Personal Data Protection Policy

PxP Shape sp. z o.o. (“PxP Shape”)

1. Purpose

The purpose of this Data Protection Policy is to provide a high and consistent level of protection for Data Subjects and ensure Organization's adherence to General Data Protection Regulation.

Compliance with General Data Protection Regulation is one of the key objectives of the Organization, crucial for achieving the business objectives. It is also important for fostering and maintaining the confidence of its main stakeholders and the wider public in the Organization and its operations.

Organization recognizes the importance of and is committed to proper Data Subjects request handling in order to provide effective and fast procedure regarding examination of motions submitted to the company and dealing with potential complaints concerning Personal Data processing by the Organization.

2. Terms and Definitions

Terms used in this document have the following meanings:

- **Accountability** - a property that ensures that the actions of a person can be unambiguously assigned only to that person,
- **Avoidance (Avoid)**: removing all exposure to an identified Risk,
- **Authorization** – authorization granted to the Staff to process Personal Data for the Organization,
- **Business Continuity** - the Organization's ability to continue to deliver a product and provide services at acceptable, defined levels following a disruptive incident,
- **BCP** - acronym for Business Continuity Planning,
- **Confidentiality** - a property that information is not made available or disclosed to unauthorized persons, entities, or processes,
- **Cause -** what is driving the Risk and needs to be addressed in order to be modified,
- **Contractor** - any individual that is hired to perform work for the Organization on a contract basis,
- **Control -** definition of practices that should take place to Avoid or minimize the Likelihood of a Vulnerability being exploited or to reduce the attack or Data Breach,
- **Data Breach** - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (either accidental or deliberate),
- **Data Subject -** any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural, or social identity,
- **Data Controller** - a person, company, or other body that determines the purpose and means of Personal Data processing,
- **Data Protection Policy, Personal Data Protection Policy** - the present document,

- **Data Processor** - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller,
- **Employee** - a person, who cooperates with the Organization under any legal employment relationship concluded with the Organization,
- **Executive Management** - Board Members of the Organization,
- **General Data Protection Regulation or GDPR** - Regulation (EU) 2016/679 Of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons 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),
- **Incident** - an event or a series of undesirable or unexpected events that may significantly affect the course of the Organization's business processes or affect the security of processed Personal Data.
- **Information assets** - the resources of the Organization that are used to process information. Examples of Information assets are information in paper and electronic form, IT systems, Employee's knowledge, information storage devices (cabinets, safes, disks),
- **Integrity** - the property of ensuring the accuracy and completeness of Information assets,
- **Impact** - negative effect to the Organization and data security after a Vulnerability been exploited,
- **Likelihood** - Possibility of a potential Risk take place according to the environment and history,
- **Organization or Data Controller or Data Processor (depends on the context of this document)** – PxP Shape Spółka z ograniczoną odpowiedzialnością, with its registered seat in Cracow, entered into the register of entrepreneurs kept by the District Court for Kraków - Śródmieście in Kraków, XI Economic Department of the National Court Register, under KRS No. 0001011625, NIP: 6762633451, REGON: 524112207,
- **Personal Data** – any information relating to an identified or identifiable Data Subject,
- **Probability** – possibility, chance of an event occurring,
- **Risk** – the impact of uncertainty on goals, Personal Data security or business continuity of the Organization,
- **Risk analysis/score** – the process of finding out the nature of Risk and determining the Risk level (Likelihood x Impact),
- **Risk assessment** – the process of Risk identification, Risk analysis and Risk evaluation,
- **Risk identification** – the process of finding, recognizing, and describing Risks,
- **Risk level** – the size of the Risk or combination of Risks expressed as a combination of consequences and their Probability,
- **Risk management** – coordinated activities related to the direction and supervision of the Organization in relation to Risk,
- **Risk management process** – the systematic application of management policies, procedures and practices of communication, consultation, context setting, and Risk identification, Risk analysis, evaluation, management, monitoring, and review activities,
- **Staff**- Everyone who has access to Organization's premises/logical environment regardless of the "legal bond" (All Employees and Contractors),
- **Sensitive/special category of personal data** – the following types of personal data (specified in data protection legislation) which are particularly sensitive and private in nature, and therefore more likely to cause distress and damage if compromised:
    - Racial or ethnic origin,
    - Political opinions,

