OKTAWAVE

Rev. 20231214

Appendix no. 3 to the Terms of Service

Data Processing Agreement

("**this Processing Agreement**")

Definitions

Controller	Controller of the Personal Data entrusted to Oktawave, determining the purposes and means of processing of Personal Data;
Legal Acts	Legislation applicable to Oktawave 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 Oktawave processes Personal Data defined in the Processing Agreement;
Principal Agreement	Service agreement that specifically stipulates services consisting of providing the User 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 Oktawave subcontracts Personal Data processing to a third party that will be obliged to process the Personal Data in accordance with this Processing Agreement and Oktawave 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 User processes information constituting Personal Data,*
2) *The User has entered into the Principal Agreement with Oktawave;*
3) *Data transferred by the User to Oktawave 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 User subcontracts processing of Personal Data to Oktawave in the scope specified in this Processing Agreement, and Oktawave undertakes to process them in accordance with this Processing Agreement.
2. Oktawave 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 User represents that, subject to section 2 below, it is the Controller.
2. In each case when Personal Data include any data of which the User is not the Controller, the User 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 User is authorised to transfer such Personal Data onward to Oktawave on the terms determined in this Processing Agreement.

3. The User will, at the request of Oktawave 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 Oktawave 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 User declares that Personal Data provided to Oktawave for processing have been obtained lawfully and their processing and further processing by Oktawave is not in breach of any law or third party rights.
5. Oktawave 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. Oktawave 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 Oktawave and established in Poland apply to Oktawave in relation to entering into this Processing Agreement considering the nature of the Personal Data or special status of the User, the User will notify Oktawave about that fact in writing (other forms of notifications will not be valid), at least 30 days in advance, and Oktawave 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 Oktawave, the type of Personal Data and categories of data subjects are determined and controlled by the User. Depending on the case, Personal Data entrusted to Oktawave 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 Oktawave with its clients. Depending on the case, Personal Data processed by Oktawave 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 Oktawave may include, without limitation:
   a. Storage of the Personal Data in the technical infrastructure /Cloud service equipment provided by Oktawave, and also ensuring the use of computing power of that equipment for the processing of Personal Data by the User in a manner chosen by the User, 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 (e.g. encrypted data transmission, use of advanced communication protocols, multi-step authentication);
   d. Ensuring access to the Services, in accordance with the Principal Agreement (including the SLA), which also includes monitoring of the traffic from and to the Cloud (at the Cloud level) to identify and protect against activities such as DDOS attacks and to ensure Cloud operation stability;
   e. Provision of technical support for the User's virtual machine – only when technical assistance is used, in accordance with section 6(a) below;
   f. User's Services management for the virtual machines designated by the User – only when Cloud Operations service is used, in accordance with section 6(b) below.

3. For the avoidance of doubt, without prejudice to sections 5-6 below, the User independently administers the virtual machines where the Personal Data are processed, among other things independently installs software selected by the User, implements safeguards, makes back-up copies, and performs other obligations under the Legal Acts.
4. The User may order Oktawave to make and maintain back-up copies of User's Data, which will include making back-up copy of the whole "virtual machine" of the User, on the principles agreed in detail for such additional Service.
5. The User may provide to Oktawave access to its virtual machines (in the scope determined by the User and with the application of suitable safeguards selected by the User) by:
   a. The creation of administrative account on the virtual machine for a person acting on behalf of Oktawave to perform specific ad hoc operation; or
   b. The use of Cloud Operations service.

   In such case the User will provide to Oktawave instructions on the scope of operations that may be performed by Oktawave's designees, in electronic form, and Oktawave, in addition to the obligations specified in Article 4 below, will be obliged also to exercise due care, to the extent possible for Oktawave, to ensure accountability for the actions of those persons in the User'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 Oktawave for the purpose of the provision to the User 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. Oktawave undertakes to:
   a. Process the Personal Data only on documented instructions from the User – 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, Oktawave will notify the User 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 Oktawave 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 5 and 6 below;
   e. Insofar as this is possible and in the scope justified by the nature of the processing activities, to assist the User 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 User 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 Oktawave, to the extent required by law;
   g. At the choice of the User, delete or return all the Personal Data to the User, 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 User information necessary to demonstrate compliance with Oktawave obligations specified in this section, within the limits justified by the nature of the processing activities;
i. Allow audits and inspections conducted by the User in accordance with Article 5 below.

