INFORMATION (DATA) SECURITY POLICY (GDPR) TATAJ INNOVATION Sp. z o.o.

This Security Policy, hereinafter referred to as the Policy, was prepared to show that personal data are processed and secured in accordance with the legal requirements regarding the principles of processing and securing personal data, including Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 (hereinafter: GDPR).

definitions:

Data Administrator - TATAJ INNOVATION Sp. z o.o., ul. Królewicza Jakuba 76, 02-956 Warsaw

Data Processor - the Data Administrator if it processes Personal Data in relation to which a third party decides about the purpose of processing

Personal data, Data - all information about an identified or identifiable natural person

IT system - a set of cooperating devices, programs, information processing procedures, software tools used for data processing

User - a person authorized by the Data Administrator to Process personal data

Data set - each ordered set containing Personal Data, available according to specific criteria

Data Processing - any operations performed on Personal Data, such as collecting, recording, storing, developing, changing, sharing and deleting in traditional form and in IT systems

User identifier - a string of letters, numbers or other characters that uniquely identifies the person authorized to Process Data in the IT system (User) in the event of Data Processing in such a system

Password - a string of letters, numbers or other characters, known only to the person authorized to work in the IT system (User) in the event of Data Processing in such a system

Authentication - an action whose purpose is to verify the declared identity of the entity (User)

Supervisory authority - President of the Office for Personal Data Protection as the body responsible for monitoring the implementation of the provisions of the GDPR on Polish territory

I. General provisions

1. The policy applies to all Personal Data processed by the Data Administrator, irrespective of the form of their processing (traditionally processed record files, IT systems) and whether the data is or can be processed in data sets.

2. The policy is stored in an electronic version and in a paper version at the headquarters of the Data Administrator.

3. The policy is made available to persons authorized to process personal data on behalf of the Data Administrator at their request, as well as to persons to whom such authorization is to be issued, in order to become familiar with its content.

4. Depending on the category of data, the Data Administrator processes Data:

- based on the consent of the data subject,

- on the basis of authorizations contained in generally applicable laws,

- for the implementation of tasks arising from the legitimate purposes of the Data Administrator.

5. For effective implementation of the Policy, the Data Administrator ensures:

- technical measures and organizational solutions appropriate to the threats and categories of protected data,

- control and supervision over Data Processing,

- monitoring of protection measures applied.

6. Monitoring by the Data Administrator of the security measures applied includes, among others Users' actions, violation of data access rules, ensuring file integrity and protection against external and internal attacks.

7. The Data Administrator ensures that the activities carried out in connection with Data Processing and the protection of Personal Data are in accordance with this policy and the relevant legal provisions.

II. Personal data processed by the Data Administrator

1. The Data Administrator does not process Data in a way that could be associated with a serious probability of high risk for the rights and freedoms of persons. If such action is planned, the Data Administrator will perform the actions specified in art. 35 et seq. GDPR.

2. In the case of planning new processing activities, the Data Administrator analyzes their effects on the protection of Personal Data and takes into account data protection issues at the design stage of these activities.

3. The Data Administrator keeps a register of processing activities in the scope of administered Personal Data. The model register is attached as Annex 1 to this policy.

III. Duties and responsibilities in the field of safety management

1. All persons who gain access to Personal Data administered by the Data Administrator or processed by him as a Processing Entity are obliged to process Personal Data in accordance with applicable regulations, set by the Data Administrator for the Security Policy, as well as other internal documents and procedures related to Processing of personal data with the Data Administrator.

2. All Personal Data processed in accordance with the processing principles provided for by law, and thus:

- in any case, there is at least one of the grounds provided for by law for the processing of Personal Data,

- Personal Data is processed fairly and transparently,

- Personal Data is collected for specific, explicit and legitimate purposes and is not further processed in a way incompatible with those purposes,

- Personal Data is processed only to the extent that is necessary to achieve the purpose of data processing,

- Personal Data is correct and updated if necessary,

- the storage time of Personal Data is limited to the period of their usefulness for the purposes for which they were collected, and after that period they are anonymized or deleted,

- the data subject is subject to an information obligation in accordance with art. 13 GDPR.

Personal Data is protected against violations of the principles of their protection.

3. The violation or attempted violation of the principles of processing and protection of Personal Data shall be considered in particular:

- breach of security of IT systems in which Personal Data is processed, if processed in such systems,

- sharing or enabling the sharing of Data with unauthorized persons or entities,

- failure, even inadvertently, to fulfill the obligation to provide personal data protection,

- failure to keep personal Data confidential and how to secure it,

- processing of Personal Data not in accordance with the assumed scope and purpose of their collection,

- causing damage, loss, uncontrolled change or unauthorized copying of Personal Data,

- violation of the rights of persons whose data are processed.