    - Religious beliefs or other beliefs of a similar nature,
    - Trade union membership,
    - Genetic data,
    - Data concerning a natural person's sex life or sexual orientation,
    - Physical or mental health or condition,
    - Commission or alleged commission of any criminal offence,
    - Biometric data where processed to uniquely identify an individual.
- **Threat** – potential Causes of Information assets or information becoming compromised. It could be an environmental threat, crime syndicate, hacktivist group, government-sponsored entity, or sabotage,
- **Vulnerability** – System-level (software), Infrastructure or compliance gaps that could be exploited by any kind of Threat,
- **Information Security Clauses**:

Shall, must, will	This term is used to state a **mandatory** requirement of the document
Should	This term is used to state a **recommended** requirement of the document
May, could	This term is used to state an **optional** requirement

3. Objectives

The Data Protection Policy sets forth the principles and procedures applicable at the Data Controller's company for the processing of Personal Data both in files and in the computer system, aimed in particular at:

1) providing support to determine the protocol to be followed in order to comply with Data Subject rights,
2) ensuring compliance of the processing of Personal Data with the provisions of the GDPR and other legal regulations on personal data protection,
3) ensuring the security of the processed Personal Data in a category appropriate to the risks,
4) securing Personal Data from being accessed by unauthorized persons or taken by an unauthorized person,
5) prevent the processing of Personal Data in violation of the GDPR, as well as the loss, damage, or destruction of Personal Data.
6) develop rules to deal with suspected security breaches in the processing of Personal Data.

4. Scope

This Data Protection Policy needs to be followed by all the Management Board and the Staff regardless of their position, role, location, or bond with it.

This Policy applies to all Personal Data processed by the Organization acting as Data Controller and/or as Data Processor (if applicable).

5. Roles and Responsibilities

5.1. Executive Management

Executive Management is committed to support Personal Data protection.

5.2. Data Protection Officer (DPO) or Designated Person

If required by the provisions of GDPR, Executive Management shall appoint a Data Protection Officer. If according to GDPR appointment of the DPO is not required, the Executive Management shall designate a person being a contact person for the Personal Data issues ("**Designated Person**"). The duties of the Data Protection Officer, which are explicitly mentioned in this Policy, are performed by the Designated Person id the Data Protection Officer is not appointed, unless otherwise specified.

DPO is responsible for:

a. informing and advising the Organization and the Employees who carry out processing of their obligations pursuant to the General Data Protection Regulation;
b. monitoring compliance with the General Data Protection Regulation and with this Data Protection Policy in relation to the protection of Personal Data, including the assignment of responsibilities, awareness-raising and training of Employees and Contractors involved in the Personal Data processing, and the related audits;
c. providing advice when requested as regards the Personal Data protection impact assessment and monitor its performance;
d. cooperating with the supervisory authority as needed;
e. acting as the Single Point of Contact (SPOC) for Business Partners as well as Supervisory Authorities, as applicable, on issues related to Personal Data processing, requests, and any other Personal Data processing related matters.

If a Data Protection Officer has not been appointed, the above duties shall be performed by the Organization's Board of Directors or a Designated Person, if expressly decided by the Board of Directors.

Designated Person shall be the contact person for all the issues connected with the Personal Data processing and shall be responsible for handling and responding for the queries received by the Data Controller on the following e-mail address: dataprotection@pxpshape.com. In addition, the Designated Person may assign some of the tasks indicated in point a-e above by the decision of the Management Board.

5.3. Managers

Managers are responsible for ensuring that Personal Data is processed