PRIVACY POLICY

Technical and organizational measures for Personal Data Protection

infraTEAM

Wioletta Curyło

ul. Szafirowa

57c/19

44-121 GLIWICE

Content

Admission

implementing the provisions of Regulation of the European Parliament and of the Council (EU) 2016/679 from 04.27.2016 r. on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation) (OJ L 119, p. 1) on personal data processing documentation and technical and organizational conditions which should be fulfilled by devices and information systems for processing personal data introduced a set of rules and practical experience of governing the management, conservation and distribution of personal data, including data specific categories of (sensitive) allowing to ensure the appropriate level of protection, hereinafter the Policy for Personal Data protection (abbreviated policy).

The aim of the policy is to ensure the protection of personal data processed through **infraTEAM Street. Plebiscytowa 1, 44-100 Gliwice,**hereinafter**infraTEAM**for the purposes specified in Article. And Article 6. 9Regulation of the European Parliament and of the Council (EU) 2016/679 of 27.04.2016 r. On the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46 / EC (General Data Protection Regulation) (OJ L 119, p. 1) hereinafter RODO against all types of threats, such as internal and external, conscious or unconscious.

Policy infraTEAM applies to all employees, including interns, volunteers, trainees and suppliers, cooperating entities under civil law contracts, having any contact with personal data protected by.

Applied security are intended to achieve these objectives and to ensure:

Legality - infraTEAM committed to protecting the privacy and data processing in accordance with the law.

Security - infraTEAM ensures an adequate level of data security is constantly taking action in this regard.

individual rights - infraTEAM allows individuals whose data are processed, realize their rights and the rights of these respects.

confidentiality - **infraTEAM** It ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes,

Integrity - **infraTEAM** ensure, that the data has not been altered or destroyed in an unauthorized manner,

accountability - **infraTEAM** It documents how fulfilled his obligations under RODO, at any time, be able to demonstrate compliance with the processing of personal data by RODO keeping the register of processing operations - Appendix 7 category and registry operations - Annex **No. 8,**

Authenticity - **infraTEAM** ensure that the identity of the entity or resource is as declared (authenticity relates to data, users, processes, systems and information)

Non-repudiation - **infraTEAM** ensure that it does not disown his participation in whole or in part data exchange with another entity,

Processing of personal data in infraTEAM done on paper and using information systems.

Legal determinants of personal data processing:

1. Constitution (Art. 47, Art. 51).
2. Regulation of the European Parliament and of the Council (EU) 2016/679 of 27.04.2016 r. On the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46 / EC (General Data Protection Regulation) (OJ L 119, p. 1), hereinafter referred to as RODO.
3. The Act of 10 May 2018. On the protection of personal data.
4. Act of 7 November 2014. Facilitate the exercise of economic activity.
5. Labor Code.
6. Civil Code.

Chapter I General Provisions

1. **Administrator of Personal Data (ADO)**- it shall be understood:**Wioletta Curyło.**
2. **Data Protection Supervisor (IOD)** - appointed - not applicable.
3. **System Administrator (ASI)** - should be understood as the person responsible for the operation of the information system designated by the ADO - Mikołaj Salamak.
4. **Personal Data Protection Policy** - shall mean a set of technical and organizational measures to protect personal data entered, implemented and used in the**infraTEAM** necessary to ensure confidentiality, integrity and accountability of processed data as described herein**.**
5. **RODO** - Regulation of the European Parliament and of the Council (EU) 2016/679 of 27.04.2016 r. on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation) (OJ L 119, p. 1) - Appendix 28.
6. **Personal information (data)**- Art. 4 paragraph. 1 RODO - an identifiable natural person is a person that can be identified, directly or indirectly, in particular on the basis of the identifier, such as name, ID number, data Location ID, Internet, one or more factors specific to: physical, physiological, genetic, mental, economic, cultural or social identity of the individual;
7. **Special categories of data (sensitive)** - data containing information such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, data on sexuality or sexual orientation, biometric data, genetic code.
8. **Deleting data** - mean the destruction of personal data or such modification which will not allow the identification of the data subject (anonymous).
9. **Profiling** - means any form of automated processing of personal data, which involves the use of personal data to evaluate certain personal factors of the individual, in particular for the analysis or forecasts aspects of the effects of the work of the individual, its economic situation, health, personal preferences, interests, credibility, behavior or movement;
10. **Reducing processing** - means an indication of stored personal data in order to reduce their future processing;
11. **The consent of the data subject**- shall mean a declaration of intent, the content of which is

consent to the processing of personal data on who makes a declaration; consent can not be presumed or declaration of will of other content.

12. **Personal Database**- a set of ordered thematically linked data stored eg. In the internal memory or the external computer. The database is composed of the elements of a structured - records or objects, which are stored personal information.
13. **data processing** - means an operation or set of operations performed on the personal data or sets of data in an automated or non-automated, such as collecting, recording, organization, organization, storage, adapt, modify, download, browsing, use, disclosure by the message distribution, or otherwise making available, matching, or combination, reduction, removal or destruction.
14. **processing area** - it should be understood offices, where workers **infraTEAM**process personal data. The list of buildings and spaces representing the area of personal data processing with graphical illustration is given in Annex No. 23.
15. **Collection of personal data** - should be understood as any structured set of personal data which is available according to specific criteria regardless of whether the division of the dispersion.
16. **System, data communications system, the system** - a set of cooperating devices, programs, procedures, information processing and software tools used to process the data.
17. **Register of processing operations** - should be understood as a document that is shown in particular in which the processes **infraTEAM**personal data are processed, for what purpose, and how to relate to who are hedged. This document will have to be made available for every call PUODO - Appendix 7.
18. **safety procedures**- it should be understood procedures to protect personal data processed.
19. **Pseudonymisation**- means the processing of personal data in such a way that they can not be attributed to a specific person, the data subject without the use of additional information, provided that the information is stored separately and are subject to technical and organizational measures preventing them from being identified assign a person. Pseudonymisation personal information is so depriving the characteristics of personal data, and therefore the possibility of identification on the basis of the individual.

Data protection in infraTEAM

General rules

The data protection rules:

infraTEAM processes personal data in compliance with the following principles:

a. based on a legal basis and in accordance with the law (legalism);
b. and fairly accurately (accuracy);
c. in a manner transparent to the data subject (transparency);
d. for specific purposes and not "on reserve" (minimizing);
e. no more than necessary (appropriateness);
f. with attention to the accuracy of the data (regularity);
g. no longer than necessary (temporality);
h. providing appropriate data security (security).

The protection of personal data **infraTEAM** It consists of the following elements:

1. Inventory data. **infraTEAM** identifies the resources of personal data, data classes, relationships between data resources, to identify ways to use the data and on the basis of this inventory keeps a register of processing operations Processing- Annex 7, including:
   and) cases, data processing of special categories of data and "criminal" (convictions, violations of the law) - identified cases where processed or may be data processing of special categories of (sensitive and data penalties) and maintains dedicated mechanisms to ensure the legality of the processing of special categories of data - appendix 7.
   b) data processing cases of people whose **infraTEAM** does not identify the (unidentified data / UFO) - ADO identifies cases in which processes can process data or unidentified remains and mechanisms to facilitate the implementation of the rights of data subjects unidentified - Appendix 7.
   c) data processing cases of children - Annex 7;
   d) profiling; ADO identifies cases in which he makes the processed data profiling and maintains mechanisms to ensure compliance with the law of this process. In the case of identification of cases, profiling and automated decision-making, the ADO shall proceed in accordance with accepted principles in this area - Appendix 7.
   e) współadministrowania data; ADO data identifies cases współadministrowania and act in this respect in accordance with accepted principles - Appendix 7.
2. **infraTEAM**developed leads, maintain and update activity log processing personal data (RCPD). The registry is a tool for settling compliance with data protection**infraTEAM**.

a) RCPD is a form of documentation of data processing activities, acts as a map data and is one of the key elements to implement the fundamental principle on which is based the whole system of protection of personal data, the principle of accountability.

