

TERMS OF SERVICE OF FIBERAX SP. Z O. O. SERVICES TO CONSUMERS

(HEREINAFTER REFERRED TO AS THE "TERMS OF SERVICE")

TABLE OF CONTENTS

1.	DEFINITIONS	2
2.	SCOPE OF APPLICATION OF THE TERMS OF SERVICE	3
3.	CHANGE OF TERMS OF SERVICE	3
4.	CONCLUSION OF THE AGREEMENT	4
5.	REMUNERATION	4
6.	DURATION OF THE AGREEMENT AND ITS TERMINATION	5
7.	WAIVING	5
8.	COMMENCEMENT OF SERVICES AND MINIMUM TECHNICAL CONDITIONS	6
9.	OBLIGATIONS OF THE PROVIDER	6
10.	USER RESPONSIBILITIES	6
11.	USER DATA	6
12.	YOUR INTELLECTUAL PROPERTY	6
13.	PROVIDER INTELLECTUAL PROPERTY	7
14.	CONFIDENTIAL INFORMATION	7
15.	COMPLAINT PROCEDURE	7
16.	OUT-OF-COURT DISPUTE RESOLUTION	7
17.	PROVIDER RESPONSIBILITY	8
18.	SUSPENSION OF ACCESS TO SERVICES AND DELETION OF USER DATA	8
19.	SUBCONTRACTORS AND ENTITIES COOPERATING WITH THE PROVIDER	9
20.	TRANSFER OF RIGHTS AND OBLIGATIONS UNDER THE AGREEMENT	9
21.	YOUR PERSONAL DATA	9
22.	COMMUNICATION OF PARTIES	BŁĄD! NIE ZDEFINIOWANO ZAKŁADKI.
23.	DELETION OF USER DATA	9
24.	FINAL PROVISIONS	9

PART I - GENERAL PROVISIONS

1. DEFINITIONS

Whenever the following capitalized phrases are used in the further part of the Terms of Service, they should be understood in the following meaning, unless the context of their use clearly indicates otherwise:

Price list	a list of fees for the provision of a given Service by the Provider, which may be part of the Service Card or part of the Website;
Fiberax Cloud	an organized ICT system consisting in particular of computer hardware, software and telecommunications links, enabling the provision of services in the form of virtual applications, sharing computing power, database services, virtual servers, virtual disks and private networks, used for storing, sharing and processing User Data, in accordance with the technical conditions specified by the Provider
Personal data	data referred to in Article 4(1) of 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);
User data	any data, including images, sounds, text, software, that the User transmits or processes through the Services, and in particular stores when using the Services;
Provider	Fiberax sp. z o.o. with its registered office in Warsaw, address: Puławska 405A/303, 02-801 Warsaw, registered in the Register of Entrepreneurs of the National Court Register maintained by the District Court for the capital city of Warsaw in Warsaw, XIII Commercial Division of the National Court Register under KRS 0001043360, NIP: 9512571325, REGON: 525646336, with a share capital of PLN 1,000,000.00, support@fiberax.com ;
Service Card	where applicable - document containing detailed terms and conditions for the provision of a given Service by the Provider, including in particular a description of the Service, SLA and, where applicable, the Price List for a given Service;
User Account	a web interface enabling the User to manage the Resources within the rights resulting from the scope of Services provided by the Provider agreed in the Agreement, update the User's contact details and provide the User with

information necessary for the Service Provider to provide to the User. Access to the User Account is provided at <https://fiberax.com>

Terms of Service	this document together with appendices constituting its integral part, specifying the rules for the provision of Services by the Provider to the User, constituting an integral part of the Agreement; the current version of the Terms of Service is constantly available on the https://fiberax.com website, including in PDF format;
SLA	the Provider's obligations regarding the guaranteed quality level of specific Services, described in detail each time in the appendix to the Service Card for a given Service
Website	the content contained on the https://fiberax.com website and its subpages made available by the Provider to Internet users without access restrictions; the information provided by the Service Provider on the Website constitutes an invitation to conclude the Agreement within the meaning of Article 71 of the Civil Code;
Parties	User and the Provider together;
Agreement	an agreement between the Provider and the User specifying the rights and obligations of the User and the Provider in connection with the provision of the Services;
Service	services provided on the terms set out in the Terms of Service and in the Agreement, consisting in particular in providing the User with functionalities in the form of Fiberax Cloud Resources, as well as BaaS Services, VPS Services, User Account, Tariff Units and other functionalities or service packages introduced by the Provider, used by the User in connection with business or professional activity
User	an entity with full legal capacity, which is a consumer or a natural person concluding the Agreement directly in connection with its business activity, if the Agreement is not of a professional nature for it, resulting in particular from the subject of its business activity;
Data Loss	accidental or unintentional loss, damage, unauthorized access, modification or destruction of User Data processed as part of the Services;
Remuneration	fees charged by the Provider to the User for the provision of the Services;
Resources	m.in. disk space, computing power and other services made available to the User as part of the Fiberax Cloud;
Suspension of access	a situation in which the Provider restricts the User's access to the User Data under the Agreement (including the Appendices to the Agreement) or by law, although the User's Data is still stored by the Provider;

2. SCOPE OF APPLICATION OF THE TERMS OF SERVICE

- 2.1. These Terms of Service, together with the appendices (including Service Cards, if applicable), define the rules, scope and conditions of the provision of services by the Provider to Users who are consumers or natural persons concluding the Agreement directly in connection with their business activity, if the Agreement is not of a professional nature for them, resulting in particular from the subject of their business activity.
- 2.2. The Terms of Service constitute an integral part of each Agreement, which means that unless a given Agreement provides otherwise, their provisions apply - subject to point 4.2 below - directly to the cooperation of the Parties on its basis.
- 2.3. If the Agreement between the Parties is concluded in the form described in section 4.2. below (in electronic form), the provisions of the Terms and Conditions shall apply directly to the cooperation between the Parties on this basis.

3. CHANGE OF TERMS OF SERVICE

- 3.1. The Terms of Service and appendices to the Terms of Service constitute a model contract within the meaning of Article 384 § 1 of the Civil Code.
- 3.2. The Provider reserves the right to amend the Terms of Service in the event of the occurrence of at least one of the following important reasons:
 - a. a change in the provisions of law governing the provision of services by electronic means by the Provider affecting the mutual rights and obligations specified in the Agreement concluded between the User and

- b. a change in the way the Services are provided due solely to technical or technological reasons;
 - c. change the scope or provision of the Services to which the provisions of the Terms of Service apply by introducing new functionalities or withdrawing the existing functionalities by the Provider;
 - d. a change in the manner of providing Services caused by a change in agreements or Terms of Service of entities cooperating with the Provider, caused by a change in the provisions of law governing their activities, affecting the mutual rights and obligations specified in the Agreement concluded between the User and the Provider, or a change in the interpretation of the above provisions of law as a result of court rulings, decisions, recommendations or recommendations of competent authorities or bodies in a given scope.
- 3.3. The User will be notified of each change by sending information about the change to the User Account and to the e-mail address, which the Parties consider as entering information about the change into the means of electronic communication in such a way that the User can read its content. The change referred to in the preceding sentence shall enter into force after 30 days from the date of sending the information about the change, unless the User submits a statement on the termination of the Agreement with immediate effect within 15 days from the date of sending the information about the change.

