Videofonika spółka z ograniczoną odpowiedzialnością spółka komandytowa

Personal Data Protection Policy

confidential document

Kancelaria Pałucki & Szkutnik

2019-04-30

Table of Contents

Preamble

This Policy on Personal Data Protection at Videofonika sp. Z o.o. sp.k. developed based on the provisions of the Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of natural persons in connection with processing of personal data and on the free movement of such data; and the repeal of Directive 95/46 / EC, based on an audit carried out and based on an analysis risk.

The Personal Data Protection Policy is a set of documents defining the rules concerning security in the protection of personal data processed traditional and IT methods.

The most important pillars of personal data protection in the Company are:

Legality - The company cares for privacy protection and processes data in accordance with the law.

Security - The company ensures an appropriate level of data security by undertaking

constantly working in this area.

Rights of Units - The company enables people whose data it processes to perform its own

he pursues these rights and rights.

Accountability - The company documents how it performs its duties to make it at anytime

be able to show compliance.

The company processes personal data respecting the following principles:

a) based on the legal basis and in accordance with the law (legalism);

b) fairly and honestly (fairness);

c) in a transparent manner for the data subject (transparency);

d) for specific purposes and not for "spare" (minimization);

e) no more than necessary (adequacy);

f) with care for the correctness of data (correctness);

g) no longer than necessary (temporality);

h) ensuring adequate data security (security).

Respect defined in The Policy of Personal Data Protection is based on the principles of the basis of data processing.

PART I OF PERSONAL DATA PROTECTION POLICIES

Chapter I General provisions

Subject of regulation

§ 1.

1. The data protection policy defines the rules for processing and protection of personal data in Videofonika sp. o.o. sp.k. according to with the requirements of the Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of individuals in due to the processing of personal data and regarding the free matter the flow of such data and the repeal of Directive 95/46 / EC.
2. This document is the fulfillment of the obligation referred to in art.24 sec. 2 GDPR.
3. The policy is applicable to all processing processes personal data in the Company.
4. The policy is applicable to all activities constituting processing of personal data, regardless of the source data, their scope, purpose of the meeting, method of processing and period processing.
5. The policy applies to the data entrusted Administrator to be processed on the basis of a contract of entrustment processing personal data or other legal instrument, and to personal data that have been made available to the Administrator.
6. The obligation to protect personal data processed in the Company, including the sole obligation to comply with this Policy applies to all people who have access to them regardless of their occupancy position, place of work as well as legal form work benefits. The above means that Policy is applicable to all persons authorized to process personal data, both employed in the Company under a contract of employment and providing services to it on the basis of a civil law contract or also on a different legal basis (in particular for trainees, volunteers, apprentices).
7. Any person who as part of their official duties he processes personal data, he can process it only on the basis of authorization received.
8. Every person processing personal data in the Company is obliged to get acquainted with the Policy and other documents related to it, and to use the regulations they contain. A person who became acquainted with By policy, you must submit your signature with the date under the declarations constituting Annex No. 1 to the Policy.
9. The policy should be interpreted in accordance with the currently binding ones regulations. Any interpretation doubts should be resolved in full respect of the rules on the protection of personal data indicated in the Policy Preamble.
10. Where it is not possible to unambiguously determine the required one with the rules of conduct, a solution should be applied providing more complete protection for the processing of personal data.
11. Supervision of the Policy update shall be exercised by the Inspector and in his case not directly administrator. Policy update should take place in particular in the event of a change in regulations, issue new guidelines of the supervisory body or the European Protection Council Data or when it turns out that the current provisions of the Policy remain inadequate to the level of risk required in the Organization.
12. The company approves by way of resolution / order of the Policy and its updates.

Definitions

§ 2.

The phrases appearing in this Policy mean:

1) Personal Data Administrator (ADO, Administrator or interchangeably Company, Organization) - Videofonika spółka z ograniczoną odpowiedzialnością spółka komandytowa with its registered office in Trzebinia, ul. 32-540, entered in the Register Entrepreneurs of the National Court Register under KRS number: 0000545410, with a NIP: 6282263617.

2) IT System Administrator (ASI) - a person designated by Administrator to care for the IT system, administration and IT environment management in the Organization.

3) Personal information - all information regarding the identified or an identifiable natural person. Possible for identifying a natural person is a person who can be directly or indirectly identify, in particular on the basis of an identifier such as your name, ID number, location data, Internet identifier or one or more specific factors defining physical, physiological, genetic, psychological, economic, cultural or social identity of a natural person.

4) sensitive personal data - specific categories of data specified in art. 9 GDPR, including: data revealing racial or ethnic origin, views political, religious or ideological beliefs, belonging to trade unions; genetic data, biometric data processed to uniquely identify a natural person; data on the health, sexuality or sexual orientation of the person; how also personal data concerning convictions and infringements the rights referred to in art. 10 GDPR.

5) Password - a string of letters digital or otherwise known only the person authorized to work in the IT system.

6) Identifier - a string of letters, digits or other characters uniquely identifying the person authorized to process personal data in the IT system.

7) Data Protection Officer (Inspector, IOD) - a person designated by Data Administrator based on art. 37 GDPR, which carries out tasks monitoring compliance with data protection regulations in The company referred to in art. 39 THE GDPR.

8) Data integrity - a property that ensures that personal information is not they have been modified, removed, added or destroyed in a way unauthorized.

9) Organizational cell (KO) - Department, Department, Team, independent position - resulting from the organizational structure adopted in the Company.

10) Breach of personal data protection - breach of security leading to accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data sent, stored or otherwise processed.

11) Area of personal data processing - rooms or parts rooms in all company locations in which they are processed personal data, both in paper form and in IT system.

12) Recipient of data - an entity to whom personal data is provided.

13) Authorized person - a person authorized to process data personal data by the Administrator or a person authorized by him, having direct access to data processed in the system IT or paper documentation.

14) Third country - a country not belonging to the European Area Economic.

15) Processing entity (Processor) - an entity entrusted by the Company activities to process personal data on your behalf.

16) Personal data protection policy (Policy) - this document constituting a set of regulations and procedures in force in the Organization, created to ensure the lawful processing of data personal information.

17) Data privacy - a property that ensures that data is not shared to unauthorized entities.

18) Profiling - means any form of automated processing of personal data, which consists in the use of data personal data for the assessment of certain personal factors of a natural person, in in particular to analyze or forecast aspects relating to effects work of this natural person, its economic, health and personal situation preferences, interests, credibility, behavior, location or movement.