b) ADO keeps the Register of Operations Data Processing (**Appendix 7)**In which collates and monitors the way in which he uses personal data.

c) The registry is one of the basic tools for ADO settlement of most of the obligations of data protection.

d) In the Register, for each data processing activities, which ADO considered a separate registry for ADO record at least:
   - the name of the function,
   - purpose of the processing,
   - description of the categories,
   - a description of the categories of data
   - the legal basis for processing, together with the legitimate interest of specifying the category ADO, if the base is a legitimate interest,
   - method of data collection,
   - a description of the categories of recipients (including processing)
   - information transfer outside EU / EEA;
   - a general description of the technical and organizational data protection measures.

e) The register is attached as Appendix 7 to Policy. The register also includes optional columns. The optional columns ADO records information on needs and possibilities, taking into account the fact that a more comprehensive content of the Register facilitates the management of data protection and compliance with the settlement.

f) **infraTEAM** maintain a record of activities category, which documents the categories of personal data processing operations entrusted by the data controllers under the agreements entrusting - Appendix 8. This register Notes the following data:
   - categories of processing operations,
   - a general description of the technical and organizational security measures
   - the name and contact details of the administrator,
   - the name and contact details of the controller's representative (if appointed)
   - The Data Protection Administrator (if appointed)
   - the names of third countries or international organizations, for which the data are transferred,

- documentation of appropriate safeguards for personal data transferred on the basis of Article. 49 paragraph. 1, second paragraph.
- any other information which, in recognition of the ADO may additionally help in documenting the principle of accountability data.

g) **infraTEAM** assesses the implications for data protection (called. Data Protection Impact Assessment DPIA) - Annex 10, in the case of a high risk of violating the rights and freedoms of individuals.

The risk for the protection of personal data could result from:

- nature,
- the scope,
- context
- processing purposes.

Processing operations that are associated with a high risk of violation of the rights and freedoms of natural persons, include in particular operations that:

- They involve the use of new technologies;
- They are new and have not yet been assessed by the administrator implications for data protection;
- They made necessary due to the elapse of time from the initial processing.

High risk of violation of the rights or freedoms of individuals exists, in particular in case of:

- systematic, comprehensive assessment of personal factors relating to individuals, which is based on automated processing and is the basis for decision-inducing effects of a natural person;
- large-scale processing of sensitive data, genetics, biometrics or personal data relating to criminal convictions and violations of the law;
- systematic large-scale monitoring places accessible to the public.

3. Law basics. **infraTEAM** provides identifies, verifies the legal basis for data processing and records them in the registry (RCPD), including:
   a) manages consents to the processing of data and communication at a distance,
   b) inventories and specifies justification cases where processing data on the basis of a legitimate interest - Appendix 7.
   c) ADO documents in the Register of legal grounds for processing data for the individual

processing steps,

d) indicating a general legal basis (agreement, a contract, legal obligation, vested interests, the task of public / public authority, legitimate aim ADO)**infraTEAM**clarifies basis in a clear way, when you need it. Eg. For approval indicating its scope, when the foundation is right - pointing to a specific recipe and other documents, eg. A contract, an administrative arrangement, vested interests - pointing to the categories of events in which they materialize, the legitimate objective - pointing to a specific purpose, eg. marketing its own redress,

e) ADO manages consents (Annex 5) verify ownership consent to the processing of the specific data for a specific purpose, the consent of communication at a distance (email, phone, SMS, et al.) And the registration of a refusal, withdrawal of consent and similar activities (opposition, limitation, etc. .) appendix 5b.

4. Operation of individual rights. **infraTEAM** meet the information obligations towards persons whose data are processed, and supports their rights, realizing received a request in this regard, including:

a) disclosure obligations;**infraTEAM** transmit to the persons required by law information in data collection and in other cases, and organizes and provides documentation of the implementation of these responsibilities - information are available at the registered office **infraTEAM**, In the form of clauses on consents to the processing of data, the clause on the website.

b) **infraTEAM** and it provides the ability to verify the effective implementation of any type of lawful request for personal data by a natural person themselves and their processing.

c) **infraTEAM** It provides adequate inputs and procedures to request people were executed on dates and in the manner required by RODO and documented.

d) **infraTEAM** evaluates the result of a breach of data protection for the rights and freedoms of the individual for determining the need for notice of people affected by the identified violation of data protection.

How to handle individual rights and obligations of information:

a) ADO cares about style and readability of the information and communication with the people whose data are processed.

b) ADO facilitates people to exercise their rights through various activities, including posting on the website information or ADO references (links) to information on the rights of people how to use them**infraTEAM.** including the requirements for the identification methods of contact with ADO in order price list of the possible requests of "additional" - enclosure 30,

and the like.

c) ADO ensures adherence to legal deadlines obligations towards the people.

d) **infraTEAM** identify and authenticate individuals for the realization of individual rights and responsibilities of information.

5. Minimalization. **infraTEAM** respects the principles of minimization and management methods, including:

and) cares about the adequacy of the data;

b) observes the rationing of access to the data;

c) observes the storage periods, and further verifies the relevance;

6. Security. **infraTEAM** It ensures an adequate level of data security, including:

and) carry out risk analyzes for data processing activities or categories;

b) the impact assessment carried out for the protection of data where the risk of infringement and the freedom of people is high;

c) adapt the protection of data to the specified risk;

d) It has an information security management system in the form of appropriate policies;

e) **infraTEAM** identifies, evaluates and reports identified data breach Data Protection Authority - manages incidents.

7. Processing. **infraTEAM** adheres to the principle of selection of data processing in its favor, requirements for the processing conditions (the agreement entrusting), verifies the performance of contracts entrustment.

8. Export data. **infraTEAM** verifies whether or not transmit data to third countries (ie outside the EU, Norway, Liechtenstein, Iceland) or to international organizations and to ensure legal conditions for such a transfer, if it takes place.

9. Privacy by design.**infraTEAM**manage changes affecting privacy. To do this procedure, the launch of new projects and investments take into account the need to assess the impact of the change on data protection, ensuring privacy (including compliance purposes of the processing, data security and minimize) already in the design phase changes, investment or the beginning of a new project.

10. information obligations

a) ADO determines legal and effective ways to perform the duties of information - notices from the information obligation clause, clauses, and consents to the website.

b) ADO inform the person of more than one month extension of the deadline for consideration of the request of that person.

c) ADO inform the person about the processing of their data, collecting data from that person.

d) ADO inform the person about the processing of their data, collecting data about that person indirectly from it.

e) ADO determines how to inform people about the unidentified data processing, where it is possible (eg. Plate area on the acquisition of video surveillance).

f) ADO inform the person about the planned change to the data.

g) ADO inform the person before revoking the restriction processing.

h) ADO informs recipients of the rectification, erasure or restriction of processing of data (unless it will require a disproportionate effort or will not).

i) ADO inform the person of the right opposition in relation to data processing at the latest at the first contact with the person.

j) ADO without undue delay notify the person of the personal data breach, where it can cause a high risk of violation of the rights or freedoms of the person.