3. Oktawave declares that at the date of this Agreement it processes Personal Data exclusively in the Republic of Poland. Places of Processing may be located exclusively in the territory of the Republic of Poland or the European Economic Area.
4. Oktawave may contract Sub-processing of Personal Data exclusively on the rules defined herein. Oktawave will notify the User 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 User, 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 Oktawave as a reply email to be valid. Should Oktawave receive the objection, it will be entitled to submit a notice of termination of this Processing Agreement to the User within the next 5 days, with 14 days' notice period. If no objections arise within the specified timeframe, Oktawave may proceed with the sub-entrustment.
5. The User hereby agrees to the Sub-processing of the Personal Data by ATM S.A. with its registered office in Warsaw, ul. Grochowska 21a, 04-186 Warszawa, tel. 22 51 56 100, info@atman.pl, by POLCOM S.A. with its registered office in Skawina, ul. Krakowska 43 (32-050) and by Netia S.A. with its registered office in Warsaw ul. Poleczki 13, in relation to the activities specified in Article 3(3)(b) above.
6. The User 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, Oktawave undertakes to also apply special security measures other than those described in Article 4 of this Processing Agreement, if they are available to Oktawave and commercially and economically reasonable from the point of view of Oktawave, within 21 business days of receipt of the User's request provided in the form of an email.
7. The User will be obliged to apply appropriate cryptographic (encryption) techniques for all Personal Data at the stage of their transfer to/from Oktawave infrastructure and at the stage of their storage within Oktawave 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. Oktawave will not be liable for any effect of the violation of the above obligations by the User. Under separate agreement between the Parties, it is possible for Oktawave to provide dedicated Service security solutions as part of the Cloud Operations, including encryption of information and management of encryption keys.
8. 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 User. Subject to Article 3 sections 5 and 6 above, Oktawave 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.
9. In each case of Oktawave finding a breach of Personal Data provided to Oktawave for processing by the User, Oktawave will without undue delay, if possible within 48 hours of discovering the given breach, notify it to the User in the form of an email. Such notification will include the following information known to Oktawave 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 User is entitled independently and the Controllers listed in Annex no. 1 are entitled jointly with the User to control processing of Personal Data by Oktawave under this Processing Agreement through audits or inspections, not more frequent, however, than once every 6 months in total. The User may, at its own expense, order a Control by a professional auditor for whom the User will be responsible. In case of each control, the User will notify Oktawave of the intention to carry out a control, providing at the same time the control plan, at least 14 business days in advance, and Oktawave 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 Oktawave's obligations under the law or contracts entered into with other Controllers and Oktawave's trade secret. When a control could have an adverse effect on the ongoing functioning of Oktawave or any entity to which Oktawave 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 Oktawave 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 User in accordance with section 1 above be impossible for objective reasons (such as concurrent control by another user), Oktawave will immediately notify the User accordingly and the Parties will immediately agree a different possible date for the control.
3. The Parties will draw up a control report. The User 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 User.
5. Oktawave will be obliged to notify the User of any control carried out at Oktawave by authorised government authorities if it is related to the processing of Personal Data provided by the User, 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, Oktawave will be entitled to request the User to evidence the entitlement to onward transfer of Personal Data at any time, and the User will be obligated to deliver to Oktawave 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 User declares that it has ceased processing of Personal Data as part of Services, the User will be entitled to terminate this Processing Agreement with one month's notice period.