19) Processing of personal data - operation or set of operations performed on personal data or sets of personal data in an automated or non-automated way, such as: collecting, fixing, organizing, organizing, storing, adaptation or modification, downloading, browsing, exploitation, disclosure by sending, disseminating or other types of sharing, matching or merging, limiting, removal or destruction.

20) PUODO (supervisory body) - President of the Office for Personal Data Protection with headquarters in Warsaw.

21) GDPR - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with processing of personal data and on free movement such data and the repeal of Directive 95/46 / EC (general data protection regulation).

22) Accountability - a property that ensures that the Administrator is able show that the methods he uses are compliant with the GDPR and effective.

23) Telecommunications network - telecommunications network within the meaning of art. 2 point

35 of the Act of July 16, 2004 - Telecommunications Law.

24) Workstation - a stationary or portable computer included in the set an information system that allows users to access data personal data in the system.

25) Teletransmission - sending information via the network telecommunications.

26) UODO - the Act of 10 May 2018 on the Protection of Personal Data (Dz. U. of 2018, item 1000).

27) Authentication - an action aimed at verifying the declared one the identity of the subject.

28) User - a person authorized to process personal data in IT systems that have been assigned an ID and granted password.

29) Personal data resource - all personal data, regardless of how they are fixed, both in electronic form - in the system information and media (CD / DVD / BD, flash memory and other), as well as paper, processed by KO / Company in order to implement it tasks.

30) Personal data file - an ordered set of personal data available according to specific criteria, regardless of whether the set this is centralized, decentralized or functionally distributed or geographically.

Chapter II. Management of personal data processing and their security

Persons responsible for data processing

§ 3.

1. For the processing of personal data and their protection in accordance with the provisions of the GDPR, the UODO, the provisions of sectoral laws and Policies, answer:
    a) Administrator,
    b) Data Protection Officer,
    c) IT system administrator,
    d) managers of organizational units,
    e) e) persons authorized to process personal data.
2. If the Inspector has not been appointed in the Organization, then the provisions referring to the Inspector shall apply accordingly to the person whom responsibilities in the field of personal data protection have been assigned.
3. If the System Administrator has not been designated in the Organization information, the provisions relating to ASI apply according to the person who has been assigned care responsibilities over the IT system, its administration and management IT environment in the Organization.
4. If the person referred to in paragraph 1 has not been appointed in the Organization 2 or 3 above, the tasks and responsibilities in this area are carried out by the Administrator.

Responsibilities of the Administrator

§ 4.

1. The administrator in the processing of personal data is responsible for:
    1) providing appropriate organizational and technical resources for the purpose of processing personal data in accordance with the requirements specified in GDPR rules for the processing of personal data,
    2) implementation of appropriate procedures for the protection of personal data,
    3) use of approved codes of conduct or approved certification mechanisms as an element for confirmation of the Company's compliance with the obligations imposed on it responsibilities where it deems it necessary,
    4) providing means to enable the proper implementation of rights data subjects,
    5) keeping a register of personal data processing activities,
    6) keeping a register of processing categories made in behalf of another administrator,
    7) cooperation with the supervisory body,
    8) implementation of appropriate organizational and technical measures,to ensure a degree of security corresponding to the existing one the risk of violating the rights or freedoms of data subjects,
    9) notification of a personal data protection breach supervisory body, and where appropriate Premises, reporting to the data subject
    10) registering any breaches of personal data protection, including documenting the circumstances of the infringement, its consequences and remedial actions taken,
    11) providing adequate resources for evaluation the effects of planned processing operations for data protection personal data in a situation where a given type of processing can cause a high risk of violating the rights or freedoms of persons

physical, including where appropriate prerequisites, consultation with the supervisory body,

12) granting authorizations for processing personal data and keeping records of persons authorized to process personal data,
13) ensuring the legality of transferring personal data to third parties,
14) ensuring that the Inspector is properly and promptly included in all matters relating to the protection of personal data and supporting IOD in fulfilling its tasks by providing necessary resources to perform these tasks and access to personal data and processing operations,
15) to ensure that the Inspector does not act under pressure and he did not receive instructions on how to perform his tasks, as well as publication of contact details of the IOD and notification of supervisory body.

2. The Administrator's duties include in particular:
   1) ensuring the legality of personal data processing, and in particular, to ensure that:
      a) the consent of the data subject has been obtained another condition allowing processing of data has been met personal,
      b) the information obligation has been met in respect of the person whom data concern,
      c) data has been processed in accordance with applicable regulations law, good practices and social norms,
      d) data was collected in a designated, legitimate purpose,
      e) the data was factually correct and the scope of the data was adequate to the purpose of collection,
      f) the data was processed with a time limit.
   2) keeping documentation describing the method of data processing personal information.
   3) allowing only the possessing person to process the data authorized and / or trained in the field of data protection personal, issuing and managing authorizations, which pattern constitutes Annex No. 2 to the Policy, and keeping and updating records of persons authorized to process data personal data, constituting Annex No. 3a to the Policy, as well keeping and updating the key allocation register to individual rooms constituting Annex No. 3b to Policy.
   4) overseeing and ensuring the lawful transmission of data personal (sharing and entrusting).
   5) respecting the right of data subjects, in particular rights to obtained and information about:
      a) the Administrator and his contact details,
      b) contact details of the Inspector,
      c) the purposes of processing personal data and the basis legal processing,
      d) legitimate interests pursued by Administrator or by third parties,
      e) recipients of personal data or categories of recipients,
      f) intent to transfer personal data to a third country or an international organization,
      g) the period during which personal data will be stored and when it is not possible criteria for determining this period,
      h) the right to request access from the Administrator personal data relating to the data subject, theirs rectification, deletion or limitation of processing or the right to object to the processing, as well as about almost to transfer data,

i) the right to withdraw consent at any time without influence on the lawfulness of the processing that has been carried out on consent before withdrawal,
j) the right to submit a complaint to the supervisory authority,
k) whether the provision of personal data is a requirement statutory or contractual term or the condition of concluding a contract and whether the data subject is obliged to do so applications and what are the consequences of not providing data,
l) automated decision-making, including profiling,
m) another purpose of data processing, if the Administrator plans continue to process personal data for purposes other than the purpose for which personal data has been collected,
n) the source of personal data.

6) respecting the rights of persons whose data relate to:

a) the right to obtain confirmation from the Administrator, whether personal data concerning it is processed,
b) obtain access to personal data and information,
c) the right to obtain a copy,
d) the right to rectify and supplement data,
e) the right to delete data,
f) the right to limit processing,
g) the right to transfer data,
h) the right to object to the processing regarding their personal data,
i) the right not to be subject to a decision which is based only on automated processing, including profiling.