11. Requests persons:

a) Rights of third parties. Realizing the rights of data subjects,**infraTEAM**introduces guarantees for the protection of the rights and freedoms of third parties. In particular, in the event of obtaining reliable information about the performance demands a person for a copy of the data or the right to transfer the data may adversely affect the rights and freedoms of others (eg. The law relating to the protection of other people's data, intellectual property rights, trade secrets, personal, etc.)**infraTEAM** You can ask the person to explain the problem, or take other steps permitted by law, including the refusal to demand redress.

b) Not to process. **infraTEAM** It informs the person that does not process data concerning him, if such a person reported a request for its rights.

c) Refusal. **infraTEAM** inform the person within one month of receipt of the request, a refusal to consider the request and the rights of the individuals involved.

d) Access to the data. At the request of the person regarding access to its data,**infraTEAM**inform the person that processes its data and inform the person about the details of processing, in accordance with Article. RODO 15 (range corresponds obliged to provide information in data collection), and give the person access to data concerning him or her. Access to data can be realized by the issue of paid copies of data, provided that a copy of the data issued for the exercise of the right of access to data**infraTEAM** not deem a free copy of the first.

e) Copies of the data. On demand**infraTEAM** issue the person a copy of the data relating to **infraTEAM**implement and maintain a copy of pricing data, according to which charge a fee

for additional copies of the data. Price copy of the data is calculated based of the estimated unit cost of service for the issue of copies of data - Appendix 30.

f) Correcting data. **infraTEAM** shall rectify incorrect data at the request of the person. **infraTEAM**It has the right to refuse to correct the data, unless the person reasonably reveals irregularity data, which seeks to rectify. In the case of rectification**infraTEAM** inform the person of the recipients of the data, at the request of that person.

g) Completion of data. **infraTEAM** supplements and updates the data at the request of the person. **infraTEAM** It has the right to refuse to complete the data, if the supplement would be inconsistent with the purposes of data processing (eg. **infraTEAM** You do not have to process the data that are superfluous to him). **infraTEAM** You can rely on a statement of a person, which supplemented the data, unless it is inadequate in the light of the law or there is reason to consider the statement as unreliable.

h) Removal of data. At the request of the person**infraTEAM** delete the data when:
   - the data are not necessary for the purposes for which they were collected or processed for other purposes,
   - consent to their processing has been withdrawn and there is no other legal grounds for processing,
   - person has made an effective opposition in relation to the processing of those data,
   - data have been processed unlawfully,
   - results from the need to remove a legal obligation
   - the request is for data collected on the basis of the child's consent in order to provide information society services offered directly to the child.

ADO determines how to handle the right to delete data in such a way as to ensure the effective implementation of this law while respecting all the rules of data protection, including security, and also verify that there are no exceptions referred to in Article. 17. paragraph. 3 RODO.

If the data subject to removal have been made public by the ADO, it shall take reasonable steps, including technical measures to inform the other administrators processing personal data, the need to remove the data and access to them.

If you delete the data ADO inform the person of the recipients of the data, at the request of that person.

i) Reducing processing. The ADO shall limit the data at the request of the person, if:
   - a person question the accuracy of the data - the period for checking its accuracy,

- the processing is unlawful and the data subject objects to the removal of personal data demanded in exchange restrictions on their use,
- ADO no longer needs the personal data, but they are necessary to the data subjects to determine investigation or defense of claims,
- person filed an objection with respect to the processing of reasons related to their particular situation - until such time as, or after the ADO occur legitimate grounds override the grounds for opposition.

During processing limitations ADO stores data, but does not process them (do not use, do not forward), without the consent of the data subject, unless in order to establish an investigation or defense of claims, or to protect the rights of another natural or legal person, or because of the important public interest considerations.

ADO inform the person before revoking the restriction processing.

In the case of data limitations ADO inform the person of the recipients of the data, at the request of that person.

j) Transferring data. At the request of an ADO appear in a structured, widely used format suitable for machine readable or transfers to another entity, if possible, data on the person who provided it ADO processed on the basis of the consent of the person or for the conclusion or performance of a contract her contained in the ADO systems.

k) The opposition in the particular situation. If a person raises her particular situation motivated opposition in relation to the processing of data, and the data are processed by**infraTEAM** based on the legitimate interest of ADO or entrusted **infraTEAM** request in the public interest, ADO will take into account the opposition, unless there are on his side an important legal grounds for processing, override the interests, rights and freedom of the person submitting the objection, or basis for determining, investigation or defense of claims.

l) The opposition for research, historical or statistical purposes. If ADO conducts scientific research, historical or processing data for statistical purposes, a person can bring its particular situation motivated objection in relation to such processing. ADO will consider such objection, unless the processing is necessary for the task carried out in the public interest.

m) Objections in relation to direct marketing. If a person raises an objection with respect to the processing of data by the ADO for direct marketing purposes (including possibly

profiling), ADO will take into account the opposition and cease such processing.

n) The right to human intervention for automatic processing. If ADO converts the data automatically, including in particular profiles the people, and consequently the process with the people decisions which have legal effect or otherwise materially affect the person, ADO provides the ability to appeal to the intervention and decision-man side ADO, unless such automatic decision :

- It is necessary for the conclusion or performance of a contract between the person and referencing the ADO; or:
- It is explicitly permitted by law; or:
- based on the explicit consent of the person appealing.

12. Minimalization:

ADO cares about minimizing data for:

- adequacy of data for (amount of data and processing range)
- access to data,
- data retention.

a) Minimizing range

ADO data obtained verified the range, the range of processing and the amount of data being processed in terms of adequacy for the purpose of processing in the framework of the implementation of RODO.

The ADO shall periodically review the amount of data processed and the extent of their processing is not less than once a year.

ADO annually verifies the changes to the amount and scope of data processing.

b) Minimize access

ADO is used to limit access to personal data: legal (the commitment to confidentiality ranges authorizations), physical (access zone, closing the premises) and logical (to limit the authority of personal data processing systems and network resources, which reside in the personal data).

ADO uses physical access control.

ADO updates the access permissions to changes in the composition of staff and changes in the roles of, and changes processing entities.

The ADO shall periodically review the systems established users and update them at least once a year.

Detailed rules for physical access and logical procedures are contained in this information

security policy**infraTEAM**.

c) Minimize time

ADO implements controls the life cycle of personal data**infraTEAM**Including further verification of the data are relative terms and control points specified in the registry.

The data, which is limiting the range of applicability with the passage of time are removed from the system**infraTEAM**As well as the documents handheld and major. Such data can be archived and be on backup systems and information processed by the ADO. procedures for archiving and use of the archives, create and use a backup requirements include control over the data lifecycle, including requirements for data erasure. The data retention period described in Annex 7.

13. Security:

ADO provides a level of security appropriate to the risk of violation of the rights and freedoms of individuals as a result of the processing of personal data by the ADO.

a) Risk analysis and adequacy of security measures

ADO performs and documents the analysis of the adequacy of security of personal data. For this purpose:

1) ADO provides an adequate level of knowledge about information security, business continuity and cyberbezpieczeństwie - internally or with the support of specialized entities.
2) ADO categorizes data and processing steps for the risk, which represent - Appendix 6.
3) ADO carry out risk analyzes violation of the rights and freedoms of natural persons for the data processing activities or categories. ADO analyzes the possible situations and scenarios of undermining the protection of personal data taking into account the nature, scope, context and purposes of the processing, the risk of violation of the rights or freedoms of individuals with different probability of occurrence and severity of threats - Appendix 6.
4) ADO sets possible to apply technical and organizational security measures. In this ADO determines the usefulness and the application of these measures and approach as:
   - Pseudonymisation,
   - encryption of personal data,
   - other cyber security measures making up the ability to continually ensure the confidentiality, integrity, availability and resilience of systems and processing

services,

- measures to ensure business continuity and disaster prevention, or the ability to quickly restore the availability of personal data and access to them in the event of an incident of physical or technological - eg. a backup policy.

b) Impact assessments for data protection

The ADO shall assess the impact of the planned processing operations for the protection of personal data where risk analysis in accordance with the risk of violating the rights and freedoms of people is high.

c) Security measures

ADO uses security measures established in the risk analyzes and the adequacy of security measures and impact assessments for data protection.

Security of personal data are part of the information security measures and ensure cyber security **infraTEAM** and they are described in more detail in the procedures adopted by the ADO for these areas (Security Manual processing of personal data).

d) Reporting violations

ADO identifies, evaluates and reports identified data breach Data Protection Authority within 72 hours of establishing the infringement, Data informs administrators when entrusting data about the incident as within 24 hours of establishing the infringement.

14. Recycled

ADO selects and verifies the data processing for the**infraTEAM** in order to ensure that processing give sufficient guarantees to implement appropriate technical and organizational measures to ensure the security, realization of individual rights and other data protection obligations incumbent on **infraTEAM**.

