Fiberax

TERMS OF SERVICE
OF FIBERAX SP. Z O. O.

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

TABLE OF CONTENTS

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 or other individual arrangements between the Parties. The Price List is attached to the Terms of Serivce, to which point 3 of the Terms of Service applies.

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 using the Services

Provider

Fiberax sp. z o.o. with its registered office in Warsaw, address: Puławska 405a, 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 number 0001043360, NIP: 9512571325, REGON: 525646336, with a share capital of PLN 1,000,000.00, e-mail: 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 through which the User may be provided with the ability to manage Resources within the scope of the rights arising from the Terms and Conditions and the Service Card for the Services provided by the Provider, updating the User's contact details and providing the User with information necessary for the Provider to provide the Services to the User. Access to the User Account is provided at https://fiberax.com

Tariff Units Service consisting in the readiness of the Provider to provide the relevant Services, enabling the User to use the relevant Services

Terms of Service this document together with its 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 Provider on the Website constitutes an invitation to conclude the Agreement within the meaning of Article 71 of the Civil Code; The parties expressly exclude the application of Article 661 §§ 1-3 of the Civil Code

Parties User and Provider together

Agreement an agreement concluded between the Provider and the User specifying the rights and obligations of the User and the Provider in connection with the provision of 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

One-time service A one-off service provided by the Provider to the User

Periodic service Service provided to the User on a recurring or continuous basis during the period resulting from the Agreement

Data Loss accidental or unintentional loss, damage, unauthorized access, modification or destruction of User Data processed as part of the Services

User an entity with full legal capacity, excluding consumers, who is a party to the Agreement

Post-Paid User User who is a party to a written agreement, which is null and void unless made in writing, to which the provisions of the Terms of Service do not apply, unless the Terms of Service or the aforementioned written agreement clearly state otherwise.

Pre-Paid User A user who is a party to an Agreement concluded in accordance with the procedure specified in section 4.2 of the Terms of Service;

Remuneration fees charged by the Provider to the User for the provision of Services

Resources i.e. 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's Data based on 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.

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 has the right to amend the Terms of Service and Appendices (including to the extent that they relate to the Remuneration, which may result in particular from the improvement of the Services, an increase in costs or an increase in the remuneration of specialists on the market) at any time. The User will be notified of each change by means of information sent to the e-mail address or via the User's account, which the Parties consider to be the fulfillment of the condition set out in Article 384 of the Civil Code for the ease of learning about the modified content of the standard contract. 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 of termination of the Agreement within 15 days from the date of sending the information about the change. In such a case, the Agreement shall be terminated after the lapse of 30 days from the date of sending the above-mentioned information on the amendment of the Terms of Service.

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 Provider may enable the conclusion of the Agreement in electronic form. In such a case, the Agreement shall be concluded upon the simultaneous fulfilment of the following conditions:

a. registration via the registration form and acceptance of the Terms of Service or

b. acceptance of the Terms of Service without registering 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, PayU, PayPal 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 period for which the Agreement was concluded is specified in the Agreement.

7.2. Regardless of the period for which the Agreement was concluded, the Provider may terminate the Agreement with 7 days' notice in the event of:

a. 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;

b. adopt a resolution on the liquidation of the User;

c. violation by the User of the provisions of law or the Agreement, if the User fails to cease such violations within the time limit set by the Provider;

7.3. 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.

PART III – RULES FOR THE PROVISION OF SERVICES

8. MODES OF SERVICE PROVISION

8.1. The Services may be provided by the Provider in the following modes:

a) Test Mode

b) Commercial Mode.

8.2. The Test Mode is aimed at assessing the quality and functionality of the Service before its implementation, whereby:

a) not all Services provided by the Provider are available in Test Mode;

b) Services in Test Mode may not be used in a live production environment or for development or commercial purposes;

c) versions of the Service in Test Mode are provided 'as is', without warranty, service level commitment or security;

9. SCOPE OF SERVICES PROVIDED

9.1. The scope of Services provided by the Supplier to the User is specified each time in a dedicated Service Card.

10. LIMITATION OF THE SCOPE OF SERVICES BY THE PROVIDER

10.1. If the User Account provides for such functionality, the User may, within the limits specified in the Agreement, select the Services and modify their parameters via the User Account or another access point to the Service.

10.2. The Provider may impose technical restrictions on the use of the Services (including software within virtual machines) or maximum values (limits) for individual Services. Lifting restrictions or launching the Services above the limit requires the express consent of the Provider given at the User's reasonable request.

10.3. The restrictions or limits introduced by the Provider referred to in clause 10.2 may be global (for all customers), apply to individual customers or selected groups of customers.

