POLICY
personal data processing

The legal basis for this Policy is the Federal Law No. 152-FZ dated 27.07.2006 “On Personal Data” and laws, orders, regulations, and other legislative documents adopted in accordance with the current Russian legislation.

The Policy is developed in order to implement the legal requirements in the field of personal data processing and protection by eastconsult Limited Liability Company (hereinafter - the Company, the Operator).

The Policy provisions shall apply only to the extent not contradicting the applicable Russian legislation.

ARTICLE 1: TERMS AND DEFINITIONS

1.1. Personal data is any information relating a directly or indirectly to a defined or an identifiable individual (personal data subject);

1.2. Operator is a state body, municipal body, legal entity or individual, independently or jointly with other persons, arranging and (or) performing the personal data processing, as well as determining the personal data processing purposes and personal data content;

1.3. Processing of personal data is any action (operation) or a set of actions (operations) performed with or without the use of automation tools with personal data, including collection, recording, systematization, accumulation, storage, clarification (update, change), extraction, use, transfer (distribution, provision, access), depersonalization, blocking, removal, destruction of personal data;

1.4. Automated personal data processing is personal data processing using computer equipment;

1.5. Distribution of personal data is any action aimed at disclosure of personal data to an indefinite number of persons;

1.6. Provision of personal data is any action aimed at personal data disclosure to a certain person or a certain range of persons;

1.7. Blocking of personal data is temporary termination of personal data processing (except for cases when processing is necessary for personal data clarification);

1.8. Destruction of personal data is any action, as a result of which it becomes impossible to restore the personal data content in the personal data information system and (or) as a result of which material personal data media is destroyed;

1.9. Depersonalization of personal data is any action, as a result of which it becomes impossible, without the use of additional information, to determine the personal data identity of a particular subject of personal data;

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Web : www.eastconsult.eu

1.10. Personal data information system is a set of personal data contained in personal data bases and providing information technologies and technical means for their processing;

1.11. Cross-border transfer of personal data is personal data transfer to the foreign country to a foreign authority, a foreign individual, or a foreign legal entity.

ARTICLE 2: PERSONAL DATA PROCESSING

2.1. The Company is an operator of personal data. The Company notified the Roskomnadzor Department in accordance with art. of the Russian Federation Law on Personal Data Protection.

2.2. The subjects of information relations when ensuring the security of the Company's personal data are:

2.2.1. Company, as the information resources owner;

2.2.2. Founders, participants, managers and employees of the Company, in accordance with their functions;

2.2.3. Persons entering into civil law relations with the Company;

2.2.4. Other persons who provide their personal data.

2.3. Personal data processing is allowed in the following cases:

2.3.1. personal data processing shall be carried out with the personal data subject's consent on his/her personal data processing;

2.3.2. personal data processing is necessary to achieve the purposes set by an international treaty of the Russian Federation or by law, to perform and fulfill the functions, powers and obligations imposed on the operator by Russian legislation;

2.3.3. personal data processing is necessary for administration of justice, enforcement of a judicial act, act of another body or official subject to enforcement in accordance with the Russian legislation on enforcement proceedings (hereinafter - the enforcement of a judicial act);

2.3.4. personal data processing is necessary to perform the powers of federal executive authorities, state non-budgetary funds, executive authorities of constituent entities of the Russian Federation, local authorities, and functions of Companies involved in providing respectively state and municipal services provided by Federal Law No. 210-FZ dated July 27, 2010 "On Company of Provision of State and Municipal Services", including registration of the personal data subject on the unified portal of state and municipal services and (or) regional portals of state and municipal services;

2.3.5. personal data processing is necessary for the contract realization, which party or beneficiary or guarantor under which the personal data subject is, as well as for the contract conclusion at the personal data subject's initiative or the contract, under which the personal data subject will be a beneficiary or guarantor;

2.3.6. personal data processing is necessary to protect the life, health or other vital interests of the personal data subject, if obtaining the consent of the personal data subject is impossible;

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Internet : www.eastconsult.eu

2.3.7. personal data processing is necessary for realization of the rights and legitimate interests of the operator or third parties, including in cases stipulated by the Federal Law “On Protection of Rights and Legitimate Interests of Individuals in Debt Collection Activities and on Amendments to the Federal Law “On Microfinance Activities and Microfinance Companies”, or for achievement of socially significant purposes, provided that the rights and freedoms of the personal data subject are not violated thereby;