7) conducting regular internal audits compliance with provisions on the protection of personal data.

8) ensuring proper system operation in accordance with the objectives processing of personal data.

9) training of users of the IT system in the field of procedures and instructions that ensure the protection of personal data.

10) explaining all reported irregularities and incidents.

11) performing inspection, maintenance and updating of systems used for data processing

12) ensuring security in a computer network

13) broadcasting, changing or depriving of access to the system IT users

14) supervision of anti-virus protection

15) making backup copies.

3. The administrator appoints the Inspector, if the obligation to designate it results from generally applicable regulations or if it deems it to be necessary for other reasons, taking into account the principles of data protection personal data and respecting the provision of an adequate degree protection of personal data in the Organization.

4. The administrator appoints the Administrator of the IT system, provided that he will deem it necessary.

5. The administrator supervises the activities of the Data Protection Officer and IT system administrator.

6. The administrator each time makes the final acceptance the most important from the perspective of organizing the activities of the Security Inspector data and IT system Administrator in which third parties are involved, while maintaining and respecting full independence of the Inspector.

Verification of the obligation to appoint the Inspector

§ 5.

1. The administrator is obliged to appoint the Inspector always at situations when:

a) processing shall be carried out by a public authority or body, with the exception of courts in the exercise of their judicial system, whereas it is recommended to appoint the Inspector also in situations in which private entities carry out tasks in the interest public or in the exercise of public authority;
b) the main activity of the controller or processor it relies on processing operations that are due to its own nature, scope or objectives require regular and systematic monitoring of data subjects on a large scale; or
c) the main activity of the controller or processor involves large-scale processing of specific categories personal data referred to in art. 9 par. 1, and data personal data on convictions and violations of law, as referred to in art. 10.

2. As of the date of preparing the Policy, the Administrator is not obliged to appointing the Inspector in connection with the lack of updates of the premises referred to in paragraph 1 above. Detailed report verifying existence the obligation to appoint an Inspector is attached as Annex 4.

3. In case when verification of the obligation to appoint an Inspector leads to negative conclusions above does not prevent optional appointment of the Inspector.

4. In the case when the verification of the obligation to appoint the Inspector does not leads to unambiguous conclusions, the Administrator should designate Inspector.

5. The administrator is obliged to carry out activities verifying the existence of the obligation to appoint the Inspector every 12th months, subject to verification in a shorter period, in particular when new guidelines are issued by the authority supervisory board or the European Data Protection Board.

6. The administrator is obliged to publish contact details Inspector (email address and / or phone number) on the website Companies and making them known to employees / co-workers (name, surname, e-mail address, telephone number). Responsibilities of the Inspector

§ 6.

1. The Data Protection Officer is appointed by the Administrator for basis of professional qualifications, in particular professional knowledge on the law and practices in the field of data protection and skills completing their tasks.

2. The administrator may appoint alternate inspectors and other persons, which are part of the Inspector's Team and support the performance tasks of monitoring data protection in the Company.

3. The basic tasks of the Data Protection Officer include:

a) information on obligations resulting from the GDPR and other relevant Union or Member States provisions on protection personal data and advising in this respect,
b) monitoring compliance with the POROS and other relevant regulations data protection provisions of the Union or of the Member States personal,
c) monitoring compliance with the implemented security procedures personal data,
d) advice on the division of duties, for example between the Administrator and the processor or between Administrator's employees,
e) activities increasing the awareness of the Administrator's employees in the scope of obligations resulting from the REDO or the adopted procedures,
f) training for Administrator employees participating in data processing operations,
g) conducting audits in the scope of compliance with the GDPR and implemented procedures for the protection of personal data,
h) providing recommendations on an on-demand basis for assessing conservation effects personal data and monitoring its implementation,
i) cooperation with the supervisory body and performing the function of a point contact for the supervisory body in matters related to data processing,
j) acting as a contact point for data subjects they concern, in all matters related to the processing of them personal data and exercising the rights they are entitled to on the strength of the GDPR,
k) monitoring changes in data protection regulations personal, issuing new or modifying existing ones guidelines of the supervisory body or the European Protection Council Data.

Responsibilities of the System Administrator

§ 7.

1. The System Administrator is a person designated by Administrator.

2. The IT system administrator, in particular:

a) manages the IT system in which the data is processed personal, using the password to access all stations working from the Administrator's position;
b) prevents unauthorized access to the system information technology in which personal data are processed;
c) at the request of the right person and after acceptance by Administrator, assigns an ID to each user password to the IT system and at the Administrator's request makes possible modifications to the entitlements;
d) oversee the operation of user authentication mechanisms and control of access to personal data;
e) take actions to establish and control identifiers access to the IT system;
f) unregister users at the Administrator's request;
g) in the event of a breach of the system's security informing the Administrator and the Inspector about violation and cooperates with him in removing the consequences of the violation;
h) supervises repairs, maintenance and liquidation computer devices on which personal data are stored, supervises the execution of backups, theirs storage and periodic checking for them Further suitability for data recovery in case of failure IT system;

i) take measures to ensure reliability of power supply computers, other devices that affect security data processing and ensuring secure exchange data in the internal network and secure teletransmission;
j) identify and analyze hazards and assess the risks for which it can personal data processing in the system should be exposed information technology;
k) initiates and supervises the implementation of new tools and procedures organizational and system management methods information technology that will lead to strengthening security when processing personal data,
l) carry out periodic reviews of the timeliness and application of procedures with the scope of data processing in the IT system,
m) cooperates with the Data Protection Officer in the field security and rules for the processing of personal data in the system computer,
n) take into account the principles of data protection in the design phase ("privacy by design ") and default data protection (" privacy by default ") when planning the implementation of new processes related to processing of personal data, including in particular new ones IT systems used for data processing personal information.

Responsibilities of managers of organizational units

§ 8.

1. Managers of organizational units are responsible for management processes of personal data processing in their cells. Down to managerial responsibilities should be:

a) managing the processing of personal data in the tasks carried out by your own KO;
b) applying to the Administrator or ASI for sending, change or revocation of rights to employees to specified resources of personal data processed in the system information in accordance with the scope of authorization to processing personal data;
c) familiarizing subordinate employees and other persons (e.g. associates) with the principles of data processing and protection in subordinate to KO;
d) to perform the duties of securing the area personal data processed in a subordinate KO;
e) reporting to the Inspector the intention to start a new process processing of personal data or changes in activities data processing carried out in the KO;
f) in the case of collecting personal data, consulting with Inspector of legal grounds for the processing of personal data, including collection and archiving of consents of people to process them personal data in the cases required;
g) setting in accordance with ASI the principles of backup files with personal data on workstations users in subordinate KO.

