

PERSONAL DATA PROTECTION POLICY

1. This document entitled "Personal data protection policy" (hereinafter referred to as the Policy) is intended to map the requirements, rules and regulations for the protection of personal data in the enterprise of Andrzej Czechowski conducting business under the name ŻALMAL Andrzej Czechowski based in Warsaw (hereinafter referred to as ŻALMAL) .

This Policy is a personal data protection policy within the meaning of the GDPR - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016 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).

2. The policy includes:

- a) a description of the data protection rules in force in ŻALMAL;
- b) references to detailed attachments;

3. The owner of ŻALMAL is responsible for the implementation and maintenance of this Policy, the following are responsible for supervision and monitoring compliance with the Policy:

(i) Data Protection Officer, if appointed in ŻALMAL;

the following are responsible for applying this Policy:

(ii) Owner of ŻALMAL;

(iii) all members of ŻALMAL staff.

ŻALMAL should also ensure that the behavior of ŻALMAL contractors complies with this Policy to the relevant extent when personal data are transferred to them by ŻALMAL.

4. Abbreviations and definitions:

Policy means this Policy for the protection of personal data, unless otherwise explicitly stated in the context.

RODO means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016 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 EU L 119, p. 1).

Data means personal data, unless the context clearly indicates otherwise.

Sensitive data means special data and criminal data.

Special data means the data listed in art. 9 item 1 GDPR, i.e. personal data revealing racial or ethnic origin, political views, religious or beliefs, trade union membership, genetic, biometric data to uniquely identify a natural person or data on health, sexuality or sexual orientation.

Criminal data means the data listed in art. 10 GDPR, i.e. data on convictions and violations of the law.

Children's data means the data of persons under 16 years of age.

Person means the data subject, unless the context clearly indicates otherwise.

Processing entity means the organization or person entrusted with the processing of personal data by ŻALMAL (e.g. IT service provider, external accounting).

Profiling means any form of automated processing of personal data that involves the use of personal data to evaluate certain personal factors of a natural person, in particular to analyze or forecast aspects of the natural

person's work effects, economic situation, health, personal preferences, interests, credibility, behavior, location or movement.

Data export means the transfer of data to a third country or an international organization.

DPO or Inspector means the Inspector for Personal Data Protection

RCPD or Registry means the Register of Personal Data Processing Activities.

ŻALMAL means the enterprise of Andrzej Czechowski conducting business activity under the name ŻALMAL Andrzej Czechowski based in Warsaw

5. Personal data protection in ŻALMAL - general principles

5.1. Pillars of personal data protection in ŻALMAL:

- (1) Legality - ŻALMAL protects privacy and processes data in accordance with the law.
- (2) Security - ŻALMAL ensures an adequate level of data security by undertaking continuous activities in this area.
- (3) Individual rights - ŻALMAL enables data subjects to exercise, exercise their rights and exercise these rights.
- (4) Accountability - ŻALMAL documents how it fulfills its obligations in order to be able to demonstrate compliance at any time.

5.2. Data Protection Policy

ŻALMAL processes personal data in accordance with the following principles:

- (1) based on a legal basis and in accordance with the law (legalism);
- (2) fairly and honestly (reliability);
- (3) in a transparent manner for the data subject (transparency);
- (4) for specific purposes and not "on stock" (minimization);
- (5) no more than necessary (adequacy);
- (6) with care for data accuracy (correctness);
- (7) no longer than necessary (temporality);
- (8) ensuring adequate data security (security).

5.3. Data Protection System

The personal data protection system in ŻALMAL consists of the following elements:

- 1) Data inventory. ŻALMAL identifies personal data resources in ŻALMAL, data classes, relationships between data resources, identifies ways of using data (inventory), including:
 - (a) cases of processing special data and "criminal" data (sensitive data);
 - b) cases of data processing of persons whom ŻALMAL does not identify (unidentified data / UFO);
 - c) processing of children's data;
 - d) profiling;
 - e) data co-administration.

2) Record. ŽALMAL develops, maintains and maintains a Register of Personal Data Activities in ŽALMAL (Register). The register is a tool for accounting compliance with data protection in ŽALMAL.

3) Legal basis. ŽALMAL ensures, identifies, verifies the legal grounds for data processing and registers them in the Register, including:

a) maintains the consent management system for data processing and remote communication,

b) inventory and details the justification of cases where ŽALMAL processes data on the basis of ŽALMAL's legitimate interest.