2.3.8. personal data processing is necessary for the professional activities of a journalist and (or) the legitimate activities of the mass media or scientific, literary or other creative activities, provided that the subject’s rights and legitimate interests are not violated thereby;

2.3.9. personal data processing shall be carried out for statistical or other research purposes, except for the purposes specified in article 15 of the Federal Law, subject to mandatory depersonalization of personal data;

2.3.10. personal data shall be processed, if access to such data is provided to an unlimited number of persons by the subject of personal data or at his request (hereinafter - personal data made publicly available by the personal data subject);

2.3.11. personal data shall be processed if it is subject to publication or compulsory disclosure in accordance with federal laws.

2.4. Processing of specific personal data categories relating to health conditions is not allowed, except if:

2.4.1. personal data subject has provided a written consent to his personal data processing;

2.4.2. personal data is made publicly available by the personal data subject;

2.4.3. personal data processing is necessary to protect the life, health or other vital interests of the personal data subject or the life, health or other vital interests of others and obtaining the consent of the personal data subject is impossible;

2.4.4. personal data is processed for medical and preventive purposes, for purposes of establishing a medical diagnosis, providing medical and medical and social services, provided that processing of personal data is performed by a person professionally engaged in medical activities and obliged to maintain medical secrecy in accordance with the Russian legislation;

2.4.5. personal data processing of members (participants) of a public association or religious Company shall be carried out by the relevant public association or religious Company, acting in accordance with the Russian legislation, to achieve lawful purposes provided for in their constituent documents, provided that personal data shall not be distributed without the personal data subjects’ written consent;

2.4.6. personal data processing is necessary to establish or realize the personal data subject’s or third parties’ rights, as well as in connection with the administration of justice;

2.4.7. personal data processing shall be carried out in accordance with the Russian legislation on protection, on security, on counter-terrorism, on transport security, on anti-corruption, on operational and investigative activities, on enforcement proceedings, on criminal enforcement legislation of the Russian Federation;

2.4.8. personal data received in the cases established by the Russian legislation shall be processed by the prosecution authorities in connection with their prosecutorial supervision;

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Internet : www.eastconsult.eu

2.4.9. personal data processing is carried out in accordance with the legislation on compulsory types of insurance, with the insurance legislation;

2.4.10. personal data is processed in cases stipulated by the Russian legislation, by state authorities, municipal authorities or Companies for the purpose of providing placement for children without parental care in citizens' foster families;

2.4.11. personal data processing is carried out in accordance with the Russian legislation on Russian citizenship.

2.5. List of personal data which the Company is authorized to process: surname, name, patronymic, date and place of birth; biographical information; educational information (educational institution, time of training, qualification awarded); information about workplaces (city, Company name, position, working hours); information about family status, children (name, patronymic, date of birth); information about registration, residence; contact information (e-mail address, telephone numbers); information about tax registration (TIN); information about the registration of tax authorities (tax registration number). Special categories of personal data: race, nationality, political views, religious or philosophical beliefs, health, criminal record. Biometric personal data: image data of a person, including a personal photograph for use in personal files, for internal electronic systems, registration of plastic cards; data on fingerprints of the employee for reading and comparison for the purposes of access control and working time registration.

2.6. The Company has the right to collect, record, systematize, accumulate, store, update, change, use, distribute, depersonalize, block, destroy and transfer personal data to third parties in the order established by applicable legislation.

2.7. Principles of personal data processing:

2.7.1. legitimate basis for personal data processing, legitimate methods of personal data processing;

2.7.2. limiting the personal data processing by achieving predetermined and legitimate purposes;

2.7.3. preventing merging of databases containing personal data, processing of which is incompatible with each other;

2.7.4. processing only those personal data that meet the purposes of processing;

2.7.5. compliance of the content and range of processed personal data with the purposes of processing, prevention of excessive personal data in relation to the stated purposes;

2.7.6. providing the personal data accuracy, sufficiency and relevance in relation to the purposes of personal data processing;

2.7.7. providing necessary actions to remove or clarify incomplete or inaccurate data;

2.7.8. personal data storage in a form that allows to identify the personal data subject.