Article 7
Personal Data Erasure

1. The User may erase Personal Data processed as part of the Services at any time for example by:
   a. Appropriate overwriting through independently selected software installed and used by the User in the virtual machine and in accordance with the procedure determined by the User – erasure occurs at the time and on the principles determined independently by the User;
   b. Erasure of encrypted virtual machine of the User – in such case data becomes unavailable immediately and are erased within 48 hours.
2. The User will be able to freely export Personal Data throughout the term of this Processing Agreement through:
   a. The export of individual databases / programs created independently by the User and managed by the User, in formats appropriate for such databases / programs (functionalities managed by the User);
   b. The export of a data set that constitute the whole virtual machine of the User, in VMware format (functionality provided by the Service Provider).
3. At the latest by:
   a. Termination of this Processing Agreement or the Principal Agreement;
   b. Depletion of the Tariff Units held by the User (applicable to Pre-Paid Users);

   The User will be obliged to export Personal Data in accordance with section 2 above and make sure that all Personal Data have been erased from the Cloud in accordance with section 1 above and submitted within the deadline will be considered.
4. Regardless of the provisions of section 3 above, Oktawave will, within 14 days of the termination of the Principal Agreement or depletion of Tariff Units held by the User (applicable to Pre-Paid Users), erase User's virtual machines that had not been previously erased by the User, which will cause immediate unavailability of data stored there and their erasure within the subsequent 14 days.
5. Oktawave declares that when the steps described in section 1 above are correctly carried out by the User, Oktawave as of the time determined therein will not hold or process copies of erased Personal Data, which may be acknowledged by Oktawave in the form of an email message at the request of the User during the term of this Processing Agreement or within 30 days of the termination hereof.
6. The Parties may stipulate in the Principal Agreement separate rules of terminating the collaboration other than the above.

Article 8
Liability

1. Oktawave will be liable for damage caused to the User 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 Oktawave's liability for entities Sub-processing Personal Data for Oktawave in accordance with this Processing Agreement.
2. The User 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.

§ 9
Miscellaneous

1. Oktawave 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 Oktawave or an entity Sub-processing Personal Data for Oktawave, provided that they are compliant with the requirements specified in the GDPR. Should the User find the changes made by Oktawave in accordance with the preceding sentence to be non-compliant with the GDPR, the User will notify Oktawave 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 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:

1. Annex no. 1 – TEMPLATE: List of Controllers;
2. Annex no. 2 – Security procedures used by Oktawave S.A.;
3. Annex no. 3 - Description of the organisation and means of safeguarding information resources by sub-contractors.

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)

OKTAWAVE

Annex no. 2 Security procedures

Oktawave has provided services covered by the scope of the Processing Agreement continuously since 2014. Currently, among dozens of entities that have used Oktawave's cloud services, there are clients from such demanding sectors as healthcare or insurance.

Oktawave applies in its operations specifically the following legal, technical and organisational measures to ensure appropriate security level for the services provided by Oktawave:

1. Legal solutions:

    a. Oktawave is a joint-stock company registered in Poland. The sole shareholder of Oktawave is K2 Internet S.A., which is a company listed on the Warsaw Stock Exchange. Oktawave is the owner (100%, sole control) of the whole infrastructure used to provide Services, including servers, storage systems, network, framework and data network switches, and also routers and cables;

    b. All persons acting on behalf of Oktawave in the processing of personal data of which Oktawave is the controller or processor have undertaken to maintain confidentiality of such information and not to use them for any purpose other than related to the performance of their work duties;

    c. Any breach of confidentiality obligation referred to in section (a) above will in general constitute a data protection offence (Article 266 et seq. of the Criminal Code of 6 June 1997) and the persons bound by that obligation have been instructed accordingly;

    d. Oktawave is aware of and is committed to always fully comply with the obligations imposed by relevant laws, including specifically the 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, which also includes ongoing monitoring and consideration to the necessary extent of positions and guidelines issued by competent supervision authorities, such as the European Data Protection Board;

    e.

    f. All agreements subcontracting personal data processing to a third party by Oktawave, where Oktawave acts as the controller or the processor, are compliant with the GDPR and are only concluded with entities that provide sufficient guarantees of the implementation of appropriate technical and organisational measures so the processing is compliant with the GDPR, including also appropriate experience and reputation;

    g. Oktawave holds continuously insurance policy covering computer consultants' professional liability claims with coverage of services provided by Oktawave and actions of Oktawave personnel.

2. Organisational solutions:

    a. Oktawave holds and has implemented specifically the following policies related to the security of personal data processing:

- personal data security policy;
- management instruction for the IT system used to process personal data;
- information security policy compliant with ISO 27001;
- access management policy compliant with ISO 27001.