ADO accepted the minimum requirements for an agreement for the processing of data annexed to Policy No. 20 - the agreement entrusting data processing.

ADO settles processing of podprzetwarzających use, as well as other requirements stemming from the principles of entrusting personal data.

15. Export data

ADO record in the Register of cases of export data, the transmission of data outside the European Economic Area (EEA in 2017. = European Union, Iceland, Liechtenstein and Norway) - Annex 14a.

16. Designing Privacy

ADO manages change affecting privacy in such a way as to help ensure adequate security of personal data and minimizing their processing.

To this end, the principles of project management and investment by **infraTEAM** They refer to the safety of personal data and minimize requiring assessment of the impact on privacy and data protection, and designed to take into account security and minimize data from the beginning of the project or investment.

Chapter II Administrator of Personal Data, Data Protection Supervisor

Obligations and duties of the Administrator of Personal Data

The entity responsible for data processing is an administrator and he delegates responsibilities of the Data Protection Officer (if appointed) and its employees. On the Administrator of pregnancy legal responsibility for the discharge of their duties in connection with the processing of personal data by him or on his behalf. The primary responsibility of the administrator is to ensure that processing is carried out in accordance RODO Regulation and to be able to demonstrate this. To this end, it has implemented adequate and effective technical and organizational measures:

1) they have known and provide the highest possible at the time of processing data, the level of protection;
2) can not be a one-time action, they are, if necessary, be reviewed and updated;
3) he makes this, taking into account the nature, scope, context and purposes of the processing and the risk of violation of the rights or freedoms of individuals with different probabilities and weighing risks;
4) These measures include the implementation of the data protection policy administrator.

The risk of violation of the rights and freedoms of people with different probability and severity of threats:

1) may be due to the processing of personal data liable to prejudice or physical damage to property or intangible, if the processing:
   a) relates to a large-scale data (a large amount of data);
   b) affects a large number of data subjects, in particular:
      if the processing can result in discrimination, identity theft or fraud relating to identity, financial loss, violation of reputation, violation of the confidentiality of personal data protected by professional secrecy, unauthorized reversal pseudonymisation or any other significant economic or social harm; if the person, the data subject may be deprived of their rights and freedoms or the ability to exercise control over their personal data; if personal data are processed containing information such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, data on sexuality or sexual orientation, biometric data, the genetic code; if the assessed factors are personal to create or use of personal profiles; or if personal data are processed persons requiring special care, in particular children; if the processing relates to large amounts of personal data and affects a large number of data subjects,
2) ADO estimated risk on the basis of objective assessment, in which it is determined whether the processing operations involves risk or high risk.

With regard to the information obligation, the data controller:

1) communicates with the data subjects (individuals) and provide them with information in a concise, clear, understandable and easily accessible,
2) facilitate data subjects to exercise their rights,
3) provide free information to data subjects, including at their request, the time to information by the ADO is a maximum of one month; in complicated cases this period may be extended to two months,
4) verify the identity of the persons bringing the request for information.

Regarding the rights of the data subject:

1) The ADO confirm whether personal data are processed for a given individual, and if it does, provides information indicated Regulation;
2) facilitates the ability of the data subject to exercise its rights under Article. 15-22;
3) inform the person of the data subject of the action it has taken in connection with its demands based on Art. 15-22;

4) the justification for the rejection of the request of the data subject and teaches about the right action;
5) it allows access to the data to which they refer;
6) rectifies and updated data;
7) removes data;
8) reduces the data processing;
9) notifies of the correction or removal of data or the restriction of their processing;
10) performs the transfer of data.

Database Administrator is required by RODO to:

1. Indicate the legal basis for the lawful processing of personal data.
2. Protection of personal data processed against unauthorized access and takeover by an unauthorized person.
3. Processing data in accordance with the requirements of RODO.
4. Protect data against alteration, loss, damage or destruction.

These tasks should be carried out by:

1. Development of the documentation.
2. Keeping records of persons authorized to process personal data - Appendix 2, including interns, volunteers, trainees, students in data processing**infraTEAM.**
3. Monitoring activities performed on a set of data.
4. Providing technical security measures.

The administrator of personal data in order to ensure the protection of personal data may appoint:

1. Data Protection Supervisor (IOD) - Appendix 12.
2. System Administrator (ASI) - enclosure 13.

Responsibilities and tasks of the DPO (Art. 39 paragraph. 1 RODO)

1. The duties of the EDPS include:
   a. information administrator, a processor and the workers who process personal data, the duties incumbent on them under Regulation RODO and other legislation of the Union or Member States' data protection and advise them on this matter;
   b. monitoring compliance with Regulation RODO, other provisions of Union or Member State data protection and policies of the controller or a processor in the field of protection of personal data, including the allocation of responsibilities, awareness raising activities, training of personnel involved in the processing operations and the related audits;

c. providing on-demand recommendations for the assessment of data protection and monitoring its implementation in accordance with Article. 35;
d. cooperation with the supervisory authority;
e. act as a contact point for the supervisory authority on issues related to processing, including with previous consultation, as referred to in Article. 36, and where appropriate, consultation in all other matters;
f. provide a focal point for data subjects, in all matters relating to the processing of their personal data and the exercise of their rights under this Regulation.
g. keeping a record of the activity or activities register category.

Rights Data Protection Supervisor (IOD)

DPO has the right to:

a) determining, and recommending the enforcement of the tasks related to the protection of personal data throughout the organization;
b) to enter any premises where data files are located and conduct the necessary examination or other checks to assess the compliance of data processing with RODO, demand written or oral explanations to the extent necessary to establish the facts;
c) require the production of documents and data directly related to the subject of control;
d) requests for access to device control, media and computer systems used for data processing;

Obligations and duties of the Administrator Information Systems (ASI)

1. Systems Administrator is responsible for the smooth operation of IT systems, including workstations, server applications, databases, e-mail, their maintenance and implementation of the necessary safeguards to guarantee the security of personal data processing.
2. ASI is responsible for planning, configuring, activating specialized monitoring software for data exchange interconnection of local and wide area network.
3. ASI is responsible for planning and providing anti-virus protection.
4. Inspection and maintenance of the information system should be carried out within the time limits specified by the manufacturer of the system or according to the schedule ASI, but not less frequently than once a year. For the timeliness of carrying out inspection and maintenance as well as their proper course corresponds to ASI.
5. ASI is responsible for optimizing storage resources and server, memory and disks.

6. ASI is responsible for updating the software in accordance with the manufacturer's recommendations and the opinion of the market about the safety and stability of the new version (eg. Updates, service packs, and patches).
7. ASI is responsible for providing licensed software to process personal data.

Chapter III Technical and organizational measures

organizational security

In order to protect personal data, the following organizational safeguards:

1. It was developed and implemented for Personal Data Protection Policy and the Rules of Procedure of the personal data.
2. Processing of personal data shall be admitted only persons having valid authorization for their processing.
3. Is conducted Registry of persons having the authority to process personal data.
4. Persons having authority have been trained or familiar in the field of personal data protection and information system security as noted in Appendix 16.
5. Persons having authority filed a statement of confidentiality of personal data processed - Annex 4.
6. People employed in the processing of personal data are obliged to keep them secret - Annex 4.
7. Processing of personal data is carried out in conditions that protect personal data against unauthorized access.
8. Being unauthorized persons in the area of treatment is possible only in the presence of authorized persons and conditions that ensure the security of personal data.
9. Apply a written agreement for the processing of data in cooperation with subcontractors transforming the personal data.

physical security

In order to protect personal data, the following physical security:

1. Policy and a detailed description of the keys to deal with them - the policy described in the section Keys.
2. Doors to the processing area which is lockable (key policy).
3. Personal data on paper are stored in the furniture indoors or lockable (key policy).
4. In the area of processing and document shredder is available grade of at least P4.
5. Keys, access codes or other security to the areas of treatment are issued to employees processing the data in a specific area of processing. Keys can not share with other employees or unauthorized persons!
6. A detailed list of the issued keys to the areas of processing and is not responsible for the workers is given in Annex 11 and 11a (the list of keys issued ad hoc).

key policy

1. General principles.

Key policy areas include areas of processing of personal data used by infraTEAM in which personal data are processed,

a) list of location areas infraTEAM processing of personal data is given in Annex 23,
b) work schedule areas infraTEAM processing of personal data is listed in Annex 22,
c) access to facilities which are regions of the processing of personal data is possible only through a door designated for that purpose by the ADO. All other doors allowing access to those premises shall be permanently locked. Do not open that door by employees without the consent of ADO
d) spare keys are stored in a specific ADO safe place.