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Internet : www.eastconsult.eu

ARTICLE 3: PERSONAL DATA PROCESSING CONSENT

3.1. The personal data subject decides to provide his personal data and provides consent to its processing freely, at his own will, and in his own interest. Personal data processing consent shall be specific, informed, and conscientious.

3.2. Personal data processing consent, authorized by the personal data subject for distribution, shall be made separately from other personal data subject consents.

3.3. Personal data processing consent may be withdrawn by the personal data subject.

3.4. Personal data subject's written consent to personal data processing shall include:

3.4.1. surname, first name, patronymic, address of the personal data subject, number of the main identity document, information about the date of issue of the specified document and the authority that issued it;

3.4.2. surname, first name, patronymic, address of the representative of the subject of personal data, number of the main identity document, information about the date of issue of the said document and the authority issuing it, details of the power of attorney or other document confirming the authority of this representative (when obtaining consent from the representative of the subject of personal data);

3.4.3. name or surname, patronymic and address of the operator receiving the personal data subject's consent;

3.4.4. purpose for personal data processing;

3.4.5. list of personal data for processing or distribution of which the personal data subject's consent is provided;

3.4.6. name or surname, patronymic and address of the person processing personal data on behalf of the operator, if the processing will be entrusted to such a person;

3.4.7. list of actions with personal data for which the consent is provided, general description of personal data processing methods used by the operator;

3.4.8. term, during which the personal data subject's consent is valid, as well as the way of its withdrawal, unless otherwise provided by the federal law;

3.4.9. personal data subject's signature.

ARTICLE 4: PURPOSES FOR PERSONAL DATA PROCESSING

4.1. The purposes for personal data processing are:

4.1.1. conclusion, execution, termination of contracts with employees, legal entities or individuals, concluded during the Company activity;

4.1.2. accounting employees, ensuring compliance with labor legislation requirements, fulfillment of obligations under labor contracts or civil law contracts concluded with employees;

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Internet : www.eastconsult.eu

4.1.3. realization of labor legislation requirements: conclusion and termination of labor contracts or civil law agreements, advanced training for employees, compensations, benefits, as well as any other activities related to the maintenance of employees records;

4.1.4. realization of the tax, insurance, and pension legislation requirements.

ARTICLE 5: RIGHTS OF PERSONAL DATA SUBJECTS

5.1. The subject of personal data has the right to protect his rights and legitimate interests, including compensation for damages and (or) compensation for moral damage in court.

5.2. The subject of personal data has the right to require the operator to clarify his personal data, block or destroy it if the personal data is incomplete, outdated, inaccurate, illegally obtained or not necessary for the stated purpose, as well as to take statutory measures to protect his rights.

5.3. The personal data subject has the right to receive information regarding personal data processing, including information that contains:

5.3.1. confirmation of the fact of personal data processing by the operator;

5.3.2. legal grounds and purposes for personal data processing;

5.3.3. purposes and methods used by the operator for personal data processing;

5.3.4. name and location of the operator, information about persons (other than the operator's employees) who have access to personal data or to whom personal data may be disclosed on the basis of a contract with the operator or on the basis of federal law;

5.3.5. processed personal data relating to the relevant personal data subject, its source, unless another procedure for presentation of such data is provided by federal law;

5.3.6. terms of personal data processing, including the storage terms;

5.3.7. procedure of exercising the rights provided by the Federal Law by the personal data subject;

5.3.8. information about the carried out or expected the cross-border data transfer;

5.3.9. name or surname, patronymic and address of the person processing personal data on behalf of the operator, if the processing is or will be entrusted to this person.

5.4. The information specified shall be provided to the personal data subject by the operator in an accessible form.

5.5. Information shall be provided to the personal data subject or his representative by the operator upon application or upon request of the personal data subject or his representative. The request shall contain the number of the personal data subject's or his representative's primary identification document, the issue date of the specified document and the issuing authority, information confirming the personal data subject's participation in relations with the operator (contract number, contract execution date, conventional word mark and (or) other information), or information otherwise confirming that the operator processes personal data, and the personal data subject's or his representative's signature. The request may be sent in the form of an electronic document and signed by electronic signature in accordance with the Russian legislation.

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Internet : www.eastconsult.eu

5.6. If information, as well as processed personal data was provided for familiarization to the personal data subject at his request, the personal data subject has the right to apply again to the operator or send him a second request in order to obtain information and familiarization with such personal data not earlier than thirty days after the initial application or sending the original request, unless a shorter period is not established by federal law, a legal act adopted in accordance with it, or a contract to which the personal data subject is a party or a beneficiary or guarantor.