PART II – AGREEMENT

4. CONCLUSION OF THE AGREEMENT

- 4.1. The Provider provides Services to the User on the terms specified in the Agreement.
- 4.2. The Agreement is concluded upon the joint fulfilment of the following conditions:
 - 4.2.1. registration via the registration form made available by the Provider on the Website – the registration form collects only data that the Provider may process in accordance with the provisions of the Act of 18 July 2002 on the provision of electronic services (in particular Article 18(1)-(5) of this Act) and includes:
 - 4.2.1.1. name and surname;
 - 4.2.1.2. name of organisation (for organisation);
 - 4.2.1.3. street, apartment number, postal code, city, state and country;
 - 4.2.1.4. email address;
 - 4.2.1.5. VAT number (for organisation);
 - 4.2.1.6. a password set by the User;
 - 4.2.1.7. phone number;
 - 4.2.2. accept the Terms of Service and Service Card by indicating in the appropriate form that the User accepts the Terms of Service without changes.
- 4.3. Acceptance of the Terms of Service by the User is tantamount to the User's declaration that:
 - 4.3.1. has read the Terms of Service and Service Cards and accepts all its provisions without reservations, thus concluding the Agreement;
 - 4.3.2. the data contained in the registration form, as well as the statements made in the Terms of Service are true;
 - 4.3.3. the person who accepted the Terms of Service on behalf of the User was duly authorized to represent the User,
 - 4.3.4. the content of the Agreement is specified only in the Terms of Service, in particular the Agreement does not consist of any standard contracts or Terms of Service used by the User;
- 4.4. The Provider may enable the conclusion of the Agreement in electronic form. In such a case, the Agreement shall be concluded upon acceptance of the Terms of Service together with the appendices (if applicable), without creating a User Account.

5. REMUNERATION

- 5.1. The rules for Remuneration for Post-Paid Users are specified in each Service Card in point 6.
- 5.2. The model of Remuneration for services provided by the Provider to the User under the Agreement, price lists, payment terms and other detailed provisions concerning settlements between the Parties shall be specified each time in the Service Card dedicated to a given service and/or on a subpage of the Website dedicated to a given Service.
- 5.3. If the Agreement does not specify a different billing period, the settlement period is a calendar month.
- 5.4. In the event that the Provider issues a corrective invoice, the agreement on the terms of the correction shall be deemed fulfilled on the date of issue of the corrective invoice, unless the Parties expressly agree otherwise.
- 5.5. The User declares that for VAT purposes, the place of supply of the service being the subject of the Agreement is the territory of Poland, unless otherwise stated in the Agreement.
- 5.6. The Remuneration is subject to value added tax (VAT) in the amount consistent with the generally applicable provisions of law.
- 5.7. The User agrees to issue VAT invoices for the performance of the Agreement, in electronic form, in PDF format. Issued VAT invoices are made available to the User via e-mail, to the e-mail address indicated in the Agreement or via the User Account.

6. PRE-PAID USERS

After concluding the Agreement, the User has the option to purchase, for a Remuneration, Tariff Units which entitle them to use the relevant Services on the terms specified in the Agreement, and the Provider undertakes to remain in the Validity

Period ready to provide these Services, Provider is entitled to Remuneration for the sale of Tariff Units in the amount specified in the Price List.

Pre-Paid Users may purchase Tariff Units by paying the Remuneration in advance, by bank transfer to the Provider's bank account or using another payment system accepted by the Provider. The Provider may, in particular, make Paynow available as a payment method.

- 6.1. The Tariff Units purchased by the User are visible in the User Account. The moment of proper performance of the Tariff Units by the Provider is the moment when the Provider displays the Tariff Units purchased by the User in the User Account.
- 6.2. The User may use Tariff Units to use the Services up to their total amount after they have been purchased. As Tariff Units are used, their number in the User Account decreases. After using the Tariff Units, the User may not use them and they are not indicated in the User Account. The User may use the purchased Tariff Units within the User Account only for a period of 2 years from the moment they are made available to the User in the User Account.
- 6.3. Upon expiry of the Validity Period, due to the Service Provider remaining in the Validity Period and ready to provide the Services, it is not possible to use the Tariff Units (they cannot be used and are not indicated in the User Account).
- 6.4. Tariff Units are non-refundable. The Provider shall not redeem Tariff Units. In the event of termination of the Agreement for any reason, Tariff Units shall not be refunded.

7. DURATION OF THE AGREEMENT AND ITS TERMINATION

- 7.1. The Agreement is concluded for an indefinite period of time.
- 7.2. The User may terminate the Agreement at any time with a 30-day notice period.
- 7.3. The Provider may terminate the Agreement with 30 days' notice for the following important reasons:
 - 7.3.1. a change in the law governing the provision of services by electronic means by the Provider affecting the mutual rights and obligations specified in the Agreement concluded between the User and the Provider or a change in the interpretation of the above provisions of law as a result of court rulings, decisions, recommendations or recommendations of competent authorities or bodies in a given scope;
 - 7.3.2. a change in the way the Services are provided due solely to technical or technological reasons;
 - 7.3.3. change the scope or provision of the Services to which the provisions of the Terms of Service apply by introducing new functionalities or withdrawing the existing functionalities by the Provider;
 - 7.3.4. a change in the manner of providing Services caused by a change in agreements or Terms of Service of entities cooperating with the Provider, caused by a change in the provisions of law governing their activities, affecting the mutual rights and obligations specified in the Agreement concluded between the User and the Provider, or a change in the interpretation of the above provisions of law as a result of court rulings, decisions, recommendations or recommendations of competent authorities or bodies in a given scope.
- 7.4. The Provider may terminate the Agreement with 7 days' notice for the following important reasons:
 - 7.4.1. when access to the Services has been suspended due to circumstances for which the User is responsible, and the User has not removed the reason for the suspension within the appropriate period set by the Provider, and in any case the suspension of access to the Services lasting longer than 30 calendar days;
 - 7.4.2. violation by the User of the provisions of law or the Agreement, in a manner affecting the performance of the Agreement or the situation of the Provider or other users of the Services, if the User does not cease the above-mentioned violations or does not remedy their effects within the time limit set by the Provider in the request addressed to the User by e-mail.
- 7.5. The User may terminate the Agreement by contacting the Provider, in particular via the User Account, e-mail address: support@fiberax.com or via the correspondence address: Puławska 405a/lok. 303,02-801 Warsaw. The Provider sends its statement of termination to the e-mail address provided by the User when creating the User Account.
- 7.6. The provisions of this section do not limit the possibility of termination of the Agreement by the Provider or the User on the terms specified by law.

8. WAIVING

- 8.1. The User has the right to withdraw from the Agreement within 14 days from the date of its conclusion, without giving any reasons and without incurring any costs other than those provided for by law.
- 8.2. In order to inform the Provider about the withdrawal, the User should submit a statement in which he informs about his decision to withdraw. The statement may be submitted using the model withdrawal form, which is attached to the Terms of Service. This does not limit the User's right to make any other unequivocal statement in which he informs about his decision to withdraw.
- 8.3. In the event of withdrawal from the Agreement, the Provider shall return all payments received from the User, without undue delay, and in any event no later than within 14 days from the date on which it was informed of the User's decision to withdraw from the Agreement, subject to clause 8.4 below.
- 8.4. The User who has been informed before the commencement of the provision that after its performance by the Provider will lose the right to withdraw from the Agreement, may consent to the Provider performing this Service in full immediately after the conclusion of the Agreement. In the case of giving the consent referred to in the previous sentence, the User is not entitled to withdraw from the Agreement after the performance of this service.
- 8.5. Confirmation of the consent given by the User, referred to in point 8.4 above, takes place by way of an e-mail sent to the e-mail address provided by the User in the registration form.