2. Granting of authorizations.
   a) authorization to collect the keys to the rooms which are areas of data processing have only persons authorized by the ADO. They also include access to the premises outside of working hours,
   b) granting / canceling authorization requires a person to register, carried out in the form of Annex 11 and Annex 11 (list of keys issued ad hoc).
3. And issuing heavy reliance keys in normal mode.
   a) the keys to the rooms which are areas of data processing have been issued to employees designated for downloading, ADO, keys to these rooms are under the personal supervision of authorized persons,
   b) the keys to the rooms which are areas of data processing have been issued for downloading by the ADO. The keys to these rooms are under the personal supervision of authorized persons,
   c) keys to sensitive areas (archives) are issued for downloading in ADO, keys to the rooms are specially protected under the personal supervision of authorized persons access to these rooms a third party takes place under strict supervision (!),
   d) authorized employees are obliged to note download and key opinion - Appendix 11 or 11a.
4. And issuing heavy reliance keys extraordinary:
   a) issuing spare keys to authorized employees can only be justified in cases of emergency situations and with the consent of ADO
   b) spare keys after use should be promptly returned to the ADO.
5. Current treatment during the working day:
   a) keys used to protect the desks and cabinets must be clearly described,

b) Keys remain under the supervision of staff, who take full responsibility for their proper protection,
c) prohibited from leaving the keys in the desks and cabinets during a temporary absence of authorized persons in the room,
d) after use, the keys used to protect the desks and cabinets must be stored in the specified ADO adequately protected place, Key collection is protected by the ADO in a certain safe place,
e) After work, employees are required to:
- off and secure electronic and electrical equipment,
- off lighting,
- protection and closing windows and doors,
- leave the blinds,
- optionally an alarm is triggered,
- for compliance w / the principles of current employees are responsible.

6. Policy Violation keys can cause both of the following consequences:
a) incurring liability under Article. 52 of the Labor Code[1].
b) incurring liability under Article. 363 § 1 of the Civil Code[2].

security hardware

In order to protect personal data used security hardware and telecommunications infrastructure described in section Instructions for the management of information systems.

Owner information security management

Policies for securing a computer system, hardware, data and software

Taking into account the categories of processed personal data, connect to the network hardware ICT and the risks introduced in infraTEAM high level of security in the computer system used to process personal data.

1. Subject to control access to the premises, which is hardware, in order to protect personal data and hardware and software prior to use or destruction by third parties. Premises where there is computer hardware used for processing personal data are fitted with sturdy locks. The last of the

[1] **Art. 52 § 1**. An employer may terminate an employment contract without notice the fault of the employee in the event of: 1) a serious violation by the employee of basic employee duties, 2) committed by an employee during the employment contract of crime, which prevents further hiring him to his post, if the offense is obvious or has been confirmed by a final judgment ()

[2] **Art. 363 § 1.**Damages should be, at the option of the victim, or by the restitution or the payment of an appropriate sum of money. the principal difficulties or excessive costs, benefits in cash ()

staff who is obliged to leave the room to lock the door! He runs a written record of the issued keys to the rooms - Appendix 11 and 11a.

2. Computers, which contain personal data must be equipped units (UPS) in the event of voltage fluctuations in the grid in order to properly close all applications and safely turn off your computer, in the case of laptops efficient batteries.
3. Incremental data contained in the system is createdonce a day, and copies holistic once a month. A copy of the comprehensiveis created by ADO / or authorized user of ASI, then protected by ADO / ASI in a safe place.
4. employees **infraTEAM** absolute ban wynoszenia discs or other storage media with software or other data outside the residence of the entity and its organizational units, unless permission for such action is expressed by the ADO.
5. It is allowed, with the consent of ADO installing programs containing personal data on mobile computers. However, it must have installed protection mechanisms and comprehensive anti-virus software. In addition, such a computer user must be familiar ADO / DPO (if appointed) of all threats and keep every effort to prevent the theft of his laptop computer - see:**Terms of use of portable computers.**
6. Devices, disks or other media information for:
   a) liquidation - deprives the data by formatting and physical damage, preventing reading them,
   b) transfer - deprives a record containing personal data,
   c) repair - deprives the recording of personal data or repairs under the supervision of the ADO / ASI or persons authorized by the ADO.
7. At workplaces where personal data are processed monitor screens should be set in such a way that third parties insight into the information displayed.
8. In case of interruption of work is used "screen saver" password protected. Time-saver was defined in the Regulations.
9. Each of the computers is password-protected access to the operating system, consisting of at least eight characters and contain uppercase and lowercase letters, numbers and special characters. Each employee is required to change passwords monthly access to your computer.

password Policy

1. All computers, including laptops and server are password protected.

2. Each authorized user logs on to the system with a password to your account on the level of security specified by the ADO as high (built password of eight characters, including large and small letters, numbers, special characters).
2. Change the password to the system takes place not less frequently than every 30 days, and immediately if you suspect that the password could be disclosed.
3. If the password change does not force the system to change the password is required by the user.
4. The user of the system while working in an application can change your password.
5. Passwords can not be commonly used words. In particular, do not use passwords as: dates, names, names, initials, car registration numbers, telephone numbers.
6. You agree to keep your password confidential, even after the loss of their validity.
7. It is forbidden to store passwords in a transparent manner and communicate them to others.
8. This password policy also includes interns, volunteers, trainees, students in data processing infraTEAM.

Rules for safe use of IT equipment desktop

1. IT equipment used for the processing of personal data consists of computers, laptops, printers.
2. User is obliged to use the IT equipment in a manner consistent with its purpose and protect it against any destruction or damage.
3. User is obliged to protect IT equipment against unauthorized access, in particular, are protected contents of display screens.
4. User is obliged to immediately report the loss, loss or destruction of IT equipment entrusted to him.
5. Unauthorized opening (dismantling) of IT equipment, installation of additional devices (eg. Hard disk, memory), or connect any devices not approved by the ADO system is prohibited.

Terms of use of the software

1. You agree to use only software while maintaining copyright protection.
2. You may not copy the software installed on the IT equipment by the ADO for their own needs or the needs of others.
3. Installing the software on any IT equipment it can only be made by the ADO, or a person authorized by him.
4. Users do not have rights without the consent of the ADO / ASI to install or use software other than transferred or made available to them by the ADO / ASI. The ban applies, among others, software installation from purchased CDs, software downloaded from web pages, and automatically responding to emerging Internet advertising.

5. Users do not have the right to change the system parameters that can only be changed by ADO / ASI, or a person authorized by the ADO.
6. In case of violation of any of the above provisions of the ADO has the right to immediately and without notice to remove illegal or improperly installed.