5.7. The personal data subject has the right to apply again to the operator or send him a second request in order to obtain information, as well as to familiarize with the processed personal data before the expiration of the specified period, if such information and (or) processed personal data were not provided to him for familiarization in full after consideration of the original application.

5.8. The personal data subject's right to access their personal data may be restricted in accordance with federal laws, including if:

5.8.1. personal data processing, including personal data obtained as a result of operative investigation, counter-intelligence and intelligence activities, is carried out for the national defense purposes, state security and law enforcement;

5.8.2. personal data is processed by authorities that have arrested the personal data subject on suspicion of a crime, or have charged the personal data subject in a criminal case, or have applied a preventive measure to the personal data subject prior to charging him, except as provided for in the criminal procedural Russian legislation, if the familiarization with such personal data is permitted to the suspected or accused person;

5.8.3. personal data processing shall be carried out in accordance with the anti-money laundering and counter-terrorism financing legislation;

5.8.4. the personal data subject's access to his personal data violates third parties' rights and legitimate interests;

5.9. If the personal data subject considers that the operator carries out his personal data processing in violation of legal requirements or otherwise violates his rights and freedoms, the personal data subject has the right to appeal the operator's actions or inaction in the authorized body for the protection of the rights of personal data subjects or in court.

ARTICLE 6: ORGANIZATION OF PERSONAL DATA PROTECTION

6.1. The main objects of the personal data protection system in the Company are:

6.1.1. information resources with limited access, containing personal data;

6.1.2. personal data processing processes in the Company's personal data information systems, information technology, regulations and procedures for collecting, processing, storing and transferring information, system developer and user employees, and system maintenance employees;

6.1.3. information infrastructure, including information processing and analysis systems, technical and software tools for its processing, transfer, and display, including information exchange channels

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Internet : www.eastconsult.eu

and telecommunications, information protection systems and tools, facilities, and premises where technical tools for personal data processing are located.

6.2. The main purpose for which all provisions hereof are intended is to ensure the personal data protection in accordance with legal requirements, which is achieved by ensuring and constantly maintaining the following personal data properties:

6.2.1. personal data accessibility for legitimate users (sustainable operation of the Company's information systems, when users are able to obtain the necessary personal data and the results of tasks solution in an acceptable time for them;

6.2.2. integrity and authenticity (authorship confirmation) of personal data stored and processed in the Company's information systems and transferred via communication channels;

6.2.3. confidentiality – confidentiality of a certain part of personal data stored, processed, and transferred via communication channels.

6.3. The necessary level of availability, integrity and confidentiality of personal data is ensured by methods and means appropriate to a variety of significant threats.

6.4. In order to achieve the main purpose of protecting and ensuring the specified personal data properties, the Company's information security system shall provide an effective solution to the following tasks:

6.4.1. timely identification, assessment and prediction of the sources of threats to information security, causes and conditions that contribute to damage to the stakeholders of information relations, disruption of the normal functioning of the Company's information systems;

6.4.2. creating mechanism for rapid response to information security threats and negative trends;

6.4.3. creating conditions for minimizing and localizing the damage caused by illegal actions of individuals and legal entities, reducing the negative impact and eliminating the consequences of information security violations;

6.4.4. protection against interference in the operation of the Company's systems by unauthorized persons (only duly registered users should have access to information resources);

6.4.5. differentiation of user access to information, hardware, software and other Company resources (ability to access only those resources and perform only those operations that are necessary for specific users to perform their duties), i.e., protection against unauthorized access;

6.4.6. ensuring authentication of users involved in information exchange (authentication of the sender and recipient of information);

6.4.7. protection against unauthorized modification of software used in the Company's information systems, as well as system protection against the intrusion of unauthorized programs, including computer viruses;

6.4.8. protection of restricted data from leakage via technical channels during its processing, storage, and transmission via communication channels.

