specifies the following:

- the person of the Data Controller,
- the scope of the User's/Subscriber's personal data managed by the Data Controller,
- the legal grounds for data management,
- the way of data management (including access by the Data Controller, forwarding and transmitting data to third parties),
- the purpose of data management,
- the time of data management,
- the data protection and data security requirements and
- the possibilities for the enforcement of the User's rights.

This Data Management Policy has been written in Hungarian.

3. The data management is primarily based on the followings legislation

- 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 Protection Regulation or GDPR)** – This policy has been drafted in accordance with Article 13 of the GDPR.

- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (**Info Act**)

- Act CVIII of 2001 on certain issues of electronic commerce services and information society services ("**E-Commerce Act**")

4. Amendment

The Data Controller may unilaterally amend this Data Management Policy. However, prior to amendment, the Data Controller shall inform its Subscribers about the amendment by publishing the amended Data Management Policy in the form of an

announcement on the Website no later than five (5) days prior to the effective date of the amended Data Management Policy and sending it to the given e-mail addresses of the registered Users, as well. In order to become aware of the amendment and be able to review it, you shall have Internet access and check the Website and your given e-mail account regularly.

5. The circle of Users

Registered User or a User ordering the service from the Service Provider: The User is allowed to register on the Website only once, in one way (hereinafter referred to as "**Registration**"). On the Website, you can request an offer related to the products of the Service Provider or order a domain name registration service from the Data Controller (hereinafter referred to as the **Order**). Based on your personal data provided in the course of the Registration or the Order, you shall be entitled to use the services provided by the Data Controller on the Website (**Services**), in accordance with the General Terms and Conditions (**GTC**), which also regulate the use of the Website.

A non-registered User: If you are browsing the Website, without Registration or Order, the provisions of this Data Management Policy shall apply to the management of your personal data.

This Data Management Policy also applies to those who place their orders on paper, via e-mail or in any other way.

Special rules on the performance of the Registration and the Order:

- In the course of the Registration and the Order, you shall provide the required data and
- declare that you have read and become acquainted with this Data Management Policy.
- You shall be obliged to accept the Service Provider's GTC.
- You are allowed to place an order only over the age of 18.

6. What does it mean that you accept the Data Management Policy?

If you use the Website, you confirm that you have read the entire Data Management Policy, become acquainted with and understood its content.

By deciding to tick the relevant checkbox next to the text regarding the confirmation of having read and become acquainted with the content of the Data Management Policy in the course of the Order and the Registration on the Website, you accept that the Data Controller shall carry out data management pursuant to this Data Management Policy. Accepting the Data Management Policy is the **prerequisite for Order** (clicking on the "Order" button) and **Registration** (clicking on the "Registration" button), otherwise, you will not be allowed to order the requested service.

If **you do not agree with the terms above, do not tick the relevant checkboxes** and do not use the Website.

If you place an Order on paper, via e-mail or in any other way, it is also important that we manage your data in accordance with this policy.

7. Data management methods

Our data management methods I the following part of our policy, you can read about when we ask for or collect your personal data, how long and how we manage them.

The provisions on the protection of the personal data of the Users apply only to natural persons ("private individuals"), as such provisions can be interpreted only in this context. Consequently, this Data Management Policy covers only the management of the personal data of natural persons.

✓ Data management related to Registration:

Whose data do we manage? The data of all the registered Users of the Website.

Why do we manage these data (the purpose of data management): - to be able to identify our Users - to be able to contact and maintain contact with our Subscribers. (E.g. by means of the provided data, we confirm your Registration, send messages related to the Services, update data, send system messages included in the Services or memos related to the Services or replies with the information you request.)

What happens if you do not provide the data?

The provision of the aforementioned data is the minimum prerequisite for Registration, therefore such data are required for placing an order. If you fail to provide the data, you shall not be allowed to register on the Website.

How to cancel your registration:

During the User Relationship, you shall be entitled to have your Registration cancelled free of charge any time by sending a written request to the Data Controller to the e-mail address office@acetelecom.hu or to any of the Data Controller's contact addresses indicated in point 1 of this Data Management Policy.