Authorized persons

§ 9.

1. A person authorized to process personal data may to process personal data only to the extent individually agreed by the Administrator and only to exercise imposed on it duties. The scope of data access is assigned to a unique user ID necessary for starting work in the system. Termination of employment, solution another agreement connecting that person with the Company results in expiration authorization to process personal data.

2. Persons authorized in writing shall declare that they undertake to confidentiality of personal data and data processing personal in accordance with applicable law and compliance procedures for their

safe processing. Observing the secret personal data is valid for the whole period of employment in the Company, the entire duration of another contract between you and the Company, and also after termination of employment, termination of another contract linking the person authorized with the company.

3. Violation by authorized persons or persons without authorizations, being employees of the Company, safe procedures processing of these data, in particular, informed access data to an unauthorized person, or to data processing in the absence of data basics, is a serious violation of employee duties and can be the basis for terminating the employment relationship without notice.

4. Authorized persons undertake to:

a) get acquainted with the legal provisions regarding data protection personal data, including Policy provisions for processing personal data;
b) use the procedures specified by the Administrator, and guidelines to comply with the law, in particular adequate, data processing;
c) adequate protection of data against disclosure unauthorized persons;
d) informing the Administrator immediately from learning about any suspected violation or violation found and defects of the personal data processing system – information it should be forwarded to the e-mail address of Administrator.

5. The HR specialist is responsible for:

a) preparation of authorization to process personal data along with a contract for a job / order / work;
b) storage of authorizations granted for data processing personal data and declarations of confidentiality personal data and ways to secure them together with personal files employees or civil law contracts;
c) keeping up-to-date records of persons authorized to processing of personal data.

Chapter III Basic principles that should be followed by the person

authorized to process personal data

§ 10.

1. A list of the basic duties of a person authorized to processing of personal data in the Company constitutes Annexe No. 5 to of this Policy.

2. Each authorized person is obliged to be absolute compliance with the obligations referred to in paragraph 1, also after them update.

Chapter IV Risk analysis

Selection of appropriate technical and organizational measures

§ 11.

1. Selection of the technical and organizational measures related to processing and securing personal data in the Company implemented is based on estimating the risk of violation of the rights and freedoms of persons, whose data concern.

2. When selecting security, risk should be assessed both in context the consequences for the data subject, including, for example, discrimination, deprivation of rights, property and non-property damage, as also the risk in the context of consequences for the Company in the event of failure activities related to ensuring the processing of personal data according to the GDPR.

Basic risk analysis

§ 12.

1. Administrator, implementing appropriate technical and organizational measures, takes into account the state of technical knowledge, implementation cost and nature, scope, context and purposes of the processing and the risk of infringement of rights or freedom of physical persons with different probabilities and weight threats so that the processing takes place in accordance with the GDPR and that provide a level of security corresponding to this risk.

2. Risk analysis should be performed:

a) cyclically,
b) if the nature, scope, context or purpose changes processing
c) when processing data for a new purpose.

3. Where the risk analysis shows moderate, high or very high risk of violating the rights or freedoms of natural persons. Adequate measures must be taken immediately minimizing the risk.

4. The risk analysis procedure is attached as Appendix No. 6a and 6b to the Policy. Impact assessment for data protection (DPIA)

§ 13.

1. In the case of processing of personal data in a company that due to its nature, scope, context and goals with a large probability can cause a high risk of violation the rights or freedoms of natural persons before processing an impact assessment of planned processing operations for protection of personal data in accordance with Article 35 GDPR.

2. Regardless of the situation referred to in paragraph 1 conducting an impact assessment on the protection of personal data is necessary in the cases specified in art. 35 para. 3 and 4 GDPR.

3. Inspector in the register of data processing activities personal indicates the processes for which the assessment should be carried out effects and notes its implementation.

4. If the impact assessment for data protection has been carried out, it shows that processing would be high risk if it were not measures taken to minimize this risk, before starting the processing, consult the authority supervisory.

5. In case of consultation with the authority The Inspector shall prepare an appropriate request for consultation in accordance with art. 36 GDPR and contacts the authority in this matter supervisory.

6. The assessment of the effects on data protection shall be carried out by the procedure constituting Annex No. 7 to the Policy.

Protection of personal data

§ 14.

1. The administrator uses personal data security adapted to current risk level.

2. List of areas of data processing with an indication of them physical security is in Annex No. 8 to the Policy. Annex 8 is confidential and may only be disclosed to the authority supervisory body or in other cases on the basis of legal provisions.

Chapter V Keeping records of the processing of personal data

Register of processing activities

§ 15.

1. The company keeps a register of personal data processing activities in accordance with the requirements of art. 30 para. 1 GDPR, in relation to data which company is the Administrator.

2. The activity register is attached as Annex 9 to this Policy.

3. The Inspector is responsible for keeping the activity register.

Processing processes

§ 16.

1. The inspector shall take inventory of the processing of personal data in the company, assigning to them specific data processing activities, closely cooperating with the Administrator.

2. The inspector periodically reviews processing processes data for updating registers.

3. Managers of organizational units are obliged to keep up inform the Inspector about the processing of personal data implemented in their organizational units and about all changes in these processes, in particular regarding:

a) the purposes of data processing, including the activities carried out;
b) the category of persons whose data is processed;
c) ranges of data processed;
d) processing entities to which the data is entrusted;
e) data recipients to whom the data is made available.

Register of processing activity categories

§ 17.

1. The company keeps a register of processing activities categories in accordance with requirements of art. 30 para. 2 GDPR, in relation to the data which the company is a processor.

2. The activity category register is attached as Appendix 10 to this Policy.

Chapter VI. Responsibilities for the processing of personal data

Data processing based on consent

§ 18.

1. Persons responsible in the company for processes in which data is collected they are obliged to exercise special care with them collecting, including:

a) check if the legal basis for acquisition is met personal data, in accordance with art. 6 THE GDPR and art. 9 - 10 GDPR;
b) collect personal data for specific, legitimate purposes implemented in the Company;
c) collect data in a scope adequate to the purposes for which the data will be processed in the company.

2. In case of necessity to receive consent for data processing personal data, it should be ensured that it is obtained voluntarily and notify you of the right to revoke such consent.

3. For the use of appropriate statements of consent when collecting data personal information is answered by the head of the organizational unit responsible for the data collection process.