6.5. The main protection purposes and fulfillment of the mentioned tasks are achieved by:

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Internet : www.eastconsult.eu

6.5.1. strict accounting of all Company's information system resources to be protected (information, tasks, documents, communication channels, servers, automated workstations);

6.5.2. journaling the activities of employees engaged in software and hardware maintenance and modification of information systems;

6.5.3. completeness, practical feasibility and requirements consistency of the Company's organizational and administrative documents on information security;

6.5.4. training of officers (employees) responsible for organization and implementation of practical measures to ensure personal data protection and processing;

6.5.5. providing each employee (user) with the minimum necessary authority to access the Company's information resources in order to perform his functional duties;

6.5.6. precise knowledge and strict compliance by all users of the Company's information systems with the requirements of organizational and administrative documents on information security;

6.5.7. individual liability for the actions of each employee who has access to the Company's information resources within his functional responsibilities;

6.5.8. permanence of the necessary security level of the elements of the Company's information environment;

6.5.9. applying physical and technical (software and hardware) protection tools for system resources and continuous administrative support for their use;

6.5.10. effective control over compliance with information security requirements by users of the Company's information resources;

6.5.11. legal protection of the Company's interests when interacting with external organizations (associated with the personal data exchange) from unlawful actions, both on the part of these companies, and from service employees and third parties' unauthorized actions.

6.6. The Company's personal data protection system construction and operation shall be carried out under the following basic principles:

6.6.1. Lawfulness. Involves implementation of protective measures and development of the Company's personal data protection system in accordance with applicable legislation on personal data protection, as well as other legislative acts on information security of the Russian Federation, using all permissible detection and suppression methods of offenses when working with personal data. Measures taken for the personal data protection shall not prevent access to law enforcement agencies in cases provided by law. All users of the Company's information systems shall be aware of liability for offences in the field of personal data processing;

6.6.2. Systematization. The systematic approach to building a data protection system in the Company involves considering all interrelated, interacting and changing over time elements, conditions and factors that are important for understanding and solving the problem of ensuring the personal data protection. When making the protection system, all Company's information systems' vulnerable and weak points shall be considered, as well as the nature, possible objects, and directions of attacks on it by intruders (especially highly qualified intruders). The protection system shall be made taking into account not only all known penetration channels and

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Internet : www.eastconsult.eu

unauthorized access to information, but also taking into account the possibility of fundamentally new ways of security threats;

6.6.3. Comprehensiveness. Comprehensive use of protection methods and tools for computer systems implies the consistent use of diverse tools to make an integral protection system that covers all significant (important) channels of threat implementation and does not contain weak points at the junctions of its individual components. Protection shall be staged. External protection shall be provided by physical means, organizational and legal measures;

6.6.4. Consistency. Ensuring the personal data protection is a process carried out by the Company's management, those responsible for organizing the personal data processing and employees at all levels. It is not only and not so much a procedure or policy that is implemented at a certain period of time or a set of protection tools, but rather a process that is to be ongoing at all levels within the Company, and everyone in the Company shall be involved in that process. Information security activities are an integral part of the Company's daily activities. And its effectiveness depends on the participation of the Company's management in ensuring the personal data protection. In addition, most physical and technical tools need constant organizational (administrative) support (timely change and ensuring proper storage and use of names, passwords, redefining permissions, etc.) to perform their functions effectively. Breaks in protection tools can be used by intruders to analyze the protection methods and tools used, to implement special software and hardware "bookmarks" and other means of overcoming protection;

6.6.5. Timeliness. Involves the proactive nature of personal data protection measures, i.e., setting objectives for comprehensive personal data protection and implementation of personal data protection measures at the early stages of information systems development in general and their protection systems. Development of the protection system shall be carried out simultaneously with the design and development of the protection information systems. This will allow security requirements to be considered when designing the architecture and, ultimately, to create systems that are more efficient (both in terms of resource consumption and resilience) and have a sufficient protection level.

6.6.6. Continuity and improvement. Continuous improvement of protection measures and tools for personal data based on the continuity of organizational and technical solutions, employee resources, analysis of the Company's information systems and their protection system, considering changes in information interception methods and tools, regulatory requirements for protection, and domestic and foreign experience in this field;

6.6.7. Reasonable sufficiency (economic feasibility). Involves compliance of the cost for ensuring the personal data protection with the information resources and the possible damage from their disclosure, loss, leakage, destruction, and distortion. The measures and tools used to ensure the security of information resources shall not noticeably affect the ergonomic performance of the Company's information systems components;

