Appendix No. 1
to order of JSC Apatit
No. 900-U dated
30 December 2021

JSC Apatit's
POLICY
on personal data processing
and information about effective requirements for personal data protection

Cherepovets
2021

PHWMM065900E0KKFZ8Z

1. General provisions

1.1. JSC Apatit's policy on personal data processing and information about effective requirements for personal data protection (the "Policy") sets out the general principles and procedure for personal data processing and measures to ensure the security of personal data at JSC Apatit (the "Company").

The Policy's goal is to protect human and civil rights during personal data processing, including the right to privacy, personal and family secrets, and to ensure strict compliance with applicable Russian laws on personal data.

1.2. The Policy has been developed in pursuance of Federal Law No. 152-FZ On Personal Data dated 27 July 2006, other laws and regulations governing the procedure for personal data management, and personal data security requirements.

1.3. The following terms and definitions shall be used in the Policy:

"**Automated Personal Data Processing**" means personal data processing using computer technology.

"**Biometric Personal Data**" means information about an individual's physiological and biological characteristics that can be used to establish their identity and that are used by the operator to verify the identity of the data subject.

"**Blocking of Personal Data**" means temporary suspension of personal data processing (except where processing is required to rectify personal data).

"**Data Centre**" means a specialised entity that houses server and network equipment, leases out servers (including virtual ones), and provides access to the Internet.

"**Access to Personal Data**" means familiarisation of certain persons (including employees) with personal data of data subjects that are processed on the condition of their confidentiality.

"**Personal Data Information System (PDIS)**" means a collection of personal data stored in databases as well as hardware and software used for the processing thereof.

"**Counterparty**" means a party to a contract with JSC Apatit.

"**Confidentiality of Personal Data**" means the obligation of persons that gained access to personal data not to disclose or disseminate personal data to any third parties without consent of the data subject unless otherwise provided for by applicable laws.

"**Personal Data Anonymisation"** means actions that make it impossible, without the use of additional information, to identify personal data as related to a specific data subject.

"**Personal Data Processing**" means any action (operation) or set of actions (operations) performed with personal data, including collection, recording, systematisation, accumulation, storage, correction (updating, modification), extraction, use, transfer (distribution, provision, access), anonymisation, blocking, deletion, destruction of personal data, with or without means of automation;

"**Publicly Available Personal Data**" means personal data made accessible to members of the general public under applicable laws either by the data subject or at the request of the data subject, including data that are required to be disclosed or made available.

"**Operator**" means a state or municipal authority, legal entity or individual that processes personal data or organises such processing, whether independently or jointly with other persons, and defines the purposes of personal data processing, the scope of personal data to be processed, and the actions (operations) performed on personal data.

"**Personal Data (PD)**" means any information relating directly or indirectly to an identified or identifiable individual (personal data subject, or PD subject).

"**Provision of Personal Data**" means actions aimed at disclosing personal data to third party or a group of third parties.

"**Dissemination of Personal Data**" means actions aimed at disclosing personal data to an indefinite number of third parties.

"**Personal Data Subject**" means an individual that personal data refer to.

"**Cross-Border Personal Data Transfer**" means personal data transfer to a foreign state

authority, a foreign individual or legal entity.

"**Personal Data Destruction**" means any actions that make it impossible to recover personal data in a personal data information system and/or that result in physical destruction of media containing personal data.

2. General requirements to personal data processing

2.1. **The Company's status and categories of data subjects whose personal data are processed by the Company**

2.1.1. The Company is a PD Operator in in relation to the PD of the following individuals:

2.1.1.1. The Company's Employees that signed employment contracts, including those whose employments contracts have already been terminated (the "Employees");

2.1.1.2. Individuals that carry out work for the Company under civil law contracts, including those whose civil law contracts have already been terminated (the "Contractors");

2.1.1.3. Close relatives of the Company's Employees whose PD are required to be processed by applicable laws and are also processed by the Company (as the employer) in accordance with statutory requirements of state statistic agencies (the "Employee Relatives");

2.1.1.4. The Company's shareholders who are individuals and whose PD are processed by the Company under applicable laws on joint-stock companies, anti-trust laws, laws on state registration of legal entities, and laws on securities market (the "Shareholders");

2.1.1.5. The Company's affiliates whose PD are processed under applicable laws on securities market and anti-trust laws (the "Affiliates");