10.4. The User whose place of residence/stay, registered office or place of business is located outside the territory of the European Economic Area, Switzerland and the United States of America shall present, at the request of the Provider, appropriate official documents in Polish or English (acceptable translation certified by a notary, official or other of equal legal significance) confirming the place of residence/stay, location of the registered office or place of conduct of the User's activity. In the event of a breach of this obligation, clause 10.4 shall apply.

11. OBLIGATIONS OF THE PROVIDER

11.1. 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.

11.2. If the User Account is made available, the Provider provides the User with access and use of the User Account as is, i.e. without any assurance as to its functionality or availability, or suitability for the User's purposes, or guarantee of operation.

11.3. 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.

11.4. 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.

12. USER RESPONSIBILITIES

12.1. 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 concerning 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, under pain of considering correspondence sent to the current registered office addresses and e-mail addresses as effectively delivered;

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;

f. maintain at least one current backup copy of the User's Data in an infrastructure other than the one provided by the Provider throughout the term of the Agreement; this obligation does not apply if you purchase an additional Service consisting in the Provider making and maintaining a backup copy of User Data;

12.2. User is solely responsible to third parties for User Data.

12.3. User agree that it will use the Services only for civil purposes, including but not limited to the commercial provision of services using the Services.

12.4. 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.

13. USER DATA

13.1. The use of the Services as services provided electronically involves typical risks associated with the transmission of data via the Internet, such as the dissemination of User Data, access to it by unauthorised persons or Data Loss.

13.2. To the extent that Personal Data is processed through the Services, the provisions of the Privacy Policy available on the Website shall apply, unless the Parties have entered into a dedicated agreement for the processing of personal data, in which case the dedicated agreement shall replace the provisions of the Privacy Policy in matters not covered by the latter.

13.3. Immediately after concluding the Agreement, the User shall send an email to Gdpr@fiberax.com, under pain of nullity, describing the scope of the Personal Data entrusted and the categories of persons to whom it relates, which shall replace the relevant provisions of the Privacy Policy. By failing to do so, the User confirms that the current provisions of the Privacy Policy correspond to the scope of Personal Data entrusted by the User and the categories of persons to whom it relates.

13.4. If the User guarantees that the User Data does not contain Personal Data, they shall immediately after concluding the Agreement inform the Provider thereof by email, under pain of nullity, to the address referred to in point 13.3 above. In such a case, the Privacy Policy shall not apply between the Parties with regard to Personal Data.

13.5. The User undertakes that the scope of User Data does not require and will not require, during the term of the Agreement, the use of any special measures for its processing other than those described in the Terms of Service or the fulfilment of any other special conditions by the Provider (e.g. obtaining consent, registration, certification, etc.).

14. USER INTELLECTUAL PROPERTY

14.1. 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 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.

14.2. The User who has undertaken to obtain rights to the User Data, including intellectual property rights, for himself and, to the extent necessary for the performance of the Services, for the Provider, is obliged to indemnify the Provider against liability towards third parties making claims related to these rights to the User Data, as well as to repair the damage caused to the Provider in connection with the above, confirmed by a final judgment of a common court or in respect of which a settlement has been concluded, immediately, not later than within 7 days, at the request of the Provider.

14.3. The User is obliged to take necessary measures to protect the Provider at its own expense against claims of third parties directed to the Provider, in connection with the rights or infringement of rights to the User's Data, and to cover the costs of the Provider incurred in connection with the filing of such a claim against the Provider (including reasonable attorneys' fees), provided that the Provider immediately, i.e. no later than within 7 days, inform the User of any such claims and enable the User to take certain actions on its behalf or on its behalf in connection with the defense against such claims, and provide it with all information necessary to exercise the above rights free of charge. You will have the right and obligation to conduct and control any disputes with third parties in this regard.

14.4. For the purposes of this point, the Provider shall also be understood as employees, associates, subcontractors, etc. Provider.

14.5. The provisions of this clause shall also apply accordingly after the expiration of the Agreement, its termination or withdrawal from the Agreement by either Party.

14.6. The User is obliged to keep the Provider, its subcontractor or the entity cooperating with the Provider informed about the actions taken.

15. PROVIDER INTELLECTUAL PROPERTY

15.1. 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 15.3 below.

15.2. The Provider represents that at the time of conclusion of the Agreement, it provides the Services in particular on the basis of the Microsoft Services Provider License Agreement (SPLA).

15.3. 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. The Provider is not a party to such an agreement concluded between the User and a third party, and is not responsible for the performance of such agreement by its Parties.

16. CONFIDENTIAL INFORMATION

16.1. 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.

16.2. 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.

16.3. 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.

16.4. The confidentiality obligation is valid for the duration of the Agreement and for 10 years after its termination or expiration.

17. ACTIVITIES

17.1. The User grants the Provider permission for the Provider to use information about cooperation with the User for the purpose of marketing the Provider's products and services, including the use of the User's trademarks or other markings for this purpose (authorization / license to the extent necessary justified by the above-mentioned purpose).