Extracts from the aforementioned policies (excluding strictly confidential information the disclosure of which could compromise data security) are available to personal data controllers or their designated auditors for review at the Oktawave offices by prior appointment.

b. Oktawave holds current ISO/IEC 27001:2013 Information Security Management System Certificate issued by the British Standards Institution under certificate number IS 630529, and CSA STAR Certificate issued by the British Standards Institution under certificate number STAR 657851. Oktawave also holds ISO/IEC 27017 certificate (security of information in computing cloud) and ISO/IEC 27018 certificate (good practices of personal data protection in computing cloud;

c. As of 14 May 2013, Oktawave has got an Information Security Administrator who became the Data Protection Officer as of the effective date of the GDPR;

d. System/program update procedure is in place – systems are periodically updated in accordance with the adopted schedule. In case of any error/vulnerability that materially affects the environment security, updates are performed immediately, outside the adopted schedule;

e. Back-up copy procedure for the whole Cloud has been implemented, in accordance with the adopted schedule, and the copies are stored on the disk array located on THINX servers. At every back-up, notification is sent in case of back-up failure. Regular recoveries of each type of copies and verification of recovery correctness are performed;

f. Solutions of system hardening are performed in accordance with the adopted principles of best practice, managed through an automatic configuration server;

g. Every member of Oktawave personnel has their own identifier (login + password) and personal SSL certificate used within the organisation. Access for each person and their authorisation level is assigned in accordance with the least privilege policy and exclusively for the purpose of the performance of work duties;

h. All persons acting on behalf of Oktawave participate in regular training on personal data protection and information security;

3. Technical solutions:

a. User authentication data are not stored by Oktawave – Active Directory mechanism is used, and only password hash is stored;

b. All data transferred between Oktawave servers at the Cloud level are transferred in encrypted form (SSL);

c. Configuration of the systems used at the Cloud level is done from central configuration management system, plus the servers have local mechanisms enabling configuration change tracking;

d. Oktawave infrastructure enables the Users to use in their virtual machines all known technological solutions that may support security of the personal data stored, including the options of pseudonymisation or encryption of the data stored, VPN-type solutions, etc. Each User storing personal data in virtual machines is obligated to encrypt those machines (use cryptographic solutions);

e. Access to the internal Oktawave network used to manage the Cloud is based on multi-step authentication, additionally network segmentation is applied where a given internal user has access only to a certain part of the infrastructure;

f. The infrastructure is subject to security tests – mechanisms of automatic vulnerability detection are used, all systems are scanned on an ongoing basis (tests are deployed according to a schedule), in terms of currently published vulnerabilities (CVE). Oktawave also uses services of third parties that perform regular infrastructure security audit (DSS) and immediately implements any recommendations;

g. Functioning of the infrastructure is monitored 24/7/365 to detect any failures – both internal and external automated network monitoring tools are used, and in case of a failure an Oktawave engineer is available 24/7.

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

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

ATM S.A.

In the context of safeguard classification for processes where personal data are processed, ***ATM*** pays special attention to compliance with the General Data Protection Regulation (GDPR), which means continuous monitoring and identification of all resulting legal, supervision, contractual obligations and systemic approach to their observance. Best practices and technologies available for each safeguard category are considered in the selection of safeguards to ensure continuous confidentiality, integrity, availability and resilience of the systems used to process personal data and the processing services. The effectiveness of technical and organisational measures used to ensure security of personal data processing is subject to regular tests, measurement and evaluation.

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.

POLCOM S.A.