4. Statements regarding receipt of consent for data processing personal information must be consulted with the Inspector.

5. The inspector may determine the applicable models of consent statements for individual data processing processes carried out in the Company.

Data processing based on a legitimate interest

§ 19.

1. The administrator is authorized to process personal data on based on art. 6 par. 1 lit. f) RODO, except in situations where superior character to the interests of the Administrator or a third party they have interests or fundamental rights and freedoms of the data subject, requiring the protection of personal data, in particular when a person whose data is concerned is a child.

2. The balance of interest test procedure is Annex 11 to of this Policy.

3. The administrator acknowledges that the processing of personal data on the basis of justified interest in the scope indicated in the Register of Activities is acceptable and acceptable, without significant negative impact the data of the persons to whom the processing relates.

Implementation of the information obligation

§ 20.

1. Persons who perform tasks related to data collection personal data, are responsible for the implementation of information obligations referred to in Article 13 and 14 RH0.

2. For the use of appropriate information clauses in the collection of data personal information is answered by the head of the organizational unit responsible for the data collection process.

3. Information clauses must be consulted with the Inspector.

4. The inspector may determine the applicable templates of information clauses for individual data processing processes carried out in the Company.

Chapter VII Temporary limitation of data processing

Data retention

§ 21.

1. Personal data collected as part of the processes carried out in the Company are processed for a period determined by applicable law or determined by the Administrator while maintaining data protection rules personal information. Current retention periods are included in Appendix No. 12 to this Policy.

2. For determining the appropriate retention times of personal data in data processing in the Company is answered by the Inspector. Determination of retention times requires closer cooperation with the Administrator and authorized persons.

3. Personal data for which the processing period does not result from applicable laws, are processed for as long as possible there is both a legal basis and a necessary goal for them processing.

4. The cessation of the purpose of data processing is tantamount to necessity stop processing personal data.

5. Personal data processed only based on the premise of consent for the processing of personal data is deleted always immediately after withdrawal of such consent.

6. In each organizational unit of the Company responsible for a specific the process or processing of personal data at least once in each calendar year - in the first quarter of a given year - verification of the personal data held on paper and electronic form, including:

a) checking if the personal data for which the period has passed storage resulting from legal or internal regulations Company regulations have been removed;
b) checking whether in relation to personal data whose time
c) storage has not been determined by the applicable law or internal company regulations, there is still a legal basis as well indispensable purpose of personal data processing.

7. In the case of determination during the verification referred to in paragraph 6 that the processing period of personal data has expired or there is no basis legal or purpose for further processing of personal data, data personal data should be permanently removed from paper media, electronic and information systems.

Chapter VIII. Principles of sharing personal data

Entrusting data by the Administrator

§ 22.

1. The administrator may entrust another entity with processing personal data only through a contract or other instrument legal. The subject to whom the data have been entrusted may process data only for a specific purpose and scope. Every case entrusting personal data is registered in the register of trusts constituting Annex No. 13 to Policy.

2. The contract for entrusting the processing of personal data may be concluded only with the entity that provides sufficient guarantees implementation of appropriate technical and organizational measures to the processing complied with the requirements of the RODO regulations and protected the rights of persons, whose data concern.

3. For providing the appropriate guarantees referred to in paragraph 2, recognize in particular, but not exclusively:

a) providing the Administrator with a contract of entrustment data processing of the real right to conduct audits and processor control in the scope relating to the subject of the contract, as well as a guarantee of cooperation in the implementation of duties resulting from the GDPR;
b) the certificate holder has been certified meeting the requirements of ISO standards in the field of data protection personal data, including teleinformation security;
c) compliance with the industry code of good by the processor practices approved by the supervisory body;
d) certifying the processor obtained in the framework of certification mechanism, as referred to in the GDPR and UODO.

4. The entrustment agreement may also be concluded in electronic form.

5. Control of processing entities to which they have been entrusted the processing of personal data belonging to the Company is carried out by the Inspector or other designated persons in accordance with the provisions contained in the contracts for entrusting data processing personal data, in relation to the entitlement specified in art. 28 para. 3 lit. h GDPR.

6. Administrator before the planned start of cooperation with the entity the processor is obliged to inform the Inspector and the consult with him the provisions of the concluded contract in the field entrusting the processing of personal data.

Data processing as a processor

§ 23.

The administrator in the scope of his activity may process personal data as a processor, with reservation that such processing is not carried out on the day of entry into force Policy.

Transmission of data

§ 24.

1. Persons who make personal data available to the entity on behalf of the Company external (in paper or electronic form) before them they are obliged to check whether there are legal grounds enabling you to perform these activities, including:

a) the requirement of law regarding the provision of data;
b) consent of a person to share data with another entity;
c) entry in the contract with the cooperating entity, upon fulfilment the condition that the access does not violate the rights and freedoms of the person whom data refer to;
d) an application for access to data from an authorized entity, from indication of the legal basis for receiving a given type personal data.

2. In case of repeated and non-standard data sharing any individual disclosure in the register should be recorded shares containing at least the legal basis of the access (consent, contract, legitimate interest, legal provision), type data being shared, the designated recipient of the data.

3. The provision of personal data may only take place based on what least one of those indicated in art. 6 GDPR and / or art. 9 of the GDPR or other law.

Transfer of data to a third country

§ 25.

The administrator may transfer personal data to entities located in a third country (outside the European Area Economic), however, this can only happen while maintaining compliance with the RODO requirements.

Chapter IX Implementation of the rights of data subjects

Rights of data subjects

§ 26.

1. Any person whose personal data is processed by the Company have the rights specified in art. 15 - 22 GDPR, including:

a) the right of access to data concerning him;
b) the right to rectify the data;
c) the right to delete data;
d) the right to limit processing;
e) the right to transfer data;
f) the right to object to the processing of its data;
g) the right not to be subject to a decision solely based on automated processing.

2. For consideration of requests for permits submitted by the Company, referred to in paragraph 1, corresponds to the Inspector or other indicated person by the Administrator.

3. In the situation of entrusting data to processors or sharing data with other data controllers belongs to them notify you of any rectification, deletion or restriction data processing that was the result of the application received from the data subject.

4. The procedure for the exercise of the rights of data subjects is attached No. 14a to the Policy. Each application should be recorded in the register kept according to the model constituting Annex No. 14b to the Policy.

Chapter X Procedure in the event of a data protection breach

Duty to notify about the violation

§ 27.

1. Any person who acquired knowledge, regardless of the source, violation or suspected violation of personal data protection, is obliged to immediately inform about the above Administrator and Data Protection Officer.