PART III – RULES FOR THE PROVISION OF SERVICES

9. COMMENCEMENT OF SERVICES AND MINIMUM TECHNICAL CONDITIONS

- 9.1. In order for the User to be able to use the Services, it is necessary to meet the minimum technical conditions described in the Service Card for a given Service or in the User Account, respectively.
- 9.2. The commencement of the provision of Services requires the User to complete the registration procedure.
- 9.3. The registration procedure consists in the correct and complete completion by the User of the registration form provided by the Provider, after which the User gains access to the User Account.
- 9.4. The User receives credentials enabling access to the User Account via e-mail to the e-mail addresses of the User's authorized persons specified in the Agreement.

10. OBLIGATIONS OF THE PROVIDER

- 10.1. The Provider provides the User with the possibility of access to the Services and strives to provide them at the level indicated in the appropriate SLA.
- 10.2. The Provider is not the initiator of the transfer of User Data in connection with the access to and use of the Services, does not select the recipient of the transfer of User Data, does not select or modify the User Data. The Provider only provides technical resources in the form of access to the Services, the content, shape and use of these resources is decided solely by the User. The Provider does not monitor the content of User Data.
- 10.3. The Provider does not make the User's Data available to third parties, except at the express request of the User or authorized public authorities. If authorized public authorities request access to all or part of the User's Data, the Provider will consult such disclosure with the User in advance, if such consultation is permitted by law.

11. USER RESPONSIBILITIES

- 11.1. The User is obliged to:
 - a. comply with the provisions of the Agreement and the provisions of applicable law when accessing and using the Services,
 - b. appropriate security of access to the User's Account and use of the Services, to the extent dependent on the User, as well as securing passwords used to access and use the Services and not making them available to unauthorized persons; You are responsible for any breach of security of your User Data and other damage caused by your failure to properly secure access to and use of your Account;
 - c. cooperation with the Service Provider in the cases specified in the Agreement, i.e. in particular when such cooperation is necessary to determine whether the Services have been accessed or used in a manner inconsistent with the Terms of Service, the Agreement or the law;
 - d. update information about the User in the User Account, including contact details provided in the registration form, Agreement or User Account, immediately, no later than within 7 days after the change occurs;
 - e. immediately, no later than within 7 days of the event, notify the Provider of any case of detection of unauthorized access to the Services provided, unauthorized disclosure of or access to authentication data in the Fiberax Cloud (e.g. passwords) or any other breach of security that may affect the performance of the Agreement;
- 11.2. The User declares that he will use the Services only for civil purposes, not directly related to the subject of his professional or business activity.
- 11.3. Without the prior consent of the Provider, expressed in electronic form under pain of nullity, the User undertakes not to use the Services directly or indirectly for the purposes of the operation of the so-called "cryptocurrency mines" or "generating nodes" related to blockchain technology, including in particular to perform calculations to solve a cryptographic problem for the purpose of adding a new block or verifying a transaction, or in particular to obtain (mine) a cryptocurrency or ensure the functioning of another solution based on blockchain technology.

12. USER DATA

- 12.1. The use of the Services as electronic services involves the typical risks associated with the transmission of data over the Internet, such as the dissemination of User Data, unauthorized access to it, or Loss of Data.
- 12.2. The User undertakes that the scope of the User Data does not and will not require during the term of the Agreement the use of specific means for their processing other than those described in the Terms of Service or the fulfillment by the Provider of other specific conditions (e.g. obtaining consent, registration, certificate, etc.).

13. USER INTELLECTUAL PROPERTY

- 13.1. To the extent that the provision of the Services by the Provider and the use of the Services by the User may involve the Provider's use of intellectual property rights to the User's Data (in particular for the purpose of running software that does not originate from the Provider), the User grants the Provider free consents to the extent and free of charge any non-exclusive licenses to use such intellectual property rights (including software licenses) solely for the duration of the provision of the Services and for the purpose of their proper provision, or, to the extent that the User is not entitled to grant such a license, the User undertakes to obtain from the Provider the appropriate licenses and consents to use these intellectual property rights for the duration of the provision of the Services and for the purpose of their proper provision from the entity authorized to grant such licenses. The Provider will be granted the appropriate, free-of-charge licenses/consents referred to in this section, including the use of the image, and the license to the User's Data, if they constitute a work within the meaning of Article 1 of the Act of 4 February 1994 on Copyright and Related Rights, will take place in the fields of exploitation necessary for the proper provision of the Services throughout the world, in particular:
 - a. in the field of recording and reproduction - production of copies using magnetic, magneto-optical, optical and digital recording techniques, including placing on the Internet, servers, other elements of network infrastructure and end devices (including in the memory of computers and mobile devices);
 - b. in the field of dissemination - public performance, exhibition, display, reproduction, broadcasting and rebroadcasting, as well as making it available to the public in such a way that everyone can access it in a place and at a time chosen by them;

- c. in the field of introducing necessary changes, modifications and adaptations, as well as creating studies and translations.

14. PROVIDER INTELLECTUAL PROPERTY

- 14.1. All intellectual property rights related to the provision of Services to the User, in particular to the graphic elements of the Fiberax Cloud, such as the Provider's logo, the layout of the website and individual applications, the content of the website, trademarks, names and other designations, as well as to the technical solutions of the Fiberax Cloud, its operating concepts, functionalities, databases, computer programs and technical documentation, are vested exclusively in the Provider or entities cooperating with him. The Provider represents that it is entitled to use the relevant computer programs and other works within the meaning of copyright law, comprising the Fiberax Cloud, on the basis of appropriate licenses/proprietary copyrights, and that it is entitled to provide the Services on the terms described in the Agreement, including the license referred to in section 16.3 below.
- 14.2. The Provider represents that at the time of conclusion of the Agreement, it is providing the Service in particular on the basis of the Microsoft Services Provider License Agreement (SPLA).
- 14.3. To the extent that the Services are provided by entities cooperating with the Provider or jointly with entities cooperating with the Provider, the relevant provisions regarding the intellectual property rights of these entities, possible licenses granted by these entities to the User or possible licenses the granting of which is necessary for these entities in order to perform the Services can be found in the Terms of Service or agreements concerning the provision of services by these entities.