2.1.1.6. Applicants for the Company's job vacancies (potential new hires) that have provided their CVs or questionnaires directly or via recruitment agencies or dedicated job search websites, including participants of the programme to attract talented graduates and applicants for an internship with the Company (the "Applicants");

2.1.1.7. Representatives of the Company's counterparties provided that such counterparties have valid contracts signed with the Company, the Company intends to enter into contracts with such counterparties or such counterparties intend to enter into contracts with the Company (the "Counterparty Representatives");

2.1.1.8. Representatives of PD subjects who are not the Company's Employees provided that such representatives contact the Company on behalf of and for the account of PD subjects (the "Subject Representatives");

2.1.1.9. Visitors to any guarded premises of the Company, its branches or standalone business units provided that such visitors must apply for a single-use pass to access such guarded premises (the "Visitors").

2.1.2. The Company acts as an entity that processes PD for the account of other operators, including but not limited to:

2.1.2.1. Military commissariats and trade unions that PD shall be provided (transferred) to in cases provided for by applicable laws;

2.1.2.2. Companies that are part of the group to which JSC Apatit belongs and with respect to the Employees of which (the "**Employees of Other JSC Apatit Group Companies**") the Company carries out personnel record keeping and accounting, renders services to provide access to information systems that such companies' Employees use, arranges for the operation of a system to control and manage access to guarded premises, ensures the operation of a single telephone directory of companies that are part of the group to which JSC Apatit belongs, and carries out other actions concerning their PD as per agreements signed by the Company and such companies and/or as per internal regulations of the companies that are part of the group to which JSC Apatit belongs.

The extent of PD provided (transferred) to government authorities, state non-budget funds, military commissariats and trade unions shall be set out by applicable laws, respective government authorities or state non-budget funds as per their remit. No specific consent of PD subjects is

required for such PD transfer to take place.

Companies that are part of the group to which JSC Apatit belongs obtain written consent to have PD of their employees transferred to the Company for subsequent processing. The Company itself obtains no such consents and provides no information on such processing before it starts processing the PD of Employees of Other JSC Apatit Group Companies on the assumption that such consent was obtained and information was provided by their respective employers.

2.2. **Principles and terms of personal data processing**

The Company processes PD in accordance with the following principles and objectives:

2.2.1. Lawful and fair basis of PD processing: The Company takes all the necessary steps to ensure compliance with applicable laws, does not process PD in cases when it is not allowed by applicable laws, and does not use PD to the detriment of PD subjects.

2.2.2. PD processing is limited by the achievement of specific, predetermined and lawful purposes. The objectives of PD processing by the Company are as follows:

2.2.2.1. Relating to Employees: compliance with laws and regulations, contribution to Employees' recruitment, education and promotion, ensuring their personal safety, oversight over the amount and quality of their work, safekeeping respective property and information, calculation and payment of salaries, wages and other types of remuneration, calculation and payment of taxes and insurance contributions, and compliance with statutory requirements of state statistic agencies;

2.2.2.2. Relating to Contractors: compliance with requirements of the Russian Civil Code as regards contractual relations, and fulfilment of obligations under contracts signed with Contractors;

2.2.2.3. Relating to Employee Relatives: provision to Employees of benefits and guarantees stipulated by federal laws for parents or adoptive parents and people with family obligations; compliance with statutory requirements of state statistic agencies;

2.2.2.4. Relating to Shareholders: maintaining a register of shareholders;

2.2.2.5. Relating to Affiliates: keeping records of the Company's affiliates and preparing lists of affiliates;

2.2.2.6. Relating to Applicants: decision making on potential filling of job vacancies with Applicants that best meet the Company's requirements; attracting talented graduates and applicants to complete internships with the Company;

2.2.2.7. Relating to Counterparty Representatives: compliance with requirements of the Russian Civil Code as regards contractual relations, and fulfilment of obligations under contracts signed with Counterparties;

2.2.2.8. Relating to Subject Representatives: performing actions by the Company on behalf of Subject Representatives;

2.2.2.9. Relating to Visitors: providing access to the territory of the Company, its branches, standalone units and guarded premises to persons who have no permanent passes;

2.2.2.10. relating to Employees of Other JSC Apatit Group Companies: executing instructions of companies that are part of the group to which JSC Apatit belongs regarding their Employees' PD processing for the purposes of personnel record keeping and accounting, services to provide access to information systems that such companies' Employees use, the operation of a system to control and manage access to guarded premises, operation of a single telephone directory of such companies, and performing other actions concerning their PD as per agreements signed by the Company and such companies and/or as per internal regulations of the companies that are part of the group to which JSC Apatit belongs.