4) Handling of individual rights. ŽALMAL fulfills the disclosure obligations towards persons whose data it processes, and provides support for their rights, implementing the requests received in this respect, including:

a) Information obligations. ŽALMAL provides legal persons with the required information when collecting data and in other situations, and organizes and provides documentation of the implementation of these obligations.

b) Ability to make requests. ŽALMAL verifies and provides the possibility of effective execution of each type of request by itself and its processors.

c) Request handling. ŽALMAL ensures the appropriate outlays and procedures to ensure that people's requests are met on time and in the manner required by the GDPR and documented.

d) Notification of violations. ŽALMAL uses procedures to determine the need to notify people affected by an identified data breach.

5) Minimize. ŽALMAL has principles and methods of minimization management (privacy by default), including:

a) the principles of data adequacy management;

b) rules on rationing and managing access to data;

c) the rules for managing the data retention period and verifying further suitability;

6) Safety. ŽALMAL ensures an adequate level of data security, including:

(a) carry out risk analyzes for data processing activities or categories thereof;

b) carry out data protection impact assessments where the risk of violating the rights and freedoms of persons is high;

c) adapt the data protection measures to the risks identified;

d) manage information security;

e) applies procedures to identify, evaluate and report an identified data protection breach to the Data Protection Authority - manages incidents.

7) The processing. ŽALMAL has rules for the selection of data processors for ŽALMAL, requirements as to the processing conditions (entrustment contract), and rules for verifying the performance of entrustment contracts.

8) Data export. ŽALMAL has rules to verify that ŽALMAL does not transfer data to third countries (i.e. outside the EU, Norway, Liechtenstein, Iceland) or to international organizations and to ensure the lawful conditions for such transfers, if any.

9) Privacy by design. ŽALMAL manages changes that affect privacy. To this end, the procedures for launching new projects and investments in ŽALMAL take into account the need to assess the impact of the change on data protection, ensuring privacy (including compliance of processing purposes, data security and minimization) already at the stage of designing the change, investment or at the beginning of a new project.

10) Cross-border processing. ŽALMAL has rules for verification when there are cases of cross-border processing and rules for determining the lead supervisory body and the main organizational unit within the meaning of the GDPR.

6. Inventory

6.1. Sensitive data

ŽALMAL identifies cases in which it processes or may process sensitive data (special data and criminal data) and maintains dedicated mechanisms to ensure the lawfulness of processing sensitive data. In the case of identifying sensitive data processing cases, ŽALMAL proceeds in accordance with accepted principles in this respect.

6.2. Unidentified data

ŽALMAL identifies cases in which it processes or may process unidentified data and maintains mechanisms to facilitate the implementation of the rights of persons to whom unidentified data relate.

6.3. Profiling

ŽALMAL identifies cases in which it profiles processed data and maintains mechanisms ensuring compliance of this process with the law. In the case of identifying profiling cases and automated decision making, ŽALMAL follows the adopted principles in this respect.

6.4. Co-administration

ŽALMAL identifies cases of data co-administration and proceeds in this respect in accordance with accepted principles.

7. Register of Data Processing Activities

7.1. RCPD is a form of documenting data processing activities, acts as a data processing map and is one of the key elements enabling the implementation of the fundamental principle on which the entire personal data protection system is based, i.e. the principle of accountability.

7.2. ŽALMAL maintains a Register of Data Processing Activities in which it inventories and monitors the manner in which it uses personal data.

7.3. The register is one of the basic tools enabling ŽALMAL to settle most data protection obligations.

7.4. In the Register, for each data processing activity that ŽALMAL has recognized as separate for the purposes of the Registry, ŽALMAL shall record at least: (i) the name of the activity, (ii) the purpose of the processing, (iii) description of the categories of persons, (iv) description of the categories of data, (v) the legal basis for the processing, together with the specification of the legitimate interest category ŽALMAL, if the basis is a legitimate interest, (vi) the method of data collection, (vii) a description of the categories of data recipients (including processors), (viii) information on transfers outside the EU / EEA ; (ix) a general description of the technical and organizational data protection measures.

7.5. The template of the Register is attached as Annex 1 to the Policy - "Template for the Register of Data Processing Activities". The Registry template also contains optional columns. In the optional columns, ŽALMAL records information as necessary and possible, taking into account that the fuller content of the Registry makes it easier to manage and settle data protection compliance

8. Basics of processing

8.1. ŽALMAL documents in the Register the legal grounds for data processing for individual processing activities.