Safeguards of personal data processing

1. To secure personal data processing the following organisational safeguards have been implemented:
   a. Only persons who hold personal authorisation to process personal data are allowed to process personal data;
   b. Personal data are processed only in the European Economic Area and cannot be transferred to any country from outside that Area;
   c. The zone in which personal data is processed is secured against access of unauthorized persons during the time of absence of persons authorized to process personal data by locking the entrance to the given zone;
   d. The aforementioned safeguard is implemented through locking a given zone by the last person leaving iton a given day and unlocking it by the first person entering the zone on the given day, and also locking it during the day in case when nobody is present;
   e. Presence of anyone unauthorised to process personal data in the protected area is possible only in the following circumstances:
      - personal authorisation issued by a Member of the Management Board of the Company or the Data Protection Officer or Assistance DPO;
      - in the presence of a person authorised to process personal data;
      - with continuous video surveillance;
   f. Any person who is to be authorised to process personal data will be familiarised with personal data protection laws and internal personal data regulations, and other issues related to personal data protection, before such person is allowed to work with personal data processing;
   g. Authorisation to process personal data is issued individually by a Member of the Management Board of the Company, Data Protection Officer or another person authorised by the Management Board of the Company;
   h. Written personal data processing agreements are signed with entities processing personal data for the Company;
   i. 24/7 physical security of Polcom Data Center: licensed security guards, licensed property security agency, 24/7 incident intervention group.
2. To secure personal data processing the following technical safeguards have been implemented at the Polcom Data Center:
   a. extensive system of access control and anti-theft system;

b. multi-step access control;
c. CCTV system;
d. continuous monitoring of the CCTV;
e. building monitoring system that controls the functioning of all equipment in the data centre;
f. redundant fire-extinguishing system, double set of bottles;
g. separate fire zones of appropriate fire resistance;
h. fire detection based on the early smoke detection system;
i. extinguishing system using a gas neutral for people, equipment and the environment;
j. two underground medium voltage connections;
k. 2N power distribution;
l. backup power generators;
m. UPS;
n. fuel tanks for uninterrupted supply to power generators;
o. extensive system of power parameters monitoring;
p. two independent cooling units;
q. redundant precision air-conditioning system;
r. IT systems and applications for personal data processing are updated on regular basis, verified for attack vulnerability and protected by anti-virus systems;
s. safeguards are used against unauthorised access to the systems and networks with firewall;
t. network traffic monitoring systems are used and any anomalies are logged and reported.

NETIA S.A.

The data centre meets Class 3 certification requirements, according to EN/PN 50600 standard

(European standard covering specific requirements for critical infrastructure and data centre security systems, developed by the European Committee for Electrotechnical Standardisation – CENELEC – approved by the European Commission)

At the same time, the facility has appropriate organisational and technical measures in place to safeguard data, including personal data.

1.The following organisational security measures are in place to protect data processing:

a. Implementing an Access Control System (ACS) to grant access cards to employees and authorised personnel;

b. Establishing detailed internal procedures for granting access to individuals without access cards;

c. Enclosing the entire facility and the adjacent yard with a secure fence;

d. Conducting checks on vehicles entering and leaving the premises;

e. Providing data protection training, including personal data protection, to all staff members, along with regular refresher courses;

f. Requiring all employees and associates to maintain the confidentiality of facility security-related information and to only use such information for their official duties;

g. Prohibiting photography or recording of any elements on site on any media;

h. Entities using the facility may install equipment that:

• is fully operational for use within the territory of the Republic of Poland and has the legal title allowing installation within the facility;

• possesses the necessary legal permits, technical opinions, and expert reports, which must be provided by the facility's operator upon request;

• features durable markings to enable clear identification.

2. The following technical security measures are in place to protect data processing:

a. Precision air-conditioning (N+1 operation) with independent units, each equipped with its own control system; no installations unrelated to server room operation run through these rooms;

b. A 3N/2 power supply system utilising three independent tracks, adhering to the 2N redundancy principle; a single track can be switched off as needed (e.g., for maintenance);

c. UPS (Uninterruptible Power Supply) system and generators, forming a redundant power supply;

d. Emergency backup via the DRUPS system;

e. Two independent power circuits;

f. Dual power connections from the municipal grid;

g. Early smoke detection system;

h. Fire alarm system with signal monitoring connected to the National Fire Service;

i. Fixed fire-fighting equipment;

j. CCTV monitoring;

k. Burglary and robbery alarm system (intrusion alarm system);

l. Facility design based on the integration of technical security systems (including intrusion alarm system, access control and time registration systems, and CCTV monitoring) and physical security measures.

m. A Building Management System (BMS) that consolidates alarms from various detection systems, including water detectors, gas detectors, over-temperature detectors, fire detectors, and power supply detectors.