2.2.3. Processing only of PD that are compatible with the stated processing purposes. Consistency of processed PD content and scope with the stated purposes of processing. Preventing the processing of PD that is incompatible with the purposes of PD collection or excessive with respect to the stated purposes of PD processing. The Company does not collect or process PD that are not required for the purposes stated in clause 2.2 hereof, nor does it use PD of PD subjects for any purposes other than those stated above.

2.2.4. Preventing of integration of databases that contain PD intended for incompatible processing purposes.

2.2.5. Accuracy, sufficiency and up-to-date status of PD in accordance with PD processing purposes. The Company takes all reasonable measures to make sure the processed PD are up-to-date, including but not limited to by exercising the right of every PD subject to obtain their PD for familiarisation and to request that the Company update, block or destroy their PD should they be incomplete, out-of-date, have been obtained illegally or are not necessary for the processing purposes stated above.

2.2.6. Keeping PD in a form which permits identification of the PD subject for no longer than is necessary for PD processing purposes unless the retention period is provided for by applicable laws or a contract to which the PD subject is a party.

2.2.7. Destruction or anonymisation of PD after achieving their processing purposes or after such purposes have become irrelevant or if the Company is unable to rectify its violations of the statutory procedure for PD processing or the PD subject's revocation of its consent to PD processing, unless otherwise provided for by applicable laws or contracts entered into with the PD subject.

2.3. **Conditions of personal data processing**

2.3.1. The Company may process PD on the following conditions:

2.3.1.1. The PD subject has provided consent to their PD processing. The procedure for the Company to obtain consent of a PD subject is set out in section 2.5 hereof;

2.3.1.2. PD processing is necessary for the Company to exercise its functions or powers and performance of obligations provided for by applicable laws. This includes but is not limited to processing of special categories of PD of Employees and Employees of Other JSC Apatit Group Companies for purposes set out in applicable laws.

2.3.1.3. PD processing is necessary for the execution of a contract to which the PD subject is a party, or for the signing of a contract at the request of the PD subject. Such contracts include but are not limited to employment contracts with the Company's Employees and civil law contracts with Contractors; precontractual efforts include recruitment efforts, with the PD subject's consent to PD processing confirmed with a questionnaire filled in by the Applicant by hand or with a questionnaire (CV) handed over to the Company, transferred to an HR agency, posted on dedicated websites in the Internet or sent by the Applicant to the Company by email.

2.3.1.4. PD processing is required for the exercise of rights and legitimate interests of the Company or third parties, or for any public purpose provided that no rights or freedoms of PD subjects are affected.

2.3.1.5. PD are processed for statistical or other research purposes provided they are anonymised at all times;

2.3.1.6. Access to the PD has been granted to the general public by the PD subject or at their request;

2.3.2. The Company does not disclose PD to third parties or disseminate PD without the PD subject's consent unless otherwise provided for by applicable laws.

2.3.3. The Company does not process PD relating to and associated with race, ethnicity, political views, religious or philosophical beliefs, health status (except for matters relating to the Employee's ability to perform their job duties and the Contractor's ability to perform their obligations under respective contract), intimate life or memberships of Employees or Contractors with public or trade union associations unless otherwise expressly required by applicable laws.

2.3.4. The Company may process PD on a person's criminal record only as and when required by applicable laws.

2.3.5. Where PD must be transferred outside of the Russian Federation, such transfer shall be in accordance with applicable Russian laws. Prior to the commencement of any cross-border transfer of PD, the Company shall make sure that the foreign country to which the PD will be transferred provides adequate protection of the rights of PD subjects. Cross-border PD transfer to foreign countries without adequate protection of rights of PD subjects may take place in the

following cases:

- the PD subject has given their written consent to such transfer;
- such transfer is required under international treaties and applicable Russian laws;
- such transfer is required for the execution of a contract to which the PD subject is a party;
- such transfer is required for the protection of the life, health, or any other essential interests of the PD subject or other persons if the PD subject's written consent may not be obtained.

2.4. **Confidentiality of personal data**

The Company's Employees that have obtained access to PD shall treat such PD as confidential. PD that have been anonymised do not need to be treated as confidential.