6.6.8. individual liability. Assumes the liability for ensuring the personal data protection and processing system to each employee within the limits of his authority. In accordance with this principle, the rights and duties of employees are distributed in such a way that in case of any violation the range of perpetrators is clearly known or minimized;

6.6.9. Authority minimization. Means providing users with minimum access rights in accordance with the duties. Access to personal data shall be provided only if and to the extent that it is necessary for the employee to perform his duties;

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Internet : www.eastconsult.eu

6.6.10. Avoiding conflicts of interest (duties segregation). An effective information security system involves a precise division of employees' duties and the exclusion of situations where employees' responsibilities allow for conflicts of interest. Areas for potential conflicts shall be identified, minimized, and shall be under strict independent control. Realization of this principle supposes that no employee shall have powers, which could allow him to carry out critical operations by himself. Providing employees with the power to create conflicts of interest gives them the opportunity to falsify information for self-interest or to hide problems or losses incurred. To reduce the risk of manipulation of personal data and the risk of theft, such powers should, to the extent possible, be divided between different employees or divisions of the organization. Periodic reviews of employees' duties, functions and activities in key functions should be conducted to ensure that they do not have the ability to conceal the commission of misconduct. In addition, special measures should be taken to prevent collusion among employees;

6.6.11. Flexibility of the protection system. The information security system shall be able to respond to changes in the external environment and the environment in which the Company conducts its activities. Such changes include: changes in the organizational and employee structure, changes in existing information systems or the introduction of fundamentally new information systems, and new technical means;

6.6.12. Openness of algorithms and protection mechanisms. The essence of this principle is that protection should not be provided only by structural organization secrecy and algorithms of subsystems functioning. Knowledge of the algorithms of the protection system should not allow (even the authors) to overcome it. This, however, does not mean that information about the systems and protection mechanisms used should be publicly available;

6.6.13. Simplicity of applying protection means. Protection mechanisms and methods shall be intuitive and easy to use. Applying protection mechanisms and methods shall not be associated with special language skills or with performing actions that require significant additional labor input during normal operation of registered users, and shall not require the user to perform routine operations that he does not understand well;

6.6.14. Relevance and technical feasibility. Information technologies, technical and software tools, means and measures for personal data protection shall be implemented at the current level of science and technology development, justified in terms of achieving a given level of information security and economic feasibility, and shall comply with established standards and requirements for personal data protection;

6.6.15. Specialization and professionalism. Involves involvement in the development of means and implementation of personal data protection measures of specialized organizations that are best prepared for a particular activity to ensure the information resources security, with experience in practical work and a state license to provide services in this field. Implementation of administrative measures and operation of protection means shall be carried out by professionally trained specialists of the Company (responsible for organization of personal data);

6.6.16. Obligatory control. Involves the obligatory and timely detection and suppression of attempts to violate the established rules, ensuring the personal data protection, based on the systems and means of personal data protection used, while improving the criteria and methods for assessing the effectiveness of these systems and means. Control over the activities of any user, each protection tool and in respect of any object of protection shall be carried out based on the application of operational control and registration tools and shall cover both unauthorized and authorized actions of users. In addition, an effective information security system requires

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Internet : www.eastconsult.eu

adequate and comprehensive information about the current status of the processes involved in the information flow and compliance with regulatory requirements, as well as additional information relevant to decision-making. The information must be reliable, timely, accessible, and properly formatted. Deficiencies in the information security system identified by the Company's employees should be immediately reported to the Company's director and promptly corrected. Issues that seem insignificant when individual processes are considered in isolation, when considered along with other aspects, may indicate negative trends that threaten to escalate into major deficiencies if they are not addressed timely.

6.7. All security measures for the Company's information systems are divided into:

6.7.1. Legislative (legal) protection measures. Legal protection measures include laws, orders and regulations applicable in the country, which regulate the rules for handling personal data, stipulate participants' rights and obligations during processing and information use, as well as establishing liability for violations of these rules;

6.7.2. Technological protection measures. This type of protection measures includes various technological solutions and techniques based on the use of certain types of excessiveness (structural, functional, informational, temporal, etc.) and aimed at reducing the possibility of employees committing errors and violations within the rights and powers provided to them;

6.7.3. Organizational (administrative) protection measures. Organizational (administrative) protection measures are organizational measures that regulate the personal data processing system functioning, use of its resources, activities of service employees, as well as procedures for interaction of users with the system in such a way as to make it most difficult or impossible to implement security threats or reduce the number of losses in case of their implementation. The main purpose of administrative measures taken at the top management level is to form a personal data protection policy (reflecting the approaches to personal data protection) and ensure its implementation by allocating the necessary resources and controlling the state of affairs.