17.2. The Provider may provide information about cooperation with the User, in particular as part of such activities as:

a. INTERNET MARKETING, which is understood as marketing activities on the Internet;
b. EVENT MARKETING, which is understood as the promotion of a company or product at various types of events;
c. advertising with the use of mass media, m.in. television advertising, press advertising;
d. Information addressed to a specific customer, m.in. information contained in leaflets, offer catalogues, etc.

17.3. The provisions of this section are valid for the duration of the Agreement. After this period, they become an agreement concluded for an indefinite period of time, with a one-month notice period (in writing under pain of nullity), with effect at the end of the month.

PART IV – PRINCIPLES OF LIABILITY

18. COMPLAINT PROCEDURE

18.1. The User may raise objections related to access to the Services, their use or their functioning in the form of a complaint, within 30 days from the occurrence of the event justifying the complaint.

18.2. The Provider will consider the User's complaint within 14 days of receipt of the User's complete complaint, with the proviso that this time may be extended to 30 days in justified cases.

18.3. Complaints may be submitted to the Provider via the User Account or to the following e-mail address: support@fiberax.com or to the address of the Provider's registered office. A complaint should always include at least:

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.

18.4. In the event of the absence of any of the elements indicated in point 18.3, the Provider will call the User to supplement the deficiencies within 7 working days, unless the User did not indicate the address in the written complaint. If the deficiencies are not completed within the set deadline or the address is not indicated, the complaint will not be considered, unless the content of the complaint indicates that it may also be considered in the event of deficiencies.

19. USER RESPONSIBILITY

19.1. The User is responsible for access to and use of the Services by persons whom the User has authorised to access or use the Services or to whom the User has provided data enabling authentication in the Fiberax Cloud and on the User Account.

20. PROVIDER RESPONSIBILITY

20.1. The Provider will be liable for any damage caused to the User intentionally.

20.2. The fact that the action or omission from which the damage resulted constituted a non-performance or improper performance of an obligation excludes the User's claims for compensation for damage on the grounds of a tort.

20.3. In any case where the Provider is liable under contract or in tort, such liability shall be limited to the amount of the Remuneration actually paid by the User in the month preceding the occurrence of the event for which the Provider is liable.

20.4. The total limit of the Provider’s liability for contractual and tortious damages incurred in a given calendar year shall be equal to the sum of the Remuneration paid to the Supplier by the User for the last 6 months of the provision of the Services or for the actual duration of the Agreement, if it is shorter than the above-mentioned period of 6 months.

20.5. In each case where the Provider is liable under contract or tort, such liability shall be limited to the amount of the Remuneration actually paid by the User in the month preceding the occurrence of the event for which the Service Provider is liable, and if the term of the Agreement is shorter, for the entire term of the Agreement for the provision of:

a. Tariff Units redeemed in exchange for those Services performed in connection with which the Pre-Paid User suffered damage/harm; or
b. those Services in connection with the performance of which the Post-Paid User suffered damage/harm.

20.6. The Provider shall not be liable for any lost profits of the User. The Provider shall not be liable to the User for any damages related directly or indirectly to the provision of Services to the User, arising from the fault or as a result of claims or actions of third parties resulting from access to the Services, their use by the User or their employees/associates.

20.7. 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 an event which is force majeure, i.e. events beyond the control of the Parties, in particular wars, natural disasters, cyber attacks (including DDoS), provided that such an event does not release the User from the obligation to pay the Fee.

20.8. The Provider shall not be liable for the Loss of Data, unless the Agreement provides otherwise or the Loss of Data was intentional – in such a situation, the Provider's liability shall be governed by the relevant SLA, and in the scope of the non-regulated SLA, the limitations resulting from this section shall apply.

20.9. For the purposes of this point, the Service 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.

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

21.1. In the event of any of the circumstances indicated below, the Provider may Suspend the User's access to the Services 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 7-day deadline from the moment the Provider sends the e-mail;
f. the existence of an obligation resulting from the law or from the decisions of competent state authorities or courts;
g. other breach by the User of the provisions of the Agreement.

21.2. If the Provider determines that, in its opinion, any User Data constitutes illegal content within the meaning of Article 2(g) 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.

21.3. 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.

21.4. The Provider is entitled to the Remuneration for the period of Suspension for being ready to provide the Services or process the User Data.

PART V – MISCELLANEOUS

22. SUBCONTRACTORS AND ENTITIES COOPERATING WITH THE PROVIDER

22.1. The Provider may entrust the performance of the Services in whole or in part to subcontractors.

22.2. The Provider may provide the Services with or on behalf of the Provider's partners.

22.3. Some Services may also be provided directly by third parties, on the basis of separate Terms of Service and as part of separate remuneration.