Rules for Internet use

1. User is obliged to use the Internet for business purposes.
2. It is forbidden to rip to your hard drive and runs any illegal programs and files downloaded from an unknown source. Such files should be downloaded only by the consent of the respective ADO / ASI and only in justified cases.
3. You are responsible for damages caused by the software installed from the Internet.
4. It is forbidden to enter the pages where the presented information about criminal hacking, pornographic, or other prohibited by law (on most pages of this type of malicious software is installed, automatically infect the computer's operating system).
5. Do not options in your web browser options enable autocomplete forms and remembering passwords.
6. If you use an encrypted connection through the browser, you should pay attention to the appearance of the respective icon (lock) and a Web address beginning with the phrase "https:".
7. Caution should be exercised in the case of a request or request a code, PINs, credit card numbers over the Internet. This particularly applies to requests such information by giving a reputed bank.
8. Users can not also use the Internet for private purposes, except with the consent of ADO and it should be kept to a minimum.
9. Using the Internet for private purposes can not affect the quality and quantity of work provided by the user and the correct and reliable performance of his official duties, as well as the performance of the system the employer.
10. When using the Internet, users are required to observe the industrial property rights and copyright law.
11. To the extent permitted by law, the ADO reserves the right to control how the use of the Internet for the above rules.
12. In addition, reasonably, ADO reserves the right to control the time spent by a user on the Internet.
13. The employer can also block access to certain content available via the Internet.

Rules for the use of electronic mail

1. Transferring data using the mail can take place only by persons authorized to do so by the ADO.
2. In the case of transfer of personal data outside infraTEAM must use cryptographic mechanisms (uploaded files with passwords, a trusted profile, qualified certificate).
3. In case of password protection of files, apply a minimum of 8 characters: uppercase and lowercase letters and numbers or special characters and password, please send a separate e-mail or any other method, eg. By telephone or SMS.
4. Users should pay particular attention to the correct address of the recipient of the document.
5. It is recommended that the user when transferring personal data entered into the content of e-mail request for confirmation of receipt and read the information by the addressee.
6. Do not open attachments (files) in e-mails sent by an unknown sender or suspicious attachments granted by a known consignor.
7. Users can not distribute via e-mail information about the risks for the system, "chain letters", etc.
8. Users should not send out e-mails containing attachments with large size.
9. Users should periodically delete unwanted e-mails in the mail business.
10. When sending emails to multiple recipients at the same time, use the method of "blind carbon copy - bcc" (e-mail function allows you to send messages to multiple recipients, so that they did not see each other's addresses).
11. Mail is designed to perform duties.
12. Users do not have the right to use e-mail for private purposes, except with the consent of the ADO only occasionally and should be kept to a minimum.
13. Using e-mail for private purposes can not affect the quality and quantity of work provided by the user and the correct and reliable performance of his official duties.
14. When using e-mail, users are obliged to observe the industrial property rights and copyright law.
15. Users do not have the right to use the mail to disseminate content that is offensive, immoral or improper to the generally applicable rules of conduct.
16. A user without the consent of the ADO has no right to send messages containing personal data relating to the Employer, its employees, customers, suppliers or business partners via the Internet, including using personal electronic mailbox.

antivirus protection

The aim of the procedure is to protect systems from malicious software (eg. The type of worms, viruses, Trojan horses, rootkits), and unauthorized access to personal data processing systems.

1. Users are obliged to scan files from external media introduced anti-virus program.
2. On computers and laptops Virus was installed, and the employees were trained in its use, Annex No 17.
3. It is forbidden to disable antivirus system while the system processing personal data.
4. Virus provides protection: operating system, stored files, incoming and outgoing mail.
5. Updating virus definitions is done automatically by your antivirus program.

System security against unauthorized access

Safeguards are used to protect information systems against unauthorized access to the local network, eg. By spyware, hackers.

1. For planning, configuring, activating specialized monitoring software for data exchange interconnection of local and wide area network corresponds to the ADO / ASI.
2. Firewall is used.
3. Mechanisms used to control access to the network.
4. Wireless network is properly secured.
5. It is allowed to join the Web to a system in which personal data are processed under the following conditions:
   a) on each computer workstation must be installed antivirus software,
   b) every email entering the unit must be checked for viruses,
   c) forbidden to use devices of unknown origin without first checking their antivirus software, which is user intending to use it,
   d) It prohibited from downloading Internet files of unknown origin, and reading e-mail attachments without first checking their antivirus software.

1. Each user of the system must be trained to use antivirus program, which certifies the appropriate signature, in accordance with the**Annex 17** to this security policy.
2. ADO / ASI carries out regular checks on all computers anti-virus system.
3. System users are responsible for not sharing jobs to outsiders.

Procedures for the inspection and maintenance of systems and information media used for the processing of personal data

1. The procedures for repair of computer equipment:

and) repair of computer equipment operated in the system can take place at the headquarters of **infraTEAM** and it can only make designated employee orspecialized IT company. These activities must be carried out in the presence of ADO / ASI or other authorized user of the system by the ADO,

b) repair of computer hardware in the system operated outside the headquarters office must be preceded by the removal of any hard disk databases, records and files containing data of a personal nature. ADO / ASI or the designated employee is responsible for creating a copy of the database, which is stored by the ADO / ASI in a safe place. After returning from the service computer hardware, databases, registers, files are reinstalled.

2. The procedure for review of the system:

and) review of the system makes ADO / ASI

b) AND TO (ASI has been called upon) support unit in terms of information technology,

c) Inspection activities carried out by an external company must be carried out in the presence of ADO, ASI, or other employee authorized by him.

Proceeding with the electronic media containing personal data

1. Electronic media include hard disks, removable hard drives, external hard drives, pen drives, CDs, DVDs, Flash memory.
2. Each carrier should be described in a way that uniquely identifies it. List of electronic media is given in Annex No. 26.
3. Users can not be externally removable electronic media with stored personal data without the consent of the ADO.
4. Personal data taken out of the organization must be encrypted.
5. In case of damage or wear media containing personal data, it needs to be physical destruction or permanent removal are on the data.
6. Transfer of media of personal data should be carried out with regard for safety. The recipient should be informed about the shipment and the consignor shall make a copy of the transmitted data. The recipient should notify the sender of the receipt of the shipment. If the sender has not received confirmation, the addressee claims not received the shipment, a user who is the sender should inform about the situation ADO / DPO (if appointed).

The procedure for personal data storage media in the paper and electronic versions:

1. The data carriers such as:

b) laptop,

c) cell phone / smartphone

d) pen drive / memory card,

e) external hard drive

f) CD / DVD / BR,

g) paper printouts

are stored in a manner to prevent access to persons not authorized and to protect them against damage caused by flooding .: eg, burning, melting, etc.

2. Persons authorized are required for permanent destruction / erasing personal data after the termination of the processing.
3. It is forbidden to wynoszenia personal data outside the processing without the consent of the ADO, and in the case of receipt of such approval to provide at least the same conditions of security of the processing of personal data in force in the area of processing.
4. Personal data sent electronically outside the processing area must be password protected or encrypted.
5. In the case of the transmission media of personal data outside of the organization, use the following safety rules:
   a) the recipient should be informed of the shipment,
   b) The consignor shall make a copy of the transmitted data,
   c) before sending the data should be encrypted and password provided to the addressee by a different route,
   d) use safe deposit envelopes,
   e) the recipient should notify the sender of the receipt of the shipment.
7. Users are obliged to immediately and permanently delete / erase data from the media after the termination due to storage (unless because of separate provisions should be maintained for longer.)
8. Affected winding damaged or obsolete carriers, especially hard disks personal data are collectively destroyed physically / g enclosure 27.
9. Information carriers mounted IT equipment, in particular the hard drives of personal data should be removed or cleaned specialized software, before being transferred outside the organization (eg. The sale or donation of desktops / laptops).

Securing documents and prints

1. Documents and durable printouts with personal data stored in an archive or physically protected areas, desks and cabinets.
2. Employees are required to secure documents (eg. The closure of the premises, the key closing documents in cabinets, desks) from unauthorized access during his absence from the premises or after work (ie. A clean desk policy).
3. It is forbidden to leave printing and photocopying printers, scanners and copiers without supervision.

4. Employees are required to destroy documents and temporary prints shredder immediately after the termination of the processing.
5. For ensuring the security of documents and prints all employees are responsible.