ARTICLE 7: ACCESS TO PERSONAL DATA

7.1. Access to premises regulation.

7.1.1. The Company's information systems components shall be located in secured or monitored premises that prevent unauthorized access to the premises and ensure the physical safety of the protected resources (documents, workstations, etc.) in the premises. Such premises shall be cleaned in the presence of the responsible employee to whom these components are assigned, and measures shall be taken to prevent unauthorized access to protected information resources.

7.1.2. All unauthorized persons shall be allowed into the premises with information system components only in the presence of the Company employees.

7.1.3. At the end of the working day, the premises in which components of the Company's information systems are located shall be locked with an electromechanical lock with biometric access control to the premises.

7.1.4. If the premises are equipped with security alarm system, as well as an automated system for receiving and recording signals from such systems, the acceptance and handover of such premises for guarding shall be carried out based on a specially developed instruction.

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Internet : www.eastconsult.eu

7.2. Regulation of employee access to information resources.

7.2.1. User access to the Company's information systems and access to their resources must be strictly regulated. Any changes in the subsystems content and user's authorities shall be carried out according to the established procedure.

7.2.2. The authority level of each user is determined individually, according to the following requirements:

- each employee shall exercise only the rights prescribed in relation to the personal data with which he is required to work in accordance with his duties. Extending access rights and providing access to additional information resources shall, without fail, be coordinated with the person responsible for the organization of personal data processing,

- the Company director has the right to view the information of his employees only within the prescribed limits in accordance with his official duties.

7.2.3. All employees of the Company shall be individually liable for violations of the established personal data processing procedure, storage, use and transfer of protected resources of the system in their disposal. Each employee (when employed) must sign an obligation to comply with and be responsible for violations of the established requirements for the preservation of the Company's personal data.

7.2.4. Personal data processing in the Company's information systems components shall be carried out in accordance with the established technological instructions.

7.3. Regulation of the maintenance and modification of hardware and software resources.

7.3.1. In order to maintain the information protection mode, the hardware and software configuration of the automated workstations of the Company's employees, from which access to the information system resources is possible, must comply with the range of functional responsibilities entrusted to these users.

7.3.2. In the components of the information system and users' workstations, licensed software must be installed and used.

7.4. Ensuring and controlling the physical integrity (unchanged configuration) of hardware resources. Information systems equipment used for personal data access and storage, to which access by service employee is not required during operation, shall be closed after adjustment, repair and other work related to access to its components.

7.5. Staff recruitment and training, user training.

7.5.1. Users of the Company's information systems, as well as senior and service staff, must be familiar with their authority, as well as organizational and administrative, regulatory, technical, and operational documentation defining the requirements and procedure for processing personal data in the Company.

7.5.2. All users of the Company's information systems shall be familiar with the organizational and administrative documents on the Company's personal data protection, as they relate to them, shall know, and strictly comply with the instructions and know the general responsibilities for the personal data security. Informing the persons admitted to the processing of protected personal data of the requirements of these documents shall be carried out against signature.

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Internet : www.eastconsult.eu

7.6. Liability for violations of the established procedure for using the Company's information system resources. The degree of responsibility of employees for actions taken in violation of the established rules for the safe handling of personal data shall be determined by the damage caused, the presence of malice and other factors at the discretion of the Company's management.

ARTICLE 8: TOOLS OF ENSURING PERSONAL DATA SECURITY

8.1. Protection tools shall be applied to all the Company information system resources, regardless of their type and form of information representation in them.

8.2. Physical protection tools. Physical protection measures are based on the use of various kinds of mechanical, electronic, or electronic-mechanical devices and facilities specifically designed to create physical barriers to possible entry and access routes of potential intruders to system components and protected personal data, as well as technical means of visual monitoring, communication, and security alarms. To ensure physical security of information system components, the Company shall implement a number of organizational and technical measures, including checking the equipment intended for personal data processing for:

8.2.1. presence of specially implemented devices (bugs),

8.2.2. additional restrictions on access to the premises intended for personal data storage and processing,

8.2.3. equipment of information systems with protection devices against power failure and interference in communication lines.