22.4. With respect to the cooperation referred to in Section 16.2 (cooperation with Microsoft under SPLA), by signing the Agreement, you accept and agree to be bound by the following Microsoft documents:
https://www.microsoft.com/licensing/spur
https://www.microsoft.com/licensing/terms,

22.5. If you update any of the documents listed in Section 22.5 above, you must accept the terms of the updated documents within the time period specified by Provider or directly by Microsoft. Failure by the User to perform the obligations indicated in this section 22.6 of the Terms of Service may result in suspension or refusal to provide the Services to the User.

22.6. In the event that the provision of Services by the Provider to the User or the use of the Services by the User results in the Provider's obligation to pay any additional amounts to the third party referred to in this Section 22, the User is obliged to immediately return such amounts to the Provider in full.

22.7. You are fully responsible for any breach of any third party Terms of Service referred to in this section by you or persons using the Services on your behalf or through you. In particular, you will be required to fully compensate the Provider for any damages (recourse liability) incurred by Microsoft or any other third party for any infringement of the rights of such third parties in connection with or in connection with the use of the Services.

23. TRANSFER OF RIGHTS AND OBLIGATIONS UNDER THE CONTRACT

23.1. 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.

23.2. 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 agrees. The Provider undertakes to ensure that such transfer will not affect the quality and continuity of the Services provided.

24. DELETION OF USER DATA

24.1. Upon termination, you will lose access to any User Data and it will be deleted, subject to clauses 23.2 and 23.3 below.

24.2. 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.

24.3. 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.

24.4. Upon termination of the Agreement, the Provider will delete the User Account. The provisions of clause 23.3 above shall apply accordingly.

25. CONTRACTS CONCLUDED WITH NATURAL PERSONS

25.1. The User acknowledges that the Provider's intention is to apply these Terms of Service only to professional services provided to entities that are not consumers. Therefore, by concluding this Agreement, the User who is a natural person confirms that the subject matter of the Agreement is entirely directly related to the business activity conducted by the User and has a professional character for the User, resulting in particular from the subject of the business or professional activity performed by the User. In particular, the User acknowledges that the Services will be used directly in connection with his/her business or professional activity (e.g. to operate/support the User's key processes related to such activity).

25.2. The subject matter of the Agreement is understood by the Parties as all the Services used or will be used by the User.

25.3. In cases where the subject matter of the Agreement does not correspond to the statement referred to in clause 25.1, the User is obliged to inform the Provider about this fact before concluding the Agreement or at the latest before the commencement of the provision of Services.

25.4. The Parties agree to exclude the Provider's liability resulting from the User's breach of the obligations referred to in clause 25.1 or 25.3 above. The User is obliged to repair in full the damage caused as a result of concluding the Agreement inconsistent with the statement in clause 25.1, and where possible, indemnify the Provider from liability.

25.5. In the event of a breach of clause 25.1 or 25.3 by the User, the Agreement shall be interpreted as meaning that the intention of the Parties is that the cooperation between the Parties in its entirety proceeds as if the User's statement in clause 25.1 were true. Section 28.3 shall apply mutatis mutandis.

26. FINAL PROVISIONS

26.1. The applicable law for the Agreement is the Polish law. To the extent that it is permitted, the application of provisions of international law and provisions of foreign law which, according to the relevant Terms of Service, would be appropriate in the absence of the choice of law, is expressly excluded. In the event that international or foreign law is to apply to the Agreement in an absolute manner, the User is obliged to inform the Service Provider of this fact before concluding the Agreement, and in the event of the entry into force of Terms of Service forcing the application of international or foreign law to the Agreement during the term of the Agreement, immediately after the adoption of such Terms of Service by the competent authority. In the event of failure to inform the Provider before the conclusion of the Agreement about the need to apply international or foreign law to the Agreement, as well as in the event of any change in Terms of Service during the term of the Agreement resulting in the need to apply foreign or international law to the Agreement, the Provider has the right to terminate the Agreement with immediate effect.

26.2. Disputes that may arise from the application of the Agreement are settled amicably by the Parties within thirty (30) days from the date of the dispute. In the event of disagreement, the Parties shall submit the dispute for resolution to the court competent for the Provider's registered office. Matters arising out of or in connection with the Agreement shall always be subject to the jurisdiction of the Polish courts.

26.3. 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 purpose assumed by the Parties will apply.

26.4. In the event of any discrepancies between the English and Polish versions of the Terms of Service, the provisions of the Polish version shall prevail.

26.5. 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 a given 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 and, unless otherwise provided for in the Agreement concluded with the User, shall govern the entire relationship between the Parties.

List of appendieces:

1. Data Processing Agreement

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 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: **ON BEHALF OF CUSTOMER:**

________________________________ **Olha Yuzbekova** ________________________________ **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.