2.4.1. Provided that the PD subject has consented to it and unless otherwise envisaged by law, the Company may instruct another entity/person to process the subject's PD under a contract with such entity/person, the material terms of which include the obligation of such entity's/person's to comply with PD processing principles and rules when processing PD at the Company's instruction as required by law. The volume of PD transferred to another entity/person for processing and the number of processing ways used by such entity/person shall be limited to the minimum necessary to perform their obligations to the Company. The Company's instruction shall detail the list of actions (operations) with PD to be performed by the entity/person processing the PD, and processing purposes, along with the entity's/person's obligation to treat PD as confidential and keep them secure during processing, as well as requirements to PD protection in line with article 19 of Federal Law No. 152-FZ On Personal Data dated 27 July 2006.

2.4.2. The Company may host its PDIS at a data centre owned by another entity/person provided that a contract has been signed with such data centre and an instruction has been given for PD processing.

2.4.3. If the Company assigns PD processing to another entity/person, the Company shall be responsible to the PD subject for the actions taken by such entity/person. The entity/person that processes PD on behalf of the Company shall be responsible to the Company.

2.5. **Personal data subject's consent to their PD processing**

2.5.1. The PD subject shall decide on the provision of their PD to the Company and give consent to their processing acting freely, independently, and in their own interest. Consent to PD processing shall be specific, informed and conscious and can be provided by the PD subject in any verifiable form, unless otherwise provided for by applicable laws.

2.5.2. If consent to PD processing has been given by a Subject Representative, the Company shall check the powers of such representative to give consent on behalf of the PD subject.

2.5.3. If the Company receives PD from a counterparty on the basis of a valid contract, the counterparty providing such PD shall be responsible for the PD validity and reliability and for obtaining consent of PD subjects (or their representatives) for the transfer of their PD to the Company.

2.5.4. The Company that received PD from a counterparty assumes no obligation to inform PD subjects (representatives) whose PD were transferred to the Company about the start date of the PD processing on the assumption that the PD subjects (representatives) were informed accordingly by the counterparty that provided their PD to the Company when entering into a contract with the PD subject and/or when obtaining their consent to such transfer. This obligation of the counterparty shall be included in their contract with the Company.

2.5.5. Employees are not required to give their consent to the processing of their PD by the Company for the purposes of compliance with applicable labour laws. All other cases that involve processing of an Employee's PD aligned with the Company's stated purposes require obtaining such consent.

2.5.6. No consent is required to be given by a Contractor to process their PD as such processing is required for the execution of a civil law contract to which such Contractor, which is

a PD subject, is a party, except for cases where a Contractor's consent is required to be given in writing for specific purposes of PD processing.

2.5.7. No specific consent is required to be given by Employees' spouses if their PD are processed under applicable federal laws (for purposes of child support, social payments, benefits and guarantees, etc.) or are processed by the Company as an employer in accordance with statutory requirements of state statistic agencies.

2.5.8. No specific consent is required to be given by Applicants to process their PD as such processing is required for the purposes of signing an employment contract at the request of such Applicant, who is a PD subject, except for cases where an Applicant's consent is required to be given in writing for specific purposes of PD processing.

2.5.9. For entities/persons entering into contracts with the Company, PD contained in unified state registries of legal entities and sole traders shall be open and publicly available, except for information on the number, issue date and authority issuing the person's identity document.

2.5.10. A Subject Representative's consent to the subject's PD processing shall be given through a course of conduct in the form of issuing a power of attorney to act in the name and on behalf of the PD subject and their identity document.

2.5.11. Visitors' consent to their PD processing shall be given through a course of conduct in the form of either provision of their PD required for access to the Company's guarded premises or in the form of transfer of their identity document to security officers.

2.5.12. No consent from a subject to their PD provision is required when the Company receives, in line with respective scope of authority, reasoned requests from prosecution bodies, law enforcement agencies, inquiry and pre-trial investigation authorities, security agencies, state labour inspectors as part of state control and oversight over compliance with labour laws, or other bodies authorised to request information in line with their powers and authorities as prescribed by applicable laws.

A reasoned request shall include its purpose, reference to the legal grounds, including those confirming the requesting body's powers and authorities, and list of information so requested.

2.5.13. In all cases the Company shall be responsible for providing evidence that the PD subject has consented to their PD processing or evidence stipulated by Federal Law No. 152-FZ On Personal Data dated 27 July 2006.