8.2. By indicating the general legal basis (consent, contract, legal obligation, vital interests, public task / public authority, legitimate purpose of ŽALMAL) ŽALMAL specifies the basis in a legible manner when it is needed. E.g.

for consent indicating its scope, when the basis is law - indicating a specific provision and other documents, e.g. contract, administrative agreement, vital interests - indicating categories of events in which they will materialize, legitimate purpose - indicating a specific purpose, e.g. own marketing, redress.

8.3. ŽALMAL implements consent management methods enabling registration and verification of a person's consent to the processing of specific data for a specific purpose, consent for distance communication (email, telephone, sms, etc.) and registration of refusal of consent, withdrawal of consent and similar activities (objection, restriction e.t.c.).

9. Method of handling individual rights and information obligations

9.1. ŽALMAL cares about the readability and style of the information provided and communication with the persons whose data it processes.

9.2. ŽALMAL makes it easier for people to exercise their rights through various activities, including: placing on the ŽALMAL website information or references (links) to information about the rights of persons, how to use them in ŽALMAL, including identification requirements, methods of contact with ŽALMAL

9.3. ŽALMAL ensures compliance with legal deadlines for fulfilling its obligations towards persons.

9.4. ŽALMAL introduces adequate methods of identification and authentication of persons for the purposes of exercising individual rights and information obligations.

9.5. In order to implement the rights of the ŽALMAL unit, it provides procedures and mechanisms to identify the data of specific persons processed by ŽALMAL, integrate this data, introduce changes to it and delete it in an integrated manner,

9.6. ŽALMAL documents handling information obligations, notifications and requests of persons.

10. Information obligations

10.1. ŽALMAL defines lawful and effective ways of performing disclosure obligations.

10.2. ŽALMAL informs a person about extending the period of over one month to consider this person's request.

10.3. ŽALMAL informs a person about the processing of his data when obtaining data from that person.

10.4. ŽALMAL informs a person about the processing of their data when acquiring data about that person indirectly from him.

10.5. ŽALMAL defines the method of informing people about the processing of unidentified data, where possible (e.g. a plate about the area covered by video monitoring).

10.6. ŽALMAL informs the person about the planned change in the purpose of data processing.

10.7. ŽALMAL informs the person before lifting the processing restriction.

10.8. ŽALMAL informs data recipients about rectification, deletion or limitation of data processing (unless it requires disproportionate effort or impossible).

10.9. ŽALMAL informs a person about the right to object to data processing at the latest upon the first contact with that person at the latest.

10.10. ŽALMAL notifies the person about the breach of personal data protection without undue delay, if it may cause a high risk of violating the person's rights or freedoms.

11. People's requests

11.1. Third Party Rights. By exercising the rights of data subjects, ŽALMAL introduces procedural guarantees to protect the rights and freedoms of third parties. In particular, if you receive reliable information that the performance

of a person's request for a copy of the data or the right to transfer data may adversely affect the rights and freedoms of others (e.g. rights related to data protection of other persons, intellectual property rights, trade secrets, personal rights etc.), ŽALMAL may refer a person to clarify doubts or take other lawful steps, including a refusal to satisfy the request.

11.2. Not to process. ŽALMAL informs a person that he does not process data concerning him, if such a person has made a request for his rights.

11.3. Refusal. ŽALMAL informs the person, within one month of receiving the request, of the refusal to consider the request and of the rights of the person related thereto.

11.4. Access to the data. At the request of a person regarding access to his data, ŽALMAL informs the person whether he is processing his data and informs the person about the details of the processing, in accordance with art. 15 GDPR (the scope corresponds to the information obligation when collecting data), and also grants the person access to data concerning him. Access to data can be made by issuing a copy of the data, with the proviso that a copy of the data issued in the exercise of the right of access to data ŽALMAL will not be considered as the first free copy of the data for the purposes of fees for data copies.

11.5. Data copies. On request, ŽALMAL issues a copy of the data concerning him to the person and notes the fact that the first copy of the data has been issued. ŽALMAL introduces and maintains a price list of data copies, according to which it charges fees for subsequent copies of data. The price of a copy of the data is calculated based on the estimated unit cost of handling the request for a copy of the data.

11.6. Correction of data. ŽALMAL corrects incorrect data at the request of a person. ŽALMAL has the right to refuse to rectify data, unless a person reasonably reveals irregularities in the data which he is demanding to rectify. In the event of data correction, ŽALMAL informs the person about the recipients of the data, at the request of that person.