What kind of data do we manage when processing the Order?	What is our data management based on? (the legal grounds for data management)	How long do we manage the data? (duration)	To whom do we disclose the data (data transmission, data forwarding)
- name - e-mail address - password	The management of your data is necessary for the fulfilment of the General Terms and Conditions for the use of the Website and the Services/the performance of the Order or for taking the actions at your request prior to signing the General Terms and Conditions/confirming the Order (point b) of Article 6 (1) of the GDPR).	The duration of data management shall last for five (5) years as of the cancellation of the Registration, with regard to the fact that the Data Controller may have civil claims against the User or a third party may have civil claims against the User or, arising from the User's activity, against the Data Controller, in this period following the termination of the Service.	-

8. Access to the data, data security measures

In accordance with Article 32 of the **General Data Protection Regulation** (**GDPR**), the Data Controller shall apply best efforts to ensure the security of the data, take the necessary technical, organisational measures and establish the rules of procedure required for the enforcement of the **General Data Protection Regulation** and other data protection and confidentiality rules.

The Data Controller shall guarantee the appropriate level of data security as follows:

Such measures include (but are not limited to) (i) storing the User's/Subscriber's data in secure technical environment and not making them available to the public, (ii) making the User's/Subscriber's data available exclusively to the employees listed in this point only after appropriate identification and (iii) using encrypted data transmission (TLS). (iv) The Data Controller uses HTTPS protocol when managing the data, therefore the communication between the User/Subscriber and the server takes place through an encrypted link; (v)The natural persons who have access to personal data are allowed to manage the personal data exclusively in accordance with the instructions of the Data Controller; (vi) pseudonymisation; (vii) the Service Provider stores the data on its own servers (viii) the data are forwarded to the Registry in encrypted form; (ix) our security measures are regularly tested, assessed and improved; (x) before the data subjects (you) are allowed to exercise their (your) rights, we check their (your) identity to ensure that the personal data are safe and they are not disclosed to unauthorised parties.

Within the Data Controller's organisation, the Service Provider's employees and the employees of data processors shall have access to your personal data, in accordance with the applicable internal policies.

Data-related incidents: If any incident occurs in relation to your data, the Data Controller shall undertake any action required to reduce risks after becoming aware of the incident. If, in relation to your data, any incident occurs that is likely to pose high risk regarding your rights and liberties despite the protective measures taken by the Data Controller (or its data processor), we shall notify you and the competent authority of the incident free of charge, without delay.

Links: On the Data Controller's Website, there are some references, links (including buttons and logos representing login and sharing options) to websites operated by other service providers on which the Data Controller does not have any influence on the practice related to the management of personal data. We would like to warn our Users that by clicking on such links, they may be redirected to the websites of other service providers. In such cases, we suggest that you should read the valid data management rules for the use of the above-mentioned websites. This Data Management Policy shall apply only to the Website operated by the Data Controller. If the User modifies or changes any of their data on an external website, the change shall not affect the data management activity carried out by the Data Controller. Such amendments shall be made on the Website, as well.

9. Placing anonymous UIDs (cookies)

The anonymous UIDs (cookies) are unique signal sequences suitable for identification and the storage of profile information, placed on the User's computer by the service providers. It is important to know that these signal sequences themselves are not able to identify the User in any manner, but instead they are only able to recognise the User's computer. In the world of the Internet, personalised information and custom service can only be provided if service providers are able to uniquely identify the habits and needs of their clients. On the one hand, service providers opt for anonymous identification to learn more about how their clients tend to use information, with the purpose of further improving the level of their services and being able to offer custom options to their clients.

Blocking cookies If the User does not want to allow the Service Provider to place the aforementioned identifiers on its computer, they shall set their browser to disable the placement of UIDs or enable the placement of only certain UIDs. In the latter case, some Services may not be available to the User in the same form as they would have been available if the User had enabled the placement of the identifiers.

10. Profiling

Google Analytics: The Data Controller measures the number of visitors on the Website by using the Google Analytics web analytics service provided by Google, Inc. ("Google"). Google Analytics compiles a report on user interactions on the websites of Google Analytics clients primarily on the basis of internal cookies. The advertising functions of Google Analytics can be activated by means of Google Ad cookies, e.g. the remarketing function regarding products of the Google Display Network, such as AdWords. All computers and devices connected to the Internet receive a unique number called IP address (Internet Protocol address). Such numbers are assigned in blocks by country. The given country, state/county where the computer is connected to the Internet can often be identified by the IP address. As websites use IP addresses because of the operating principles of the Internet, the owners of websites can often learn the IP addresses of their users even if they do not use the Google Analytics