2. The inspector is obliged to assess the risk and recommend it Administrator, in cooperation with ASI, how to proceed in within the scope of security measures to be taken, consideration report violations to the supervisory body and notification of persons, whose data concern.

Report a violation to the supervisory body

§ 28.

1. In the event of a breach of data protection personal data and the likelihood of a risk of infringement of rights or the freedom of individuals, information about the violation should stay notified to PUODO. In doubtful or ambiguous situations you must report to PUODO.

2. Reporting the violation shall be prepared by the Inspector in cooperation with Administrator and, if it is indicated, ASI, and performs within 72 hours after finding the violation, in accordance with the requirements of art. 33 GDPR.

3. Where the data protection breach relates to processes processing carried out by the Company as an entity The organization is obliged to take adequate remedies and to promptly inform administrator of entrusted data.

Notification of data subjects

§ 29.

In a situation where a breach of personal data protection can be found cause a high risk of violating the rights or freedoms of persons physical, the breach must be notified to all persons whom data concern. The inspector examines whether in relation to the requirements of art. 34 paragraph. 3 RODO notification of data subjects will be required. High risk occurs if the process of weight estimation the violation referred to in § 30 para. 3 of the Policy, showed a weight other than low and medium.

Procedures and records of violations

§ 30.

1. A detailed procedure regulating the process of data protection violations constitutes Annex No. 15 to the Policy.

2. Any identified breach of personal data protection, regardless of whether it is reported to the supervisory authority or not, is documented by the Inspector. Pattern of record of protection violations personal data is attached as Annex 16 to the Policy.

3. Verification of the need to notify data subjects, requires estimation of the severity of the violation according to the scheme described in Annex No. 17 to the Policy.

Chapter XI. Accountability of compliance with the implementation of the RODO obligations

Monitoring compliance

§ 31.

1. In order to verify the technical means used in the Company and organizational arrangements ensuring the processing of personal data according to the RODO, they are monitored.

2. Monitoring of personal data protection is carried out:

a) on a current basis by the KO managers in which the data is processed personal;
b) through periodic and ad hoc audits (in the event of occurrence incidents of data protection violations) performed by inspector;
c) during internal audits carried out by authorized entities.

3. The inspector periodically analyzes the compliance of the processing documentation personal data accepted in the Company with the provisions on data protection personal data, current case law, as well as guidelines national supervisory authority or the European Data Protection Board and recommends updating it.

Chapter XII. Effects of violation of personal data protection regulations

Responsibility for data protection breaches

§ 32.

1. Violation of provisions on the protection of personal data is at stake criminal penalties referred to in Article 107 - 108 UODO and in art. 130, 266 - 269, 287 of the Penal Code. The content of the regulations is Annex 18 to Policy.

2. Notwithstanding the liability laid down in the provisions for which referred to in paragraph 1, violation of the rules of personal data protection may be considered a serious violation of basic employee duties and result in liability on the basis of labor law (applies to persons employed under a contract of employment).

Chapter XIII Final provisions

§ 33.

1. Policy together with the Appendices is an internal document, constituting company secrets, and cannot be made available unauthorized persons in any form, unless they are obliged to do so disclosure is legal.

2. In matters not covered by this Policy, they apply provisions of the GDP, UODO and relevant sectoral laws.

3. The policy shall enter into force on 30/04/2019.

4. The Administrator informs about the change of the Policy in advance not shorter than 7 days before the planned entry into force, unless the considerations security are in favor of introducing changes in the mode immediately.

5. The amendment of the Annexes shall come into force as soon as persons are informed authorized, subject to the entry into force of Attachments having implicit in nature as soon as they are drawn up.

6. Annex 8 remains secret and may only be disclosed authorized bodies.

Part II Systems security procedures

information

Chapter II Access to information systems

Record of data sharing

§ 1.

1. An IT system that processes personal data must have mechanisms allowing to notice the fact of performing operations on data. In particular, this provision should include:

1) start and end of work by the system user,
2) operations performed on the processed data,
3) sending personal data through the system processed in the IT system to other entities not being the owner or co-owner of the system,
4) unsuccessful attempts to access the IT system processing personal data and unsuccessful implementation tests operations on personal data,
5) errors in the operation of the information system during a given work user.

2. Each operation performed in the system is dated and dated the user entering the data and the computer's IP address.

Procedure for starting, suspending and terminating work

§ 2.

1. The user starts working with the IT system processing personal data by logging in using ID and password. Each user must have an individual ID. It is forbidden to work many users on a common basis account.

2. Identifier of a person who has lost the right to access data personal data is immediately removed from the system information in which they are processed and the access password remains annulled and other actions necessary for the purpose are taken prevent further access of the person to the data.

3. The user is obliged to notify ASI about login attempts to an unauthorized person's system if the system signals it.

4. In case when the user attempts to log in, he or she will block system, he is obliged to inform ASI, who is responsible for unblocking the system to the user.

5. The user is obliged to prevent unauthorized persons (eg clients, employees of other departments) access to data displayed on computer monitors.

6. Before leaving the workstation temporarily, the user is required to trigger a password-locked screensaver or log out of the system. If he does not do it - after 3 minutes the system should automatically activate the screensaver.

7. After completing the work, the user is required to log out of IT system, and then turn off the computer equipment, secure the workplace, in particular, all documentation and magnetic and optical media on which the data is located personal.

User rights management

§ 3.

1. Process personal data in information systems can only a person authorized to process personal data.

2. After granting the authorization, the Administrator submits it to ASI for posting user ID and privileges in information systems and applications.

3. Each user must have his own individual identifier (login).

4. A person authorized to process personal data works in the workstation's operating system from the user's access level and not administrator.

5. For registering the right to process personal data in IT system is the responsibility of the Administrator.

6. The right to work in the IT system is received temporarily, by blocking an account in the absence of an employee in work lasting longer than 21 calendar days or in the case of reasonable suspicion of a culpable data protection breach.

7. User ID after deregistration from the system IT cannot be assigned to another person. Deregistration the user from the IT system is made by the System Administrator at the request of the Data Administrator, with the date and reason picking up permissions.

Chapter II Methods and means of authentication

General rules for dealing with passwords

§ 4.

1. ASI informs the user about assigning the first password to the workstation.

2. The user is obliged to change the received password immediately to the workstation.

3. Passwords cannot be commonly used words, in particular not you should use dates, names, surnames, initials, numbers as passwords car registration numbers, phone numbers, month names.