11.7. Completion of data. ŽALMAL supplements and updates the data at the request of a person. ŽALMAL has the right to refuse to supplement data if the supplement would be incompatible with the purposes of data processing (e.g. ŽALMAL does not have to process data that is ŽALMAL redundant). ŽALMAL may rely on a statement of a person regarding supplemented data, unless this is insufficient in the light of the procedures adopted by ŽALMAL (e.g. regarding the collection of such data), rights or there are grounds to consider the statement unreliable.

11.8. Data deletion. At the request of a person, ŽALMAL deletes data when:

- (1) the data is not necessary for the purposes for which it was collected or processed for other purposes,
- (2) consent to their processing has been withdrawn, and there is no other legal basis for processing,
- (3) the person has effectively objected to the processing of this data,
- (4) the data was processed unlawfully,
- (5) the need to remove results from a legal obligation,
- (6) the request concerns the child's data collected on the basis of consent for the provision of information society services offered directly to the child (e.g. child's profile on a social networking site, participation in the competition on the website).

ŽALMAL defines the manner of handling the right to delete data in such a way as to ensure the effective implementation of this right while respecting all data protection principles, including security, as well as verifying whether there are any exceptions referred to in art. 17. paragraph 3 GDPR.

If the data subject to deletion has been made public by ŽALMAL, ŽALMAL takes reasonable steps, including technical measures, to inform other controllers processing this personal data about the need to delete data and access it.

In the event of deletion of data, ŽALMAL informs the person about the recipients of the data, at the request of that person.

11.9. Restriction of processing. ŽALMAL limits the processing of data at the request of a person when:

- a) a person questions the correctness of the data - for a period that allows checking their correctness,
- b) the processing is unlawful and the data subject opposes the deletion of personal data, demanding instead a restriction on their use,
- c) ŽALMAL no longer needs personal data, but it is needed by the data subject to determine, pursue or defend claims,
- d) the person has objected to the processing for reasons related to his particular situation - until it is determined whether ŽALMAL has legally justified grounds superior to the grounds for the objection.

During the limitation of processing, ŽALMAL stores data, but does not process them (does not use, do not transfer), without the consent of the data subject, unless to establish, assert or defend claims, or to protect the rights of another natural or legal person, or for important reasons of public interest.

ŽALMAL informs the person before lifting the processing restriction.

In the event of limitation of data processing, ŽALMAL informs the person about the recipients of the data, at the request of that person.

11.10. Data Transfer. At the request of a person, ŽALMAL issues in a structured, commonly used machine-readable format or transfers to another entity, if possible, data on the person who ŽALMAL provided, processed on the basis of that person's consent or for the conclusion or performance of a contract with contained in IT systems ŽALMAL.

11.11. Opposition in a special situation. If a person raises an objection motivated by his particular situation against the processing of his data, and the data is processed by ŽALMAL based on the legitimate interest of ŽALMAL or the task entrusted to ŽALMAL in the public interest, ŽALMAL will accept the objection, unless there are valid legally justified grounds for ŽALMAL processing, overriding the interests, rights and freedoms of the person raising an objection, or grounds for establishing, pursuing or defending claims.

11.12. Opposition on scientific, historical or statistical research. If ŽALMAL conducts scientific or historical research or processes data for statistical purposes, a person may lodge an objection to such processing motivated by his particular situation. ŽALMAL will accept such an objection, unless the processing is necessary to perform a task carried out in the public interest.

11.13. Opposition to direct marketing. If a person objects to the processing of his data by ŽALMAL for the purposes of direct marketing (including possibly profiling), ŽALMAL will accept the objection and stop such processing.

11.14. Right to human intervention in automatic processing. If ŽALMAL processes data automatically, including in particular profiling persons, and consequently makes decisions towards the person causing legal effects or otherwise significantly affecting the person, ŽALMAL provides the opportunity to appeal to human intervention and decisions on the part of ŽALMAL, unless such automatic decision (i) it is necessary for the conclusion or performance of the contract between the appellant and ŽALMAL; or (ii) is expressly permitted by law; or (iii) is based on the explicit consent of the dismissing person.

12. MINIMIZING

ŽALMAL ensures minimization of data processing in terms of: (i) adequacy of data for the purposes (amount of data and scope of processing), (ii) access to data, (iii) time of data storage.

12.1. Range minimization

ŽALMAL has verified the scope of the data obtained, the scope of their processing and the amount of data processed in terms of their adequacy for the purposes of processing as part of the implementation of the GDPR.

ŽALMAL periodically reviews the amount of data processed and the scope of their processing at least once a year.