8.3. Technical protection tools. Technical (hardware and software) protection measures are based on the use of various electronic devices and special software and performing (independently or in combination with other tools) protection functions (user identification and authentication, differentiation of access to resources, event registration, cryptographic information closure, etc.). Considering all personal data security requirements and principles in all protection areas, the following tools shall be included in the protection system:

8.3.1. tools for data access differentiation,

8.3.2. tools for access registration to information system components and control over information use,

8.3.3. tools for responding to information security violations.

8.4. The technical protection tools are to be used for the following main purposes:

8.4.1. user identification and authentication using names or special hardware (Advantor, Touch Memory, Smart Card, etc.),

8.4.2. regulating and managing user access to premises, physical and logical devices,

8.4.3. protection against computer viruses and the destructive effects of malware,

8.4.4. protecting the data protection system on the file server from access by users whose job duties do not include working with the information on it.

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Internet : www.eastconsult.eu

8.5. Users identification and authentication tools. In order to prevent unauthorized persons from working with the Company's information system resources, it is necessary to ensure that each legal user (or groups of users) can be identified. Different kinds of devices can be used for identification: magnetic cards, keys, key inserts, floppy disks, etc. User authentication (authentication exchange) can also be performed:

8.5.1. by checking whether users have any special devices (magnetic cards, keys, key inserts, etc.),

8.5.2. by checking their password knowledge,

8.5.3. by verifying the users' unique physical characteristics and parameters with special biometric devices.

8.6. Access differentiation tools. Liability and tasks of particular technical protection tools shall be set based on their capabilities and operational characteristics described in the documentation supplied with these tools. Technical access differentiation tools shall, if possible be an integral part of the unified access control system:

8.6.1. to the territory under control,

8.6.2. to separate premises,

8.6.3. to components of Company's information environment, personal data protection system elements (physical access),

8.6.4. to information resources (documents, media, files, data sets, archives, certificates, etc.),

8.6.5. to active resources (application programs, tasks, etc.),

8.6.6. to the operating system, system programs and protection programs.

8.7. Integrity assurance and control tools. Integrity assurance tools include backup tools, anti-virus protection programs, operating environment, and database integrity recovery programs. The tools of systems integrity control are designed to detect system resources modification or distortion in a timely manner. They make it possible to ensure correct protection system functioning and integrity of stored and processed information. Information integrity control and protection tools, in order to ensure integrity of information environment defined by processing technology and protection against unauthorized modification of personal data shall be provided:

8.7.1. by access differentiation tools (to rooms, documents, information carriers, servers, logical devices, etc.),

8.7.2. by electronic signature tools,

8.7.3. checksum calculation tools (for the applied software).

8.8. Tools of operational control and security events registration. Means of objective control shall provide detection and registration of all events (user actions, unauthorized access attempts, etc.) which can lead to security violations and lead to crisis situations. The analysis of the information collected by the logging tools makes it possible to identify the violations, their nature, suggest the investigation method and ways to find the perpetrator and remedy the situation. Control and recording tools shall provide capabilities:

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Internet : www.eastconsult.eu

8.8.1. to maintain and analyze security event logs (system logs),

8.8.2. to organize the logs, as well as to establish limits on the logs storage term,

8.8.3. to promptly notify on violations the person responsible for organizing the personal data processing.

8.9. When registering security events in the log the following information shall be recorded: date and time of the event, identity of the subject performing the registered action, action (access type).

8.10. Efficiency control of the protection system. Efficiency control of personal data protection system is carried out in order to timely detect and prevent personal data leakage due to unauthorized access, as well as to prevent possible special impacts aimed at personal data destruction, information tools destruction. Controls may be carried out by organizations licensed for this purpose. Effectiveness of personal data protection measures shall be assessed using technical and software controls for compliance with the established requirements.

eastconsult LLC
Varshavskoye Chaussee, 125 D, Corpus 2
office 15i, 117587 Moscow
Russian Federation

ООО «истконсалт»
Варшавское шоссе, 125 Д, корпус 2
помещение 15и, 117587 Москва
Российская Федерация

Tel./Тел.: +7 495 225 5006
Hotline: +7 800 500 8529
Fax/факс: +7 495 258 3706

Email : office@eastconsult.eu
Skype : eastconsult.weiss
Internet : www.eastconsult.eu