3. Rights of personal data subjects

3.1. A PD subject has the right to obtain information relating to their PD processing. A PD subject may request the Company to update, block or destroy their PD if such data are incomplete, out-of-date, inaccurate or unreliable, or have been obtained illegally, or are not necessary for the stated purposes of processing, as well as take any lawful measures to protect their rights.

3.2. If a PD subject believes that the Company processes their PD in violation of applicable laws or infringes on their rights and freedoms in any other way, the PD subject may file a complaint against the Company's act or omission to a competent authority for PD subjects' rights protection (the Russian Federal Service for Supervision of Communications, Information Technology, and Mass Media) or seek remedy through courts.

3.3. A PD subject has the right to protect their rights and legal interests, including right to compensation of losses and/or moral damages in court.

3.4. If the provision of personal data is mandatory under a federal law, the operator shall inform the personal data subject of the legal consequences of a refusal to provide their personal data.

4. Information about effective requirements for personal data protection

4.1. The protection of PD processed by the Company shall be ensured by regulatory, organisational and technical measures required and necessary for compliance with applicable laws on the protection of PD.

4.2. Regulatory measures include:

4.2.1. Development of the Company's internal regulations in pursuance of statutory requirements, including the Company's Policy on PD Processing;

4.2.2. Refraining from any ways of PD processing not aligned with purposes defined by the Company in advance.

4.3. Organisational measures include:

4.3.1. Appointment of a person responsible for organising PD processing;

4.3.2. Appointment of a person responsible for ensuring PD security in the PDIS;

4.3.3. Limiting the list of the Company's Employees who have access to PD, and organising a system of permits to grant such access;

4.3.4. Making the Company's Employees directly engaged in PD processing aware of the provision of laws on PD, including requirements for PD protection, this Policy, and the Company's other internal regulations on PD processing;

4.3.5. Training all categories of Employees directly engaged in PD processing how to process them correctly and ensure their security;

4.3.6. Including in job descriptions of the Company's Employees obligations to ensure the security of PD processing and liability for any violations;

4.3.7. Regulating procedures for PD processing;

4.3.8. Keeping records of media containing PD and storing them so as to prevent theft, fraudulent misrepresentation, unauthorised copying, or destruction;

4.3.9. Identifying types of threats to PD relevant to the PDIS based on assessment of potential damage to PD subjects that can result from violations of security requirements, and defining the PD protection level;

4.3.10. Identifying threats to PD during their processing in the PDIS and developing on this basis a model (models) of threats to PD;

4.3.11. Hosting technical means of PD processing within guarded premises;

4.3.12. Limiting the access of third parties to the Company's premises and preventing their access to premises where PD are processed and technical means of their processing are located unless such third parties are supervised by the Company's Employees.

4.4. Technical measures include:

4.4.1. Implementation of requirements to PD protection during their processing in the PDIS provided that such requirements ensure specified levels of PD protection;

4.4.2. Based on a model of threats, development of a PD protection system for levels of PD protection established by the Russian government for PD processing in information systems;

4.4.3. Reliance on data protection tools that have undergone conformity assessment to neutralise relevant threats;

4.4.4. Assessment of effectiveness of measures in place to ensure the security of PD;

4.4.5. Implementation of a system of permits to provide employees with access to PD processed in the PDIS and to hardware and software data protection tools;

4.4.6. Registration and keeping records of PDIS users' actions involving PD;

4.4.7. Detection of malware (by using antivirus software) at all parts of the Company's information systems provided that relevant technical capabilities are in place;

4.4.8. Secure internetworking (using firewalls);

4.4.9. Detection of intrusions into the Company's information systems that violate, or may cause violation of, relevant requirements for PD security;

4.4.10. Encryption of PD transmitted via insecure channels, including via the Internet;

4.4.11. Recovery of PD modified or destroyed as a result of unauthorised access to them (using a PD backup and recovery system);

4.4.12. Monitoring of users' actions from time to time and investigation of any cases of violations of PD security requirements;

4.4.13. Control over compliance with these requirements (using the Company's internal resources or by contracting legal entities or sole traders licensed to engage in activities to provide

technical protection of confidential information) at least once every three years.

5. Final provisions

5.1. Other rights and obligations of the Company as a PD operator and entity that arranges for PD processing at the request of other operators shall be set out by Russian laws on personal data.

5.2. The Company's officers and employees who have violated provisions on PD processing and protection shall be subject to financial sanctions, disciplinary action, or administrative, civil or criminal liability as per applicable laws.