4. It is unacceptable to use identical or similar terms for both private and business devices and applications.

5. The user undertakes to keep the password confidential, even after losing their validity.

6. It is forbidden to save passwords in an open manner and to pass them on other people.

7. It is recommended to store passwords while using them password manager, to which the user will establish stronger password.

8. All passwords are passed to employees in a secured form against access by third parties.

Users' passwords to workstations

§ 5.

1. The password for workstations is at least 8 characters long - they are submitted from uppercase and lowercase letters and numbers or special characters.

2. The workstation system should enforce changing the password no less than what 90 days.

Server / network passwords

§ 6.

1. The password for access to the server / network consists of at least 11 characters.

2. The password consists of uppercase and lowercase letters and numbers.

3. The password change takes place once every 90 days.

Administrator's passwords

§ 7.

1. The administrator password consists of at least 10 characters.

2. The password consists of uppercase and lowercase letters as well as numbers or special characters.

3. The password should only be known to the administrator and the authorized person to represent the Company.

4. In the event of loss of rights by the person administering the system you should immediately change the passwords to which she had access.

5. In emergency cases, the password may be forwarded by decision Administrator to the person replacing the administrator.

6. After the emergency situation has ceased, the Administrator is obliged to change password.

Chapter III Backup procedure

Creating backup copies of server documentation

§ 8.

1. The administrator has his own server located on the first floor the building in which the company's headquarters are located. The server room is separate a closed room that ASI and others have access to authorized persons.

2. A disk array (RAID) is configured on the server. Server it is additionally secured with an UPS.

3. ASI shall supervise the execution of backup copies and verifies their correctness.

Other backup copies

§ 9.

1. Backup data stored on local critical disks workstations are automatically created once a week and include such data as company mail data and the program database Commerce and payroll. Copies of data are sent to an external cloud service provider after they have been encrypted. The backup can be deleted one year after its creation.

Chapter IV. Method, place and period of electronic storage

information and print media

Protection of electronic information carriers

§ 10.

1. Data media is stored in a way that prevents access to unauthorized persons, as well as protecting them against environmental hazards (flooding, fire, impact of fields electromagnetic).

2. Personal data carried out outside of the portable processing area media must be encrypted.

3. Devices, discs or other computer media containing data personal data, intended for liquidation, is previously deprived of these data, and in the event that it is not possible to be damaged in a way mechanical, making it impossible to read them.

4. Devices, discs or other IT media containing data personal data, intended for transfer to another entity, unauthorized to receive personal data, it is deprived of previously, write this data.

5. It is forbidden to process personal data on external magnetic, optical media without their prior

encrypted.

6. If you use data media from an external entity, the user is obliged to check themantivirus program on your computer.

7. Magnetic carriers with encrypted unit data personal - they are stored in places for the time of their usefulness protected against unauthorized access, and after them the use of data on them is permanently deleted or these media are destroyed.

Chapter V Procedure for securing the IT system

Antivirus protection

§ 11.

1. ASI is responsible for planning and ensuring anti-virus protection including providing the right amount of licenses for users.

2. The antivirus system is installed on workstations.

3. The antivirus system provides protection for: the operating system, stored files and outgoing and incoming e-mails.

4. Users are required to scan files with the program antivirus.

5. Users ensure constant activity of the antivirus program - the antivirus program must be active while the system is running information processing personal data.

6. The virus definitions update is done automatically by the system.

7. In case of finding a virus or similar Threats Each user is obliged to notify about ASI above.

8. It must be installed on every computer workstation antivirus software working in monitor mode (continuous work in the background).

9. Each e-mail and attachments must be checked by the program antivirus for the presence of viruses.

10. Definitions of virus patterns are updated at least once in month.

11. If the antivirus software allows, it should be set task schedule so that it checks once a week or more computer unit for the presence of viruses.

12. The Administrator of the system is responsible for updating antivirus software and frequency determination automatic updates of virus definitions made by this software.

13. It is prohibited to use media of unknown origin without prior checking their antivirus program. The check is performed by the user who wants to use the media.

14. It is prohibited to download files of unknown origin from the Internet. Every file downloaded from the Internet must be checked with the program antivirus. The check is made by the user who downloaded the file.

15. It is forbidden to read e-mail attachments without prior checking their antivirus program. The check is made by the employee who received the post.

16. The anti-virus check is carried out on the selected computer in the case of irregularities reported by the employee in the functioning of computer hardware or software.

17. In the case of detection of computer viruses, it is checked computer station on which the virus was detected and all media held by you.

18. The User is obliged to notify the System Administrator about appearing messages indicating the occurrence of a threat caused by malware.

19. Users can connect external data carriers only after prior checking the contents of the media with software antivirus.

Protection against unauthorized access to the local network

§ 12.

1. The wireless network is secured by WPA2 technology.

2. The administrator may introduce monitoring mechanisms Internet by users. They can include: blocking pages types of websites, blocking specific pages on the internet, analyzing the information sent in terms of a dangerous one software.

3. The administrator uses the IDS / IPS system for detection and blocking attacks to a computer network that after 5 attempts to gain access blocks the attacker's IP address.

Securing the IT and telecommunications infrastructure

§ 13.

1. Users of portable computers carried out outside the area Organizations on which personal data are processed are required to compliance with the security rules described in the Regulations use of portable computers constituting Annex 19.

2. In the case of access to personal data via the Internet to funds teletransmission is required to authenticate (enter login and password).

3. Access to computer workstations or operating system in which personal data are processed, secured by means of a process authentication using the user ID and password.

4. Measures that prevent unauthorized use have been implemented copies of personal data processed using systems information.

Protection of programs and databases processing personal data

§ 14.

1. Access to personal data in a program or database requires authentication using the user ID and password.

2. An access lock mechanism was applied after 3 unsuccessful attempts login.

3. The means used to register changes made to individual elements of the personal data collection.

4. A mechanism for automatic registration has been applied user ID and date of first data entry personal information.

5. Measures to determine access rights to the indicated range of data within the processed dataset personal information.

6. Systemic measures have been applied to determine the appropriate access rights to IT resources, including data sets personal data for individual users of the IT system.

7. Screen savers have been installed on the stands where personal data are processed.

Software update

§ 15.

1. ASI is responsible for updating the software as recommended producers and market opinion as to safety and stability new versions (e.g. updates, service packs, patches).

2. The administrator is responsible for providing the licensed software for processing personal data.

Chapter VI Procedure for carrying out repairs and maintenance

§ 16.

1. ASI is responsible for failure-free operation of the IT system, including workstations, server applications, databases.

2. Review and maintenance of the IT system should be performed on dates specified by system manufacturers or according to the ASI schedule, but not less than once a year.