5. In the event of a breach of the personal data protection rules, the User is obliged to take all necessary steps to limit the effects of the breach and to immediately notify the Data Administrator.

6. The duties of the Data Administrator in the employment, termination or change of employment conditions of employees or associates (persons undertaking activities for the Data Administrator under other civil law contracts) include ensuring that:

- these people were properly prepared and trained to perform their duties,

- each of the processors of Personal Data was authorized in writing to process in accordance with the "Authorization to process personal data" subject to paragraph 7 - the model Authority is attached as Annex 2 to this Security Policy,

- each of the data processors has committed to keeping the Personal Data confidential.

7. All employees are authorized to process personal data of other employees to the extent necessary for the proper functioning of internal communication within the Administrator's enterprise.

8. Persons referred to in para. 6 are obliged to:

- strict compliance with the scope of the authorization granted;

- processing and protecting Personal Data in accordance with regulations;

- keep personal data secret and how to secure it;

- reporting incidents related to data breach and system malfunction.

IV. The area of personal data processing

1. The area in which Personal Data are processed consists of rooms located in locations used by the Data Administrator.

2. The area of personal data processing also includes objects that are not rooms in the form of IT media and computer systems owned by the Data Administrator, rented or leased by the Data Administrator, if they are outside the area defined in point 1.

V. Specification of technical and organizational measures necessary to ensure confidentiality, integrity and accountability of processed data

1. The Data Administrator ensures the application of technical and organizational measures necessary to ensure confidentiality, integrity, accountability and continuity of Data Processing.

2. The security measures (technical and organizational) used should be adequate to the level of risk identified for individual systems, types of files and categories of Data. These measures include, inter alia:

- limiting access to the rooms in which the Data Processing takes place only to duly authorized persons (unauthorized persons may stay in these rooms only in the company of an authorized person),

- closing rooms forming the area of Personal Data Processing specified in point IV above for the duration of employees' absence in a manner preventing access by unauthorized persons,

- use of lockers to secure documents,

- using a shredder for effective removal of documents containing personal data,

- protection of Data processed in the local computer network against external and internal threats.

VI. Violations of personal data protection rules

1. The Data Administrator maintains a "Register of personal data breaches". The register template is attached as Annex 2 to this policy.

2. The Data Administrator assesses whether an event bearing the hallmarks of a personal data breach may result in a risk of violating the rights or freedoms of data subjects.

3. In every situation in which the event may have caused the risk of violation of the rights or freedoms of natural persons, the Data Administrator shall without undue delay notify the given violation to the supervisory body - if feasible, not later than within 72 hours after finding the violation. The obligation to notify does not arise if it is unlikely that the consequence of the event would be an infringement of the rights and freedoms of natural persons. The application form is set out in Annex 3 to this policy. Reports can also be made using a dedicated ICT system made available by the supervisory authority.

3. If the risk of violation of rights and freedoms is high, the Administrator shall also notify the data subject of the incident, unless in a given case one of the circumstances specified in art. 34 section 3 GDPR, or the provisions of Polish law will exclude the Administrator's obligation to fulfill this obligation. The content of the notification, if applicable, may be of a general nature, if premature disclosure of the details of the violation could hinder law enforcement activities.

VII. Entrusting the processing of personal data

1. The Personal Data Administrator may entrust Data Processing to another entity only by means of a contract concluded in writing, in accordance with the requirements indicated for such contracts in art. 28 of the GDPR, provided that this entity guarantees the introduction of appropriate technical and organizational measures so that Data Processing takes place in accordance with the GDPR, national law on the protection of personal data, and guidelines and decisions of the supervisory authority.

2. The administrator monitors the manner in which the entity referred to in point VII point 1 processes data and takes appropriate action if Data Processing does not meet the requirements of the GDPR, national law on the protection of personal data or guidelines and decisions of the supervisory authority.

VIII. Transfer of data to a third country

1. The Personal Data Administrator transfers Data to a third country, except in situations where this occurs at the request of the data subject.

IX. Final provisions

1. This Security Policy is provided to persons obliged to use by the Data Administrator.

X. Contact

1. For notifications of the Data violations or inquiries regarding this policy document, please contact Tataj Innovation Data Administrator at office@tatajinnovation.com.