Handling of personal data in paper

1. For the security of documents and printouts containing personal data are the responsibility of authorized persons (users).
2. Documents and printouts containing personal data are stored physically in rooms protected against unauthorized access.
3. Users are required to use "clean desk policy". It involves securing documents, for example. In cabinets, desks, premises against theft or access by unauthorized persons.
4. Users are required to carry documents in a way that prevents the theft, loss or loss.
5. Users are required to document destruction and temporary prints shredder immediately after the termination of the processing.

Terms of use of portable computers

1. Every laptop user should refer to the Regulations of use portable computers.
2. If you store on your laptop or personal information constitutes a trade secret infraTEAM, the user is required to store them on disk encrypted, secured at least 8 character password (large, small letters, numbers and special characters).
3. On a portable computer designed for external multimedia presentations should not, as far as possible, be personal information or a trade secret infraTEAM**.** In the case of lost or stolen laptop, you should immediately notify the ADO, noting at the same time, what kind of data was stored on the device.
4. User is obliged to protect the laptop during transport and in particular:
    1. it is recommended to move it in a special case,
    2. forbidden to leave the laptop in the car when in a public place without supervision,
    3. while driving a car is recommended to keep the laptop in the driver's seat. The carrying it, for example. On the seats, which can result in theft at intersections, pedestrian crossings or in traffic jams.
5. If the laptop is left in a place accessible to unauthorized persons, the User is obliged to use the security cable. In particular, the computer security at the workplace, during conferences, presentations, seminars, trade fairs, etc.
6. In the case of leaving laptops in the office it is advisable to place them after working in locked cabinets.

7. Laptop user is obliged to regularly backup the data on the server or on specific media (USB stick, CD, DVD). Holders of such copies should be kept in a safe place, including protection against unauthorized access unfitch.
8. Working on a laptop in public places and transport, the User is obliged to protect the information displayed on the monitor against access by unauthorized persons.

Principles of data sharing

1. Allows the transfer of personal data referred to in Article. 6 RODO operators and bodies authorized under separate regulations.
2. Model application for access to personal data referred to in point. 1 of the enclosure 21.
3. ADO / DPO (If appointed) It is obliged to keep records sharing of personal data from the collection in accordance with Annex 14.

Procedure in case of violation of security policy.

1. Any person processing personal data, in case of suspected breach of security of personal data, it shall immediately inform the DPO and the ADO (if appointed).
2. ADO / DPO (If appointed) upon receipt of notification:
   a) checks the status of devices used to process data,
   b) look at the behavior of programs (including computer viruses)
   c) checks the quality of communication in a telecommunications network
   d) checks the contents of the personal data file,
   e) analyzes the methods of work of persons authorized to process personal data.
   f) if the incident could affect the violation of the rights and freedoms of the individual reporting the incident to the fact that the supervisory authority within 72 hours of being informed about the incident.
   g) If the incident relates to data entrusted by another ADO reports that the incident competent ADO within 24 hours.

3. In the event of a breach of data security administrator:
   b) take the necessary measures to prevent further violations of their (disconnection of defective devices, block access to the telecommunications network, programs and data files, etc.)
   c) in order to prevent or restrict access to personal data of unauthorized take appropriate steps through: physical disconnection of devices and network segments, which would allow access to the database for an unauthorized person log off a suspected violation of data protection safeguards, change the password for the administrator account and the user, by which were obtained illegal access in order to prevent any re-attempts to compromise.

d) protects, preserves all information and documents that may assist in determining the causes of the violation,
e) immediately restores normal operating status of the system,
f) analyzes the state of security with an estimate of the size of the damage caused by violations,
g) draw up a detailed report containing in particular: the date and time of receipt of information about the violation, the description of its course, the reasons and conclusions of the event.

3. The report, together with any attachments (copies of evidence documenting the violation) joins ADO documentation of the incident.
4. ADO / DPO (If appointed) shall take the necessary measures to eliminate violations of data security in the future, in particular:
   b) if the cause of the event was the technical condition of the device, method of operation of the program, the activation of a computer virus or communication quality in a telecommunications network, immediately carry out inspections and maintenance of equipment and programs, determine the source of the virus and implements effective antivirus protection, if necessary, contact your service provider telecommunications
   c) if the cause of the event was defective methods of work, errors and omissions of persons employed in the processing of personal data carried out additional courses and training of people involved in the processing of data, and to persons guilty of negligence applies to the administrator of personal data to draw the consequences provided for by law,
   d) if the cause of the event is illegal act or there is suspected, notify law enforcement authorities.

The procedure start, suspension and termination of work that requires the processing of personal data:

1. The authorized person logs on to the system and computer program processing personal data using the login and password.
2. Authorized person is obliged to inform ADO / DPO (If appointed) unauthorized attempts to log on to the system or program, or a program if the system monitors such phenomena.
3. Authorized person is required to prevent access to personal data displayed on the screen or on paper to unauthorized persons.

4. The person authorized to process personal data is required in the course of time out of work to run a password-protected screen saver or log off the system and remove the printouts with personal data from the desk.
5. After working authorized person is required to log off or shut down your computer and remove any desktop media containing personal data and protect premises against intrusion, flood, fire, etc.

The procedure for creating and storing a backup

1. Backup (incremental, comprehensive) creates ADO / ASI - if it has been appointed, or authorized personnel, as described in point. 3 Rules protecting hardware, data and software of this manual.
2. Backups of personal data in the electronic version can be stored on an external data carrier secured in accordance with organizational security described in point. 3 Rules protecting hardware, data and software of this manual.
3. The person making backups is required to mark them and check the consistency of data and the possibility of their replay.
4. After a period of storage backups are permanently destroyed or rendered anonymous.

Procedure for and disclosure of personal data to third parties:

1. Each introduction and sharing of personal data must be made in accordance with both RODO and this document and have a legal basis.
2. This leads to shared data records, specifying in particular:
    a. date available,
    b. name and surname of the person whose data available (medical records)
    c. person, entity, to whom the data available,
    d. way to share,
    e. range of available data that has been provided,
    f. name of the person whose personal data have been made available, the name of the authorized authority or body,
    g. the name of the employee who made available the personal data.

Control procedures and staff training:

1. Every year, carried out checks compliance with applicable rules on the protection of personal data.

2. With inspection report shall be drawn up, which is the basis for the update procedures, and this document.
3. Once a year, the update is carried out training in the protection of workers personal data.
4. Each employee prior to being authorized must be trained.
5. Any repair or maintenance of computer hardware containing personal data or premises constituting the processing area can be done only under the supervision of authorized persons.

disciplinary proceedings

1. Cases of unjustified abandonment obligations under this document will be treated as serious misconduct. A person who, in the event of a breach of security system or the presumption of such a breach has not taken action referred to in this document, in particular, had not notified the appropriate person in accordance with certain rules and, if not implemented appropriate action documenting the case, you can bring disciplinary proceedings .
2. Disciplinary punishment, imposed on a person repealing the notification does not exclude criminal liability of the person and the possibility of bringing the case to the civil action by the employer to compensate the losses incurred.

manual alarm

Manual defines the catalog of threats and security incidents of personal data and describes how to respond to them. The aim of the guide is to minimize the impact of security incidents, reducing the risk of occurrence of threats and incidents in the future.

1. Each employee infraTEAM in case of any threat to the protection of personal data is obliged to inform the ADO / DPO (if appointed).
2. Typical threats to security of personal data include:
   a) inadequate protection of physical facilities, equipment and documents,
   b) inadequate protection of IT hardware, software against leakage, theft and loss of personal data,
   c) failure to comply with data protection rules by the employees (eg. non-application of the principle of clear desk / screen, password protection, unlocked rooms, cabinets, desks)
3. Typical security incidents of personal data include:
   a) random external event (fire object / premises, flooding, loss of power, loss of communications).
   b) internal random events (server failures, computers, hard drives, software, mistakes specialists, users, loss / loss data)

c) intentional incidents (breaking into a computer system or premises, stealing data / equipment, information leakage, unauthorized disclosure, deliberate destruction of documents / data, viruses and other malicious software)

4. In case of an emergency, ADO / DPO (if appointed) leads the investigation in the course of which:
    a) determine the scope and causes of risk and its possible consequences,
    b) The proceedings documents,
    c) sets the time of the infringement, its scope, causes, consequences, and the amount of damage that occurred,
    d) protects any evidence,
    e) determine the persons responsible for the breach,
    f) take corrective action (removes the effects of the incident and the damage is limited)
    g) initiates disciplinary
    h) It draws conclusions and recommends corrective actions aimed at the elimination of similar incidents in the future,
    i) state that a breach of personal data protection supervisory authority within 72 hours from when the infringement.