3. For timely inspection and maintenance and their maintenance the correct course corresponds to ASI.

4. ASI is responsible for optimizing server resources, memory size and disks.

5. ASI is responsible for identifying and accepting applications for irregularities in the operation of the informatics system and software for immediate removal.

6. Any maintenance and repair work on computer equipment and IT system updates should be performed by authorized person.

7. Before and after the maintenance and repair operations, data and programs in the system should be protected from them destruction, copying or incorrect change.

8. In the event that maintenance and repair work can not to be implemented within the Organization, services should be used an external entity. Using the services of an external entity requires prior conclusion of a confidentiality agreement with him containing a contractual penalty in the event of a breach.

9. As far as possible, maintenance and repair activities performed by external entities should be carried out on the premises Organization under the strict supervision of an authorized person.

10. In the event of the necessity of handing over the damaged equipment computer with personal data for repairs outside the Organization it is necessary to: remove media with personal data, permanently delete data using specialist software or supervise the repair process by an authorized person when there is no possibility removing data from the medium.

11. Implementation of maintenance and repair works by entities the external one should be registered in the book containing the type performed activities, start and end dates of the service, recording persons performing these activities by name and surname.

Chapter VII Procedures of using electronic communication

Procedure for using the Internet

§ 17.

1. The User is obliged to use the Internet only for business purposes.

2. It is forbidden to rip workstation and startup onto hard disk any illegal programs and files downloaded from unknown source.

3. The user is liable for damage caused by software installed from the Internet.

4. It is forbidden to enter pages on which information is presented of a criminal, hacker, pornographic or other nature prohibited by law.

5. Do not enable options in the options of the web browser autocompleting forms and remembering passwords.

6. When using an encrypted connection via a browser you should pay attention to the appearance of the appropriate icon (padlock) and web address beginning with the phrase "https".

The procedure for using e-mail

§ 18.

1. Due to numerous threats resulting from the use of e-mail electronic, a complete ban on private use is introduced a mailbox on computers that process personal data and computers operating in them in one subnet.

2. Only mailboxes created or are allowed to operate accepted for use by the Administrator.

3. The mailbox should be used only on computers that are safe and protected from viruses. In conjunction with this suggests using the box outside of the company or on devices other than work only in emergency situations and necessary.

4. The password for the mailbox should be treated with due care with diligence, like other passwords, in accordance with established quality policies password.

5. Due to mass attacks of dangerous software carried out using e-mail, launching attachments sent

this way, regardless of the file format, it must be preceded the following activities:

a) it should be considered whether any company is binding on the sender connections that require file transfer;
b) Consider whether the sender has reason to send such a file;
c) it should be considered whether the content of the message does not deviate from the usual applied, does not contain stylistic and language errors.

6. Where the e-mail contains links to indicated websites on the Internet, the user before clicking them is obliged to carry out the following analysis:

a) Consider whether the company is binding on the sender any connections that require clicking links;
b) Consider whether the sender has reason to send such a link;
c) it should be considered whether the content of the letter does not deviate from the usual applied, does not contain stylistic and language errors;
d) it should be considered if it is not possible to enter the address indicated by entering it manually in the browser window;
e) if entering data is required after entering the given address the authentication should be considered for sure that the site does not is used to extort this data.

7. If at any stage of the above procedures appear doubts, please immediately stop using the mail and

consult doubts with ASI, Administrator or Inspector.

8. In the case of sending messages containing personal data in small amounts (invoices, individual forms), directed you can send directly to the data subject unencrypted message.

9. For sending messages containing a larger amount of data, personal data or containing data of a specific category (sensitive data), the encryption process described below should be performed.

10. Regardless of the type of message you send, please make sure that the recipient's entered address is correct and no one has appeared in it a distortion that can cause the data to go completely different recipient.

11. If the data is contained in individual files of the MS office suite (Word, Excel) or LibreOffice / OpenOffice (Writer, Calc) can be choose the method of saving the file with the encryption password.

12. If the data is contained in a larger number of files or are files from programs without encryption, data files should be encrypted using a password-protected ZIP archive or similar. One can here, use the free 7-zip program that provides the creation encrypted 7z and ZIP archives (also available to people without a 7-zip program).

13. The encryption password should be provided to the recipient in a different way than via email. You can give them by phone or via SMS.

14. The encryption password should be selected in accordance with the principles of good quality selection password, and it should be different to the ones used for the dispatch data to other recipients.

15. If sending data between two recipients is often and the encryption and password management process becomes cumbersome, ASI implements at the employee's request, asymmetric encryption methods, such as GPG or SMIME, and train both parties using this method. In the asymmetric encryption process is no longer necessary to establish passwords and forwarding them with another channel, because it is based on the principle use of private and public keys.

16. Personal data sent and received by e-mail goes to folders (sent, received etc.) in the mail program or on the server supporting the mailbox.

17. If the box service system or mail program does not allow Automation of content cleaning, ADO obliges the employee to manual removal of messages at least once a month stored longer than indicated periods.

18. Users should pay special attention to the correctness of the address recipient of the message.

19. It is recommended that the user when sending personal data by email included in the content a request for confirmation of receipt and familiarization with information from the addressee.

20. Do not open attachments (files) in e-mails sent by unknown sender or suspicious attachments assigned by a known sender.

21. Users should not send information via e-mail threats to the IT system, "chains of luck" etc.

22. Users should not send e-mails containing large size attachments.

23. When sending e-mails to many recipients at once, use "hidden messages - BCC" methods.

24. The User is obliged to put information in the footer of the e-mail about the confidential nature of the message, the need to delete the received messages in case the message has reached the wrong one recipient.

Attachments:

1. A statement of confidentiality with information about data violation.

2. Authorization to process data.

3a. Records of persons authorized to process data.

3b. Registry of the assignment of keys.

3. Report verifying the obligation to appoint an inspector.

4. Responsibilities of authorized persons.

6a. Procedure defining the principles of risk estimation.

6b. Risk analysis sheet.

7. Impact assessment for data protection.

8. Areas of data processing with their physical

security / secret attachment /.

9. Register of processing activities.

10. Activity category register.

11. Balance test procedure based on art. 6 par. 1 lit. f) GDPR.

12. Data retention periods.

13. Register of trusts.

14a. Procedure for examining the claims of the rights of the data subjects.

14b. Records of the applications of the rights of data subjects.

15. Procedure for data protection violations.

16. Record of data protection violations.

17. Violation weight algorithm.

18. Extract from the rules.

19. Regulations for the use of portable computers