service. However, Google Analytics collects the IP addresses of the users of the website only to protect the security of the service and allow the owners of the website to get information about from which part of the world their visitors come from (this is also called “IP-based geolocation”). Google stores the data in a performance-optimised, encoded format rather than in traditional file systems or databases. In order to render access more difficult and due to redundancy, the data are distributed among multiple physical and logical volumes. As a result, the misuse of data can be prevented. Google applications are running distributed in several places of their environment. The data of individual clients are not stored separately on a single computer or on a group of computers, but the data of all Google clients (the data of clients, businesses and even Google’s own data) are mixed, in a shared infrastructure consisting of several homogeneous computers located in Google’s data centres. You can find further information about Google’s data protection principles here: https://policies.google.com/privacy?hl=hu.You can unsubscribe from following Google Analytics in the future by downloading the Google Analytics Opt-out Browser Addon application, installing and adding it to your current browser: tools.google.com/dlpage/gaoptout.
For further information: https://support.google.com/analytics/answer/6004245?hl=hu

11. User rights, possibilities for the enforcement of user rights

In relation to your personal data managed by the Data Controller, you shall be entitled to request the following (itemised below):

- ✓ access to your data managed by us
- ✓ rectification of your data
- ✓ deletion of your data
- ✓ restriction of data management
- ✓ portability of the data managed by us
- ✓ objection to data management

The Data Controller shall inform you about the actions taken based on your request or the reasons for the lack of such actions without undue delay, but in any case within one month after the receipt of the request. If the request is complex or too many requests arrive, the deadline can be extended by additional two months. If possible, you shall be informed by e-mail. Information shall be provided and actions shall be taken free of charge, except for requests which are clearly unfounded or exaggerated, particularly due to their repetitive character. In such cases, a reasonable fee is charged or the requested action is denied. Related to the request, we may ask you for information to prove your identity. The first copy of your personal data managed by us is free of charge, but we charge a fee equalling the administrative costs for any further copies.
You shall be entitled to lodge a complaint against our action with the supervisory authority or to exercise your right to judicial remedy.
You **can have access to the following information** related to the management of your personal data:

- which data of yours we manage;
- for what purpose we manage your data;
- how long we manage the data;
- who have and who will your personal data been disclosed to;
- data management guarantees in the case of data management outside the EU or international data management;
- if you were not the person who provided the data, who did we receive them from;
- the fact of automated decision-making, including profiling, information about the applied logic, the importance of data management and its consequences affecting you.
- your rights and entitlement for judicial remedy in connection with data management.

Rectification You shall be entitled to request the Data Controller to rectify your inaccurate personal data without undue delay or to complete your incomplete personal data.

Deletion You shall be entitled to request the deletion of your personal data from the Data Controller if:
- the personal data are not needed for the original purpose of data collection and management anymore
- you withdraw your consent to data management and the data management has no other legal ground
- You object to data management and no high-priority legitimate reason for data management exists
- the personal data have been illegally managed
- the data shall be deleted to fulfil a legal obligation
- as regards services provided directly to children.

Right to be forgotten: If you are entitled to request the deletion of your data in view of the above and we have published your personal data, we shall take all reasonable measures to inform other data controllers managing the data about the fact that you have requested us to delete links to the relevant personal data or the copy or duplicate of such personal data.

We warn you that **we cannot fulfil your deletion request** if the data are required for the submission, enforcement and defence of legal claims or if the deletion of the data restricted the right to the freedom of expression and information or if we are bound by a legal obligation (or the public interest, any scientific, research or statistical purpose) that is contrary to the deletion request.

Restriction: Restriction means that we are allowed to store such personal data or manage them with your consent (except for when the data are required for the submission, enforcement or defence of legal claims, the protection of other persons' rights or that of the public interest). You shall be entitled to request restricted use of your data if

- you believe that the data are inaccurate. In this case, restriction applies to the period during which we check the accuracy of the personal data.
- the management of your data is illegal, but instead of deletion, you request the restricted use of your data.
- we do not need your personal data anymore, but you need them for the submission, enforcement and defence of legal claims
- if you object to data management, the restriction shall apply during the period until it is established that our legitimate reasons have priority over your legitimate reasons.

We shall notify all the parties of correction, deletion or data management restriction to whom the personal data have been disclosed unless this proves impossible or involves a disproportionate effort. You shall be entitled to receive the list of such recipients upon request.

Data portability: You shall be entitled to receive your personal data you provided to us or forward them to another data controller if data management is based on your consent or contractual performance and is automated. Portability shall not infringe other persons' rights and liberties or their right to deletion (right to be forgotten).

You shall also be entitled to request the Data Controller to directly forward your personal data to the new service provider if its is technically possible.