The procedure for corrective and preventive actions

1. The aim of the procedure is to organize and present activities related to the initiation and implementation of corrective and preventive actions resulting from the occurrence of security incidents or threats to personal data protection system.
2. The procedure for corrective and preventive action includes all those processes in which security incidents or threats may affect the conformity with the requirements of RODO, as well as the proper functioning of the system of protection of personal data.
3. The person responsible for supervision of the procedure is the ADO / DPO (if appointed).

definitions

1. **Incident** - breach of information security because of the confidentiality, availability and integrity.
2. **Danger** - the potential for an incident
3. **Correction** - action to eliminate the effects of the incident.
4. **corrective action** - it is an activity carried out in order to eliminate the cause of the incident or other undesirable situation.
5. **preventive action** - this is the action that should be taken to eliminate the causes of potential hazards or other undesirable situation.

6. **Control** - systematic, independent and documented evaluation of the effectiveness of the protection of personal data, based on statutory requirements, data protection policy.

Description of activities

1. (ADO if DPO has been appointed) is responsible for the analysis of security incidents or threats to personal data protection. Typical sources of information on incidents, threats or vulnerabilities are:
   a) applications from employees,
   b) knowledge ADO / DPO,
   c) audit results.
2. If the ADO (DPO when he was appointed) considers it necessary to take corrective or preventive actions, determine: the genesis of the incident, or threat thereof, the scope of corrective or preventive deadline, the person responsible.
3. (ADO if DPO has been appointed) shall be responsible for the correctness and timeliness of implemented corrective or preventive actions.
4. After completion of corrective or preventive ADO (IOD if it has been called) is required to evaluate the efficiency of their use.
5. The above steps (ADO if the DPO has been appointed) records in the file attachment No. 9.

The audit of the protection of personal data

1. The aim of the procedure is to organize and present activities related to the monitoring of the security of personal data.
2. The procedure involves all the processes of the organization, where the principles of protection of personal data is required.
3. For the control of personal data protection is authorized (ADO if the DPO has been appointed).
4. Be checked:
   a) systems processing personal data,
   b) physical security,
   c) organizational safeguards,
   d) personal safety and compliance with the requirements of the facts RODO.

e) (ADO if DPO has been appointed) is preparing a plan for the control of the scope and the necessary physical resources, time and personnel. The inspection should take place at least once every six months.

f) Control is carried out on the basis of an audit of compliance with RODO - Appendix 1.

g) Following the control ADO (IOD if it has been called) establishing a monitoring report, Appendix 19 - on the basis of ADO (IOD if it has been set up) initiates corrective or preventive action.

The annual report system state protection of personal data

1. Once a year (ADO if the DPO has been appointed) prepare an annual report on the state of operation of the system of protection of personal data (audit).
2. The report is prepared in Annex 18.

Staff training

1. Each user before allowing to work with the computer system processing personal data or sets of personal data in paper form should be subjected trained or familiar with the policy of protection of personal data.
2. For training or read the privacy policy corresponds to the ADO (DPO when he was appointed).
3. The scope of training RODO should include provisions, documentation of data protection (Regulations) and safety rules applicable in the system ADO, and a commitment to comply with them. The detailed scope of training, together with the attendance list is given in Annex No. 16.
4. After the training, or having regard to the policy of protection of personal data, the user is required to sign a declaration of confidentiality - Annex 4.
5. This document is stored in the personal file or user documentation for the protection of personal data and provides the basis to take action in order to give employees permission to use the computer system processing personal data.

Chapter IV Procedures to ensure the security of personal data

The procedure for granting authorization to the processing of personal data:

1. Each user of the system prior to the processing of personal data must read the following documents:
   a) Regulation of the European Parliament and of the Council (EU) 2016/679 of 27.04.2016 r. On the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46 / EC (General Data Protection Regulation) (OJ L 119, p. 1) - Annex 28,
   b) Rules of protection of personal data.
2. Getting familiar with these documents user confirms the signature on the statement, which is enclosed 16.
3. Authorization to the processing of personal data gives AND TO.

4. Processing of personal data can only be made by an authorized user of the ADO. Authorization pattern is attached as Appendix 3.
5. Before granting authorization for personal data processing employee is trained to protect them and familiar with the safety system.
6. A person is authorized to process personal data signed a declaration of confidentiality of personal data to which he has access - Annex 4.
7. Conferral of access to the system is the introduction of the system by ADO / ASI for each system user a unique identifier indicating the range of available data and operations. The password is changed manually or semi-automatically every 30 days by authorized persons.
8. Password first log in the system sets the ADO. Each system user is required to change it for individual, an eight-character password with uppercase and lowercase letters and numbers and special characters.
9. Authorized Person undertakes to maintain the confidentiality of the password to access personal data and its immediate change in the event of disclosure.
10. Do not store the password in an open or transfer it to other people.

Responsibility.

1. The system user is entitled to exercise only those activities for which it was authorized.
2. User bears all responsibility for all operations performed using the ID and password except when ADO will use the user's password in his absence. ADO is required to draw up a protocol of this event, which is familiar with the system user whose password has been used. After hearing protocol, user is required to make an immediate change password and pass them ADO.
3. Any crossing or attempting to cross any allowances allocated, will be treated as a violation of basic employee duties.
4. ADO can receive permission from the date of the employee and the reasons for receiving allowances.
5. Password, and user permissions system which they had lost, should immediately de-register with the system. Deregister from the system performs ADO / ASI.
6. The user of the system employed in the processing of personal data is obliged to keep them confidential, and make every effort to ensure that personal data are not transferred to unauthorized persons.

User registry.

1. (ADO if DPO has been appointed) is obliged to keep the register and protect users and their rights in the system.
1. The register must reflect the current state of the system in terms of users and their rights and to enable the viewing history of changes in the system.
3. Log - Appendix 2 - comprises:
   and) your name,
   b) user ID,
   c) range of powers
   d) the date of posting permissions,
   e) date of receipt of allowances,
   f) cause revoke the authorization
   g) ADO signature.

Chapter V Final

1. **Personal Data Protection Policy is an internal document and can not be made available to third parties in any form.**
2. Any procedures and rules described in this document are followed by persons authorized to process personal data with particular focus on the good of the data subject.
3. Entrusting the processing of personal data to an external entity may be required only by an agreement in writing, provided that the entity meets at least the same conditions of security of the processing of personal data as **infraTEAM**- enclosure 20.
4. ADO / DPO is required to read the contents of the Data Protection Policy of each employee's personal data processing**infraTEAM.**
5. All regulations concerning information systems, as defined in the Policy for Personal Data Protection also apply to the processing of personal data in databases maintained in any other form.
6. Users are obliged to observe the processing of personal data of the provisions contained in this Policy for Personal Data Protection.
7. Cases of unjustified abandonment obligations under this document will be treated as serious misconduct.

8. A person who, in the event of a security breach or system presumption of such breach has not taken action referred to in this document, and specifically advised ADO / DPO (if appointed) can bring disciplinary proceedings.
9. Disciplinary punishment imposed on a person repealing the notification does not exclude liability in accordance with RODO and the possibility of bringing the case to the civil action by the employer to compensate the losses incurred.
10. In matters not covered by this Policy for Personal Data Protection rules apply Regulation of the European Parliament and of the Council (EU) 2016/679 from 27.04.2016 r. on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46 / EC (General Data Protection Regulation) (OJ L 119, p. 1).