ŽALMAL verifies changes in the amount and scope of data processing as part of change management procedures (privacy by design).

12.2. Minimizing access

ŽALMAL applies restrictions on access to personal data: legal (confidentiality obligations, scopes of authorizations), physical (access zones, closing rooms) and logical (restrictions on the rights to personal data processing systems and network resources in which personal data reside).

ŽALMAL uses physical access control.

ŽALMAL updates access rights with changes in the composition of staff and changes in the roles of persons, as well as changes in processors.

ŽALMAL periodically reviews established system users and updates them at least once a year.

Detailed rules for physical and logical access control are contained in the ŽALMAL physical security and information security procedures.

12.3. Time minimization

ŽALMAL implements mechanisms for controlling the life cycle of personal data in ŽALMAL, including verification of the further usefulness of data against deadlines and checkpoints indicated in the Register.

Data whose range of usefulness is reduced over time is removed from the ŽALMAL systems as well as from handy and main files. Such data may be archived and may be on backup systems and information processed by ŽALMAL. The procedures for archiving and using archives, creating and using backups take into account the requirements of data life cycle control, including data removal requirements.

13. SAFETY

ŽALMAL provides a level of security corresponding to the risk of violation of the rights and freedoms of natural persons as a result of the processing of personal data by ŽALMAL.

13.1. Risk analysis and adequacy of security measures

ŽALMAL carries out and documents the analysis of the adequacy of personal data security measures. For this purpose:

(1) ŽALMAL ensures an appropriate state of knowledge about information security, cybersecurity and business continuity - internally or with the support of specialized entities.

(2) ŽALMAL categorizes data and processing activities in terms of the risk they present.

(3) ŽALMAL carries out analyzes of the risk of violation of the rights or freedoms of natural persons for data processing activities or categories thereof. ŽALMAL analyzes possible situations and scenarios of personal data breach taking into account the nature, scope, context and purposes of processing, the risk of violation of the rights or freedoms of natural persons with different likelihood and severity of threat.

(4) ŽALMAL sets out applicable organizational and technical security measures and assesses the cost of their implementation. In this, ŽALMAL determines the usefulness and applies such measures and approach as:

(I) Pseudonymisation.

(ii) encryption of personal data,

(iii) other cyber security measures making up the ability to continually ensure the confidentiality, integrity, availability and resilience of systems and processing services,

(iv) measures to ensure business continuity and disaster prevention, i.e. the ability to quickly restore the availability of personal data and access to it in the event of a physical or technical incident.

13.2. Impact assessments for data protection

ŽALMAL assesses the effects of planned processing operations on the protection of personal data where, according to the risk analysis, the risk of violation of the rights and freedoms of persons is high.

ŽALMAL applies the impact assessment methodology adopted in ŽALMAL.

13.3. Security measures

ŽALMAL applies security measures established as part of risk analysis and adequacy of security measures and data protection impact assessments.

Personal data security measures are part of the information security and cyber security measures at ŽALMAL and are further described in the procedures adopted by ŽALMAL for these areas.

13.4. Reporting violations

ŽALMAL applies procedures allowing identification, assessment and reporting an identified data protection breach to the Data Protection Authority within 72 hours of establishing the breach.

14. RECYCLED

ŽALMAL has rules for the selection and verification of data processors for ŽALMAL, designed to ensure that processors give sufficient guarantees for the implementation of appropriate organizational and technical measures to ensure security, implementation of individual rights and other data protection obligations incumbent on ŽALMAL.

ŽALMAL has adopted the minimum requirements for the contract for entrusting data processing constituting Annex 2 to the Policy - "Model contract for entrusting data processing".

ŽALMAL accounts for processors from the use of sub-processors as well as from other requirements arising from the Rules of entrusting personal data.

15. DATA EXPORT

ŽALMAL registers in the Register cases of data export, i.e. data transfer outside the European Economic Area (EEA in 2017 = European Union, Iceland, Liechtenstein and Norway).

To avoid the situation of unauthorized data export, in particular in connection with the use of publicly available cloud services (shadow IT), ŽALMAL periodically verifies user behavior and, if possible, provides equivalent data protection solutions in accordance with the law.

16. PRIVACY DESIGN

ŽALMAL manages the change affecting privacy in such a way as to enable ensuring adequate security of personal data and minimizing its processing.

To this end, the principles of project and investment management by ŽALMAL refer to the principles of personal data security and minimization, requiring an assessment of the impact on privacy and data protection, taking into account and designed security and minimizing data processing from the beginning of the project or investment.