Objection: You shall have the right to object to any kind of data management that is carried out on the grounds of the Data Controller's legitimate interest (or the public interest). If your personal data are managed for the purpose of direct marketing, you shall be entitled to object to the management of your personal data for this purpose, including profiling, anytime. Following your objection, we shall be not entitled to manage the data any longer.

Profiling: You shall have the right not to fall under the scope of a decision based exclusively on automated data management, including profiling, which would produce legal effects on you or would have a similarly serious effect on you. Exemptions may be made if the decision is required for the conclusion or performance of a contract between you and the Data Controller or if you give your explicit consent to it or if the decision is allowed by the law, on condition that your rights and interests are protected. However, in this case, you shall be entitled to request human intervention by the Data Controller, express your viewpoint and raise an objection to the decision.

Enforcement of rights:

The User shall be entitled to exercise their rights pursuant to the General Data Protection Regulation (GDPR) and the Civil Code (**Civil Code**). In the event of the infringement of their rights, the User shall be entitled to launch a judicial proceeding or file a complaint with the supervisory authority.

You shall be entitled to file a complaint with the supervisory authority of the member state where your habitual place of residence, your workplace is located or the alleged infringement occurred if you believe that the management of your personal data violates the General Data Protection Regulation. In Hungary, the supervisory authority is the National Agency for Data Protection and the Freedom of Information, whose registered office is located at: 1024 Budapest, Szilágyi Erzsébet fasor 22/C., website: www.naih.hu, phone number: +36 (1) 391-1400. You shall be entitled to judicial remedy against the supervisory authority's legally binding decision or if the authority does not deal with your complaint or fails to inform you about the developments related to and the results of your complaint. The proceeding against the supervisory authority shall be launched before the court of the member state where the registered office of the supervisory authority is located.

If you **suffer any damage** arising from the infringement of the General Data Protection Regulation, you shall be entitled to receive compensation for the damage from the Data Controller (or the data processor). The judicial proceeding shall be launched before the court of the member state where the Data Controller's (or the data processor's) activity is carried out. Such proceedings can also be launched before the court of the member state where your habitual place of residence is located.

If you consider that we have infringed your rights by not managing your personal data in compliance with the General Data Protection Regulation, you shall be entitled to launch a judicial proceeding for the violation of law. The judicial proceeding shall

be launched before the court of the member state where the Data Controller's (or the data processor's) activity is carried out. Such proceedings can also be launched before the court of the member state where your habitual place of residence is located.

Of course, launching a judicial proceeding does not exclude that you have the right to seek any other possible administrative or non-judicial redress.

Legal actions for enforcing a tort and property actions below HUF 30 million (e.g. actions for damages) fall under the jurisdiction of the district court, while property actions exceeding HUF 30 million fall under the jurisdiction of the tribunal. The action can be initiated before the court within the jurisdiction of which the registered office of the Data Controller is located, in accordance with the general rules. However, if you are considered to be a consumer, at your choice, you shall be entitled to bring the action before the court within the jurisdiction of which your domestic residence or, for lack of this, your domestic place of abode is located. In the case of an action against the supervisory authority, the action at your choice, you shall be entitled to bring the action before the court within the jurisdiction of which your domestic residence or, for lack of this, your domestic place of abode is located or before the court within the jurisdiction of which the registered office of the supervisory authority is located.

12. Appointed data controller, the person in charge of data protection

In relation to taking decisions related to data management and guaranteeing the rights of the data subjects, the Users are supported by the Data Controller's appointed data protection officer via the e-mail address office@acetelecom.hu , from Monday to Friday between 9:00 a.m. and 15:00 p.m.

13. Legislation in force, other provisions

This Data Management Policy shall be governed by the Hungarian law.

If in accordance with the effective legislation of your country, stricter rules apply to the relationship of the Parties than those in this Data Management Policy, you shall be obliged to follow the stricter rules. At the same time, you acknowledge and accept that the Data Controller's liability is based on the legislation applicable to this Data Management Policy and the Data Controller's liability for the User's non-adherence to their country's provisions shall be excluded to the highest possible extent possible pursuant to the relevant legislation and court decisions.

The headings of this Data Management Policy shall be only for information purposes, they are not sufficient for understanding data management.

If you have any questions which have not been clearly answered by this Data Management Policy, please write to the following e-mail address: office@acetelecom.hu

This Data Management Policy shall be valid as of 1 April 2019.

ACE Telecom Kft.