15. CONFIDENTIAL INFORMATION

- 15.1. The Parties undertake to maintain the strict secrecy of the Confidential Information and not to use it (in whole or in part) for any purpose not directly related to the performance of the Agreement. The Parties consider the following to be Confidential Information:
 - a. legal, financial, technical, IT, technological, or organizational information about the Services;
 - b. information of economic value relating to the Parties;
 - c. information concerning third parties, including the Provider's associates, entities related to the organization or capital, members of their bodies or partners, persons cooperating with them, customers, former customers and persons cooperating with customers or former customers.
- 15.2. The confidentiality obligations set forth in this paragraph do not apply to Confidential Information that:
 - a. are or become generally known, other than by breach of the Agreement or applicable law;
 - b. have been obtained by the Party in accordance with the law and its obligations before obtaining the information from the other Party;
 - c. have been disclosed on the basis of the prior, written consent of the other Party, to the extent and to the entities specified in this consent;
 - d. must be disclosed by law to competent public authorities;
 - e. includes statistical data or derived statistical data obtained by the Provider in connection with the provision of the Services;
 - f. shall include only the Parties' communication of the fact of cooperation.
- 15.3. The Parties shall ensure that the above confidentiality obligation is respected by all persons representing them and any third parties connected to them in any way who may have become aware of confidential information through this website.
- 15.4. The confidentiality obligation is valid for the duration of the Agreement and for 10 years after its termination or expiration.

PART IV – PRINCIPLES OF LIABILITY

16. COMPLAINT PROCEDURE

- 16.1. The User may raise objections related to access to the Services, their use or their functioning in the form of complaints.
- 16.2. The Provider shall consider the User's complaint immediately, no later than within 30 days from the date of its receipt, in accordance with Article 7a(1) of the Act of 30 May 2014 on consumer rights, unless a different deadline is provided for by law or separate Terms of Service.
Complaints may be submitted to the Service Provider in particular via the User Account or to the e-mail address: support@fiberax.com or to the address of the Provider's registered office. The User may submit a complaint in any form. In order to speed up the consideration of the complaint, the complaint may contain at least the following data:
 - a) name and surname/username
 - b) User's address – in the case of a complaint submitted in writing;
 - c) the subject of the complaint and the period complained about along with the circumstances justifying the complaint;
 - d) determination of the claim against the Provider.
- 16.3. The date of receipt of a complaint is the date of receipt of the notification by the Provider in writing or electronically.

17. OUT-OF-COURT DISPUTE RESOLUTION

- 17.1. The use of out-of-court methods of handling complaints and pursuing claims is only voluntary. The following provisions are for information purposes only and do not constitute an obligation of the Provider to use out-of-

court dispute resolution. The Provider's declaration of consent or refusal to participate in the proceedings for the out-of-court resolution of consumer disputes is submitted by the Provider on paper or another durable medium in the event that the dispute has not been resolved as a result of the complaint filed by the User.

- 17.2. The rules for conducting proceedings for out-of-court resolution of consumer disputes and the obligations of entrepreneurs in this respect are set out separately in the provisions of law (including, in particular, the Act of 23 September 2016 on out-of-court resolution of consumer disputes) or in the Terms of Service applied by relevant entities that are competent to resolve consumer disputes. Detailed information on the possibility of using out-of-court methods of handling complaints and pursuing claims by the User and the rules of access to these procedures may be available at the offices and on the websites of district (municipal) consumer ombudsmen, social organizations whose statutory tasks include consumer protection, provincial inspectors of the Trade Inspection, in particular also at the following website address of the Office for Consumer Protection Competition and Consumers https://www.uokik.gov.pl/pozasadowe_rozwiazywanie_sporow_konsumentkich.php. The President of the Office of Competition and Consumer Protection maintains a public register of entities authorized to conduct proceedings on out-of-court resolution of consumer disputes.
- 17.3. The User has the following examples of options for using out-of-court methods of handling complaints and pursuing claims:
- 17.3.1. applying to the permanent consumer arbitration court, referred to in Article 37 of the Trade Inspection Act of 15 December 2000, with a request to resolve the dispute arising from the concluded Agreement;
 - 17.3.2. applying to the provincial inspector of the Trade Inspection, in accordance with Article 36 of the Trade Inspection Act of 15 December 2000, with a request to initiate mediation proceedings for the out-of-court settlement of the dispute between the User and the Provider.
 - 17.3.3. obtaining free assistance in resolving a dispute between the User and the Provider, also using the free assistance of a district (municipal) consumer ombudsman or a social organization whose statutory tasks include consumer protection (m.in. Consumer Federation, Association of Polish Consumers).
 - 17.3.4. submitting a complaint via the ODR online platform: <http://ec.europa.eu/consumers/odr/>. The ODR platform is also a source of information on forms of out-of-court settlement of disputes that may arise between entrepreneurs and consumers.

18. PROVIDER RESPONSIBILITY

- 18.1. The Provider's liability in the event of failure to meet the guaranteed level of Service is regulated by the SLA. To the extent not regulated in the SLA, the Provider is responsible for the Services provided to the User on the terms set out below.
- 18.2. In each case of contractual or tort liability by the Provider, it is limited to the amount of fifteen times the Fee actually paid by the User in the month preceding the occurrence of the event for which the Provider is responsible, and if the term of the Agreement is shorter – for the entire duration of the Agreement. If it is not possible to determine the limit of liability based on the principles described in the previous sentence, the total limit of the Provider's liability for damage caused in connection with the Agreement is PLN 10,000.00.
- 18.3. The total limit of the Service Provider's liability for contractual and tort damages that occurred in a given calendar year is ten times the Fee paid to the Service Provider by the User for the period of the last 6 months of providing the Services or for the actual term of the Agreement, if it is shorter than the above-mentioned period of 6 months, unless the provisions of mandatory law provide otherwise.
- 18.4. The limitation of the Provider's liability referred to in this section does not apply to damage caused to the User intentionally.
- 18.5. The Parties shall not be liable for delay, non-performance or improper performance of the Agreement if such delay, non-performance or improper performance results from a force majeure event, i.e. events beyond the control of the Parties, which cannot be foreseen, in particular wars, natural disasters, cyber attacks (including DDoS).
- 18.6. For the purposes of this point, the Provider shall also be understood as the Service Provider's employees, i.e. any natural person employed by the Service Provider on the basis of an employment contract or a civil law contract and receiving remuneration from the Service Provider in the form of salary or other remuneration, subcontractors and entities cooperating with the Service Provider in the provision of Services.

19. SUSPENSION OF ACCESS TO SERVICES AND DELETION OF USER DATA

- 19.1. In the event of any of the important circumstances indicated below, the Provider may Suspend the User's access to the Service or User Data:
- a. receive official notice or obtain reliable information/information that the Services are or have been used in a manner inconsistent with the Agreement or the law;
 - b. the User's lack of cooperation, in cases where such cooperation is necessary to determine whether the Services have been accessed or used in a manner inconsistent with the Agreement or the law;
 - c. reasonable suspicion by the Provider regarding unauthorized access to or use of the Services or User Account by the User;
 - d. the Provider's objectively reasonable presume that the immediate suspension of access to the Services is necessary to protect the integrity, availability, or security of Fiberax Cloud or other customers;
 - e. failure to pay the Fee on time, despite the User's request for payment and setting an additional 14-day deadline from the moment of sending the e-mail by the Provider;
 - f. the occurrence of an obligation resulting from the law or from the decisions of competent state authorities or courts.
- 19.2. If the Provider determines that any User Data constitutes illegal content within the meaning of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the single market for digital

- services and amending Directive 2000/31/EC (Digital Services Act), in addition to suspending the User's access to the Service, it will take action to remove such content from the Resources offered by the Provider.
- 19.3. No later than on the day of the Suspension of access to the Services or taking the actions referred to in clause 17.2, the User will be informed about the Suspension/deletion of the Data and the reasons therefor. The notification will include a justification.
- 19.4. The Provider shall immediately, i.e. no later than within 2 business days, after ascertaining that the reasons for the Suspension cease to exist, restore access to the Services or User Data, respectively, subject to the exceptions provided for by law.
- 19.5. In the event that the User's legitimate interest requires access to a specific scope of User Data during the Suspension, the Provider may, unless it is contrary to the provisions of applicable law and as long as it is technically possible to do so without incurring excessive expenses, grant the User access to the above-mentioned User Data for the time necessary to export them.

PART V – MISCELLANEOUS

20. SUBCONTRACTORS AND ENTITIES COOPERATING WITH THE PROVIDER

- 20.1. The Provider may entrust the performance of the Services in whole or in part to subcontractors.
- 20.2. The Provider may provide the Services with or on behalf of the Provider's partners.
- 20.3. With regard to the cooperation referred to in section 16.2 (cooperation with Microsoft under the SPLA), by signing the Agreement, the User accepts and undertakes to comply with the provisions of the following Microsoft documents:
<https://www.microsoft.com/licensing/spur>
<https://www.microsoft.com/licensing/terms>,

21. TRANSFER OF RIGHTS AND OBLIGATIONS UNDER THE AGREEMENT

- 21.1. The transfer of the rights or obligations under the Agreement by the User in whole or in part to any other person or entity requires the prior consent of the Provider expressed in writing under pain of nullity.
- 21.2. The Provider may transfer the rights or obligations under the Agreement to its related entities, in particular subsidiaries or parent companies, informing the User thereof, to which the User hereby consents. The Provider undertakes to ensure that such transfer will not affect the quality and continuity of the Services provided.

22. YOUR PERSONAL DATA

- 22.1. The User hereby acknowledges that in order to perform and settle the Agreement, the Provider processes the User's Personal Data as a data controller.
- 22.2. The Personal Data referred to in this section will be processed by the Provider for specific, specific purposes described in detail as part of the Privacy Policy made available to the User by the Provider.
- 22.3. The Provider uses appropriate technical and organizational measures to ensure the protection of the Personal Data processed.

23. DELETION OF USER DATA

- 23.1. Upon termination, you will lose access to any User Data and it will be deleted, subject to clauses 23.2 and 23.3 below.
- 23.2. At the request of the User submitted to the Provider during the period of termination of the Agreement in the form of an e-mail message under pain of nullity, the Provider provides the User with an additional 14-day period for exporting the User Data, and the User will be obliged to pay the Provider's Remuneration for this period on the terms specified in the Agreement. If the User successfully submits the request referred to in the preceding sentence, the duration of the Agreement (its notice period) is extended by the above-mentioned 14-day period for exporting the User Data.
- 23.3. After the termination of the Agreement, the Provider is obliged to delete all User Data immediately, i.e. no later than within 14 days. After the termination of the Agreement, during the above-mentioned period, the provisions of the Agreement shall apply accordingly. The Provider's obligations to delete the User's Data do not apply in the case and to the extent that the obligation to continue processing it arises by operation of law or from the decision of competent public authorities.
- 23.4. After the termination of the Agreement, the Provider is obliged to immediately, i.e. no later than within 14 days, delete the User Account. The provisions of clause 23.3 above shall apply accordingly.

24. FINAL PROVISIONS

- 24.1. The applicable law for the Agreement is the Polish law. The choice of Polish law on the basis of the Terms of Service does not deprive the User of the protection granted to him on the basis of provisions that cannot be excluded by way of an agreement between the Provider and the User, under the law which, in accordance with the relevant Terms of Service, would be applicable in the absence of choice.
- 24.2. If one or more provisions of the Agreement are or become invalid or ineffective, the validity or effectiveness of the remaining provisions shall not be affected, unless the Parties would not have concluded the Agreement without that provision and the application of the next sentence shall not apply. In place of an invalid or ineffective provision, the provision that is closest to the objective assumed by the Parties will apply.
- 24.3. The appendices listed in the Terms of Service constitute an integral part thereof.
- 24.4. The Terms of Service shall enter into force on the date of their publication on the Website in their current wording or on the date resulting from the Agreement concluded with the User. The Terms of Service shall replace, as of the date of their entry into force, all previous Terms of Service/contractual templates of the Service Provider to the extent covered by the Terms of Service.

List of attachments:

1. Template of the withdrawal form
2. Data Processing Agreement

City, date

.....
.....
.....

Name of consumer(s)

Address of the consumer(s)

Fiberax sp. z o.o.
Puławska 405A/303
02-801 Warsaw

**Statement
on withdrawal from a distance agreement
or off-premises**

I/My (*)..... I hereby inform (*) of my/our(*) withdrawal from the contract of sale of the following items(*)

.....
contracts for the supply of the following items(*)

a contract for specific work consisting in the performance of the following things/for the provision of the following
service(*).....

Date of conclusion of the contract¹/receipt²(*).....

.....
Signature of the consumer(s)

(*) Delete as necessary

¹ indicate if the agreement concerned the provision of services

² specify if the agreement concerned the purchase of goods

Data Processing Agreement ("this Processing Agreement")

Definitions

Controller	Controller of the Personal Data entrusted to Service Provider, determining the purposes and means of processing of Personal Data;
Legal Acts	Legislation applicable to Service Provider as a Personal Data processor in the meaning of Article 28 of the GDPR in relation to entering into the Processing Agreement, including, without limitation, the GDPR;
Personal Data	Personal data in the meaning of the GDPR;
Place of Processing	Locations where Service Provider processes Personal Data defined in the Processing Agreement;
Principal Agreement	Service agreement that specifically stipulates services consisting of providing the Customer with access to the Cloud resources (virtual machines, computing powers, database services, virtual servers) that are used to store, share and process data;
Sub-processing	Situation when Service Provider subcontracts Personal Data processing to a third party that will be obliged to process the Personal Data in accordance with this Processing Agreement and Service Provider will be liable for actions of that party as for its own actions or omissions;
GDPR	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;

Recitals

Whereas:

- 1) *The Customer processes information constituting Personal Data,*
- 2) *The Customer has entered into the Principal Agreement with Service Provider;*
- 3) *Data transferred by the Customer to Service Provider in relation to the Principal Agreement include also Personal Data;*

The Parties mutually agree to enter into this Processing Agreement as follows:

Article 1

Subject matter of this Processing Agreement

1. The Customer subcontracts processing of Personal Data to Service Provider in the scope specified in this Processing Agreement, and Service Provider undertakes to process them in accordance with this Processing Agreement.
2. Service Provider will process Personal Data as part of the fee agreed in the Principal Agreement. Capitalized terms not defined herein will have the meaning assigned to them in the Principal Agreement.

Article 2

Representations of the Parties

1. The Customer represents that, subject to section 2 below, it is the Controller.
2. In each case when Personal Data include any data of which the Customer is not the Controller, the Customer represents that its business partner is the Controller of such data and that pursuant to the law and the agreement with such business partner, the Customer is authorised to transfer such Personal Data onward to Service Provider on the terms determined in this Processing Agreement.
3. The Customer will, at the request of Service Provider specifically due to an audit carried out by competent supervision authorities or change in the interpretation of the provisions of law, immediately (i.e. within 3 business days) deliver to Service Provider in electronic form the current list of Controllers (business partners) referred to in section 2 above, in accordance with the template enclosed as Annex no. 1 hereto.
4. The Customer declares that Personal Data provided to Service Provider for processing have been obtained lawfully and their processing and further processing by Service Provider is not in breach of any law or third party rights.
5. Service Provider undertakes to only process Personal Data in the scope necessary to perform this Processing Agreement and the Principal Agreement and for the purposes defined in those Agreements.
6. Service Provider declares that it is familiar with and undertakes to observe the Legal Acts, subject to section 7 below.
7. Should any special Legal Act that is usually not applicable to enterprises similar to Service Provider and established in Poland apply to Service Provider in relation to entering into this Processing Agreement considering the nature of the Personal Data or special status of the Customer, the Customer will notify Service Provider about that fact in writing (other forms of notifications will not be valid), at least 30 days in advance, and Service Provider will be entitled to terminate this Processing Agreement within the next 14 days with 7 days' notice period.

Article 3

The scope of Personal Data and processing categories

1. Due to the nature of services provided by Service Provider, the type of Personal Data and categories of data subjects are determined and controlled by the Customer. Depending on the case, Personal Data entrusted to Service Provider for processing may include, without limitation: contact details; personnel / associate data; billing and payment data, including data processed by payment institutions; marketing data; special data categories; other types of data in accordance with agreements concluded by Service Provider with its clients. Depending on the case, Personal Data processed by Service Provider

may concern, without limitation, the following categories of data subjects: employees and associates of the Controller or associated enterprises of the Controller, clients or further customers of the Controller; clients of services / products of the Controller and their further customers; business partners of the Controller or clients/further customers of the Controller.

2. The categories of processing of Personal Data by Service Provider may include, without limitation:
 - a. Storage of the Personal Data in the technical infrastructure /Cloud service equipment provided by Service Provider, and also ensuring the use of computing power of that equipment for the processing of Personal Data by the Customer in a manner chosen by the Customer, in accordance with the Principal Agreement;
 - b. Physical security and physical maintenance of technical infrastructure / Cloud service equipment at the Cloud level;
 - c. Ensuring appropriate logical Cloud access safeguards at the Cloud level;
 - d. Ensuring access to the Services, in accordance with the Principal Agreement;
 - e. Provision of technical support for the Customer's virtual machine – only when such technical assistance is established and used,
 - f. Customer's Services management for the virtual machines designated by the Customer – only when such service is established and used.
3. For the avoidance of doubt, without prejudice to sections 4-5 below, the Customer independently administers the virtual machines where the Personal Data are processed, among other things independently installs software selected by the Customer, implements safeguards, makes back-up copies, and performs other obligations under the Legal Acts.
4. The Customer may order Service Provider to make and maintain back-up copies of Customer's Data, which will include making back-up copy of the whole "virtual machine" of the Customer, on the principles agreed in detail for such additional Service.
5. The Customer may provide to Service Provider access to its virtual machines (in the scope determined by the Customer and with the application of suitable safeguards selected by the Customer) by:
 - a. The creation of administrative account on the virtual machine for a person acting on behalf of Service Provider to perform specific ad hoc operation; or
 - b. The use of use of a service involving technical, administrative, or similar support.

In such case the Customer will provide to Service Provider instructions on the scope of operations that may be performed by Service Provider's designees, in electronic form, and Service Provider, in addition to the obligations specified in Article 4 below, will be obliged also to exercise due care, to the extent possible for Service Provider, to ensure accountability for the actions of those persons in the Customer's virtual machines (i.e. activity logs and the possibility of activity allocation to specific individual) and to obligate them to act in accordance with this Processing Agreement and the law.

Article 4

Principles of Personal Data processing

1. The Personal Data will only be processed by Service Provider for the purpose of the provision to the Customer of the Services specified in the Principal Agreement, in accordance with the Principal Agreement and this Processing Agreement (nature and purpose of the processing), within the categories of processing activities specified in Article 3(3) above.
2. Service Provider undertakes to:
 - a. Process the Personal Data only on documented instructions from the Customer – including with regard to transfers of personal data to a third country or an international organisation – unless required to do so by Legal Acts; in such case, before processing commencement, Service Provider will notify the Customer of that legal requirement unless Legal Acts prohibit such information on important grounds of public interest;
 - b. Ensure that persons authorised to process personal data on the side of Service Provider have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
 - c. Take measures required pursuant to Article 32 of the GDPR, in the scope related to the performance of this Processing Agreement, described in Annex no. 2 and Annex no. 3 hereto;
 - d. Respect the conditions for engaging another processor in accordance with sections 4 and 5 below;
 - e. Insofar as this is possible and in the scope justified by the nature of the processing activities, to assist the Customer by appropriate technical and organisational measures for the fulfilment of the obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;
 - f. Assist the Customer in ensuring compliance with the obligations pursuant to Articles 32-36 of the GDPR taking into account the nature of processing and the information available to Service Provider, to the extent required by law;
 - g. At the choice of the Customer, delete or return all the Personal Data to the Customer, in accordance with Article 7 below, after the end of the processing under this Processing Agreement, and delete existing copies unless the Legal Acts require storage of the Personal Data;
 - h. Provide to the Customer information necessary to demonstrate compliance with Service Provider obligations specified in this section, within the limits justified by the nature of the processing activities;
 - i. Allow audits and inspections conducted by the Customer in accordance with Article 5 below.
3. Service Provider may contract Sub-processing of Personal Data exclusively on the rules defined herein. Service Provider will notify the Customer of the intention to use Sub-processing, indicating the third party and specific processing activities that will be subject of the Sub-processing, in the form of an email, at least 30 days before planned Sub-processing. The Customer, within 7 days of receipt of the notice referred to in the preceding sentence, may notify justified objection against Sub-processing that will be provided to Service Provider as a reply email to be valid. Should Service Provider receive the objection, it will be entitled to submit a notice of termination of this Processing Agreement to the Customer within the next 5 days, with 14 days' notice period.

4. The Customer hereby agrees to the Sub-processing of the Personal Data by Netia S.A. with its registered office in Warsaw, ul. Poleczki 13, 02-822 Warszawa, tel. 801 801 999, biznes@netia.pl, by ATM S.A. with its registered office in Warsaw, ul. Grochowska 21a, 04-186 Warszawa, tel. 22 51 56 100, info@atman.pl, in relation to the activities specified in Article 3(3)(b) above.
5. The Customer declares that the scope of the Personal Data and the categories of processing activities covered by this Agreement do not require and will not require during the term of this Processing Agreement application of any specific measures for their processing or compliance with other special conditions (such as obtaining consent, registration, certificate etc.) other than those described in Annex no. 2 and Annex no. 3, subject to the provisions of the next sentence. For the consideration determined in the Principal Agreement, Service Provider undertakes to also apply special security measures other than those described in Article 4 of this Processing Agreement, if they are available to Service Provider and commercially and economically reasonable from the point of view of Service Provider, within 21 business days of receipt of the Customer's request provided in the form of an email.
6. The Customer will be obliged to apply appropriate cryptographic (encryption) techniques for all Personal Data at the stage of their transfer to/from Service Provider infrastructure and at the stage of their storage within Service Provider infrastructure (obligation of encryption of virtual machine or disc where the Personal Data are stored), and also to apply any other safeguards required under the GDPR for virtual machines, to appropriately secure the Personal Data and ensure lawful processing thereof. Service Provider will not be liable for any effect of the violation of the above obligations by the Customer. Under separate agreement between the Parties, it is possible for Service Provider to provide dedicated Service security solutions as part of the support.
7. For the avoidance of doubt, the Parties acknowledge that performance of the obligations under the Legal Acts, including the GDPR, in relation to the Personal Data processed in virtual machines, specifically including in the scope of organisational and technological safeguards and making back-up copies, is exclusively the obligation of the Customer. Subject to Article 3 sections 5 and 6 above, Service Provider will not obtain direct access to the Personal Data and will not perform any direct operations on that Data, but will only perform operations on the Cloud as a technology and data set without the ability to separate them directly.
8. In each case of Service Provider finding a breach of Personal Data provided to Service Provider for processing by the Customer, Service Provider will without undue delay, if possible within 48 hours of discovering the given breach, notify it to the Customer in the form of an email. Such notification will include the following information known to Service Provider and considering the nature of the processing:
 - a. The nature of the breach, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - b. Likely consequences of the breach;
 - c. The measures taken or proposed to be taken to address the breach, including, where appropriate, measures to mitigate its possible adverse effects;

Where and as far as it is not possible to provide the information at the same time, the information may be provided gradually without undue delay.

Article 5

Control rights

1. The Customer is entitled independently and the Controllers listed in Annex no. 1 are entitled jointly with the Customer to control processing of Personal Data by Service Provider under this Processing Agreement through audits or inspections, not more frequent, however, than once every 6 months in total. The Customer may, at its own expense, order a Control by a professional auditor for whom the Customer will be responsible. In case of each control, the Customer will notify Service Provider of the intention to carry out a control, providing at the same time the control plan, at least 14 business days in advance, and Service Provider will be obliged to allow such control, specifically including through provision of appropriate documents and premises to the extent necessary to carry out the control, and to provide any necessary information on the performance of this Processing Agreement, subject to Service Provider's obligations under the law or contracts entered into with other Controllers and Service Provider's trade secret. When a control could have an adverse effect on the ongoing functioning of Service Provider or any entity to which Service Provider subcontracts certain activities, the Parties will jointly set a different, suitable date of control.
2. Controls may be carried out on business days from 9:30 a.m. to 5:30 p.m. in such manner as not to interfere with the work of Service Provider or the Place of Processing. A single control at those places may not last longer than 3 business days in total. Should the performance of a control at the date designated by the Customer in accordance with section 1 above be impossible for objective reasons (such as concurrent control by another user), Service Provider will immediately notify the Customer accordingly and the Parties will immediately agree a different possible date for the control.
3. The Parties will draw up a control report. The Customer may present recommendations concerning the quality of Personal Data safeguards and means of processing, prepared as an outcome of the control, within the period agreed by the Parties.
4. Any cost of controls will be covered by the Customer.
5. Service Provider will be obliged to notify the Customer of any control carried out at Service Provider by authorised government authorities if it is related to the processing of Personal Data provided by the Customer, within 3 business days of the date of receipt of relevant letter, request or information of the planned control.
6. In the case referred to in Article 2(2) of this Processing Agreement, Service Provider will be entitled to request the Customer to evidence the entitlement to onward transfer of Personal Data at any time, and the Customer will be obligated to deliver to Service Provider appropriate declaration of the Controller, in written or electronic form, otherwise invalid, within 5 business days of the date of receipt of the request via email.

Article 6

Term of this Processing Agreement

1. This Processing Agreement is concluded for the term of the Principal Agreement concluded between the Parties, subject to section 2.
2. Termination of the Principal Agreement at any time and in any mode by any of the Parties will cause termination of this Processing Agreement.
3. In case the Customer declares that it has ceased processing of Personal Data as part of Services, the Customer will be entitled to terminate this Processing Agreement with one month's notice period.

Article 7

Personal Data Erasure

1. The Customer may erase Personal Data processed as part of the Services at any time for example by appropriate overwriting through independently selected software installed and used by the Customer in the virtual machine and in accordance with the procedure determined by the Customer – erasure occurs at the time and on the principles determined independently by the Customer.
2. The Customer will be able to freely export Personal Data throughout the term of this Processing Agreement through the export of individual databases / programs created independently by the Customer and managed by the Customer, in formats appropriate for such databases / programs (functionalities managed by the Customer).
3. At the latest by termination of this Processing Agreement or the Principal Agreement, the Customer will be obliged to export Personal Data and make sure that all Personal Data have been erased from the Cloud and submitted within the deadline will be considered.
4. Regardless of the provisions of section 3 above, Service Provider will, within 14 days of the termination of the Principal Agreement, erase Customer's virtual machines that had not been previously erased by the Customer, which will cause immediate unavailability of data stored there and their erasure within the subsequent 14 days.
5. The Parties may stipulate in the Principal Agreement separate rules of terminating the collaboration other than the above.

Article 8

Liability

1. Service Provider will be liable for damage caused to the Customer and third parties (including specifically other Controllers) in relation to the performance of this Processing Agreement, exclusively on the principles and within the limits specified in the Principal Agreement. That liability covers also Service Provider's liability for entities Sub-processing Personal Data for Service Provider in accordance with this Processing Agreement.
2. The Customer will be obligated to ensure performance of the provision of section 1 above under relevant contracts with appropriate third parties to the extent allowed by the law.

Article 9

Miscellaneous

1. Service Provider will be entitled to unilaterally update the content of Annexes no. 2 or 3 in the form of an email message, otherwise such update will be invalid, in case of a change of the scope of the solutions / safeguards used by Service Provider or an entity Sub-processing Personal Data for Service Provider, provided that they are compliant with the requirements specified in the GDPR. Should the Customer find the changes made by Service Provider in accordance with the preceding sentence to be non-compliant with the GDPR, the Customer will notify Service Provider accordingly within 14 days of the given update, in the form of a reply email message.
2. Matters not regulated in this Processing Agreement will be governed by generally applicable laws and regulations of Poland and the provisions of the Principal Agreement.
3. If the same issues are regulated differently in the Processing Agreement and in the Principal Agreement, the provisions of the Processing Agreement will prevail.

List of annexes:

Annex no. 1 – TEMPLATE: List of Controllers;

Annex no. 2 – Security procedures used by Fiberax sp. z o.o.;

Annex no. 3 - Description of the organisation and means of safeguarding information resources by sub-contractors.

ON BEHALF OF SERVICE PROVIDER:

_____ Olha Yuzbekova

ON BEHALF OF CUSTOMER:

_____ Johan Skolen

Annex no. 1 – TEMPLATE: List of Controllers

No.	Name of the Controller and its representative (if any)	Controller's registered office address	Controller's email address	Name and email address of Data Protection Officer (if any)

Annex no. 2 – Security measures used by Fiberax sp. z o.o.;

Description of Fiberax security measures

Fiberax sp. z o.o. implements the following legal, technical, and organizational measures to ensure an adequate level of security for the provided services:

1. Legal measures:
 - a. Fiberax sp. z o.o. is the owner of the infrastructure used to provide services, including servers, storage systems, network switches and routers, and cabling;
 - b. All persons acting on behalf of Fiberax sp. z o.o. in the processing of personal data for which Fiberax sp. z o.o. is the controller or processor have undertaken to keep such information confidential and not to use it for any purpose other than that related to the performance of their professional duties;
 - c. A breach of the confidentiality obligation referred to in point b above constitutes, in principle, an offense against the protection of information (Article 266 et seq. of the Criminal Code Act of 6 June 1997) and the persons to whom this obligation applies have been informed of this fact;;
 - d. Fiberax sp. z o.o. is aware of and constantly strives to fully comply with the obligations imposed on it by the relevant provisions of law, including in particular 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, including monitoring and taking into account, where necessary, the opinions and guidelines of relevant supervisory authorities, such as the European Data Protection Board;
 - e. All agreements concerning the entrusting of personal data by Fiberax sp. z o.o. to a third party for processing, where Fiberax Sp. z o.o. acts as a controller or processor, comply with the requirements of the GDPR and are concluded only with entities that provide sufficient guarantees to implement appropriate technical and organizational measures so that the processing meets the requirements of the GDPR, including having sufficient experience and reputation;
2. organizational measures:
 - a. Fiberax sp. z o.o. has developed and implemented policies related to the security of personal data processing;
 - b. Fiberax sp. z o.o. holds valid ISO 27001, ISO 27701, and ISO 9001 certificates;
 - c. Fiberax sp. z o.o. has appointed a Data Protection Officer;;
 - d. A system/program update procedure has been implemented - systems are updated periodically in accordance with a defined schedule. In the event of an error/vulnerability that significantly affects the security of the environment, updates are performed immediately, regardless of the defined schedule;
 - e. The so-called system hardening solutions are used;
 - f. Each member of Fiberax sp. z o.o. staff has their own ID (login + password) which they use within the organization. Access for each person and their level of authorization is granted in accordance with the least privilege policy and solely for the purpose of performing their professional duties;
 - g. All persons acting on behalf of Fiberax sp. z o.o. undergo periodic training in data protection and information security;
3. technical measures:
 - a. All data transmitted between Fiberax sp. z o.o. servers at the cloud level is encrypted;
 - b. The configuration of systems used at the cloud level is performed from a central configuration management system, and there is also a local mechanism for tracking configuration changes on servers;
 - c. The infrastructure of Fiberax sp. z o.o. allows Users to use any known technological solutions within their virtual machines that may serve to ensure the security of stored personal data, including the possibility of pseudonymization or encryption of stored data, the use of VPN solutions, etc. Each user storing personal data in virtual machines is required to encrypt these machines (use cryptographic solutions);
 - d. Access to the internal network of Fiberax sp. z o.o. used for cloud management is based on multi-stage authorization, and there is also network segmentation, where a specific internal user has access only to a separated part of the infrastructure;
 - e. The infrastructure is subject to security tests - vulnerability detection mechanisms are used, and all systems are scanned on an ongoing basis (tests are performed according to a schedule) for currently published vulnerabilities (CVE). Fiberax sp. z o.o. also uses the services of external companies that periodically conduct infrastructure security audits (DSS) and immediately implement any recommendations;
 - f. Infrastructure performance monitoring is used 24/7/365 to detect failures - both internal and external automated network monitoring tools are used, and in the event of a failure, a Fiberax sp. z o.o. engineer is available around the clock..

Annex no. 3 - Description of the organisation and means of safeguarding information resources by sub-contractors.

NETIA

This Annex contains a description of safeguards affecting security in the processes where personal data are processed at NETIA S.A.

NETIA S.A., a colocation service provider, implements and maintains advanced physical security measures and technical safeguards to ensure the highest level of security for the data being processed. As part of its activities, the subcontractor uses advanced technologies to protect against unauthorized access, control access to infrastructure, and monitor the IT environment, which minimize the risk associated with cyber threats. The effectiveness of the security measures implemented is confirmed by the certificates of compliance with international standards PN-EN ISO/IEC 27001:2017-06 and ISO 9001:2015 obtained by the subcontractor.

1. Organisational Security Measures

To ensure the secure processing of data, the following organisational security measures have been implemented:

- a. Access to the facility is controlled by an Access Control System (ACS)
- b. Access for individuals who do not hold access cards is strictly regulated under the facility's internal procedures.
- c. The entire facility and the adjacent premises are enclosed by fencing.
- d. All incoming and outgoing vehicles are subject to control procedures.
- e. All facility staff are trained in data protection (including the protection of personal data) and undergo regular refresher training.
- f. All employees and contractors working on-site are bound by confidentiality obligations regarding the security of the facility and may not use any related information for purposes other than the performance of their professional duties.
- g. Taking photographs or otherwise recording any part of the facility is strictly prohibited without authorisation.

2. Technical Security Measures

To ensure the secure processing of data, the following technical security measures have been implemented:

- a. Precision air conditioning operating in an N+1 configuration; no installations unrelated to the server rooms run through these areas.
- b. Power supply system configuration using independent paths, meeting redundancy principle.
- c. Uninterruptible Power Supply (UPS) systems and backup generators, forming a redundant power source.
- d. Emergency power backup system.
- e. Two power supply connections.
- f. Early smoke detection system.
- g. Fire alarm system with automatic notification to the State Fire Service.
- h. Fixed fire extinguishing systems.
- i. CCTV monitoring system.
- j. The facility integrates technical protection systems with physical security measures.
- k. Building Management System (BMS) integrating alarms from detection systems, including water leakage sensors, gas sensors, temperature limit sensors, fire detectors, and power supply monitoring.

ATM

1. Organisational safeguards

- a. ATM has the documentation that regulates organisation of the personal data protection system – the ATM S.A. Personal Data Protection Policy,
- b. ATM has the Incident Management Procedure that guarantees the ability to quickly restore personal data availability and access to them in case of a physical or technical incident,
- c. ATM has appointed a Data Protection Officer,
- d. ATM has a certified Integrated Management System compliant with ISO 27001 and ISO 9001, directly affecting security of the services,
- e. all employees and associates of ATM have been authorised to process personal data,
- f. ATM organises for its employees and associates initial and periodic personal data protection training.

2. Physical and environmental security

- a. ATM ensures complete control of people and vehicle movement within its administrative area – supervision is performed by a third party: licensed security company,
- b. ATM premises are divided into security areas and movement in the areas is supported by the Access Control System that guarantees complete accountability and access authorisation control,
- c. ATM premises are monitored by the CCTV cameras,
- d. ATM premises are equipped with the Perimeter Intrusion Detection System embedded in the monitoring system of a licensed security company that guarantees response by armed response teams,
- e. ATM premises are equipped with the fire protection system and multi-zone INERGEN® fire-fighting system,
- f. Signals from security systems are received and monitored continuously (including signals concerning network infrastructure, electricity supply and server security, administration and office facilities, and other important resources used to provide services by ATM) – those systems are tested on a regular basis,
- g. Continuity of processes in server rooms is based on cascading and redundant back-up power supply including: UPS, dedicated power generators, and redundant power stations.
- h. The following infrastructure protection and security services work continuously, i.e.

24/7/365:

- technical and reception services,
 - data centre perimeter and building security (licensed security company),
 - Customer Service and NOC (Network Operations Centre).
- i. Physical access to hardware platform on the basis of which the service is provided is limited to a selected group of consultants–engineers. Access by any third party or ATM employees from outside that group is prohibited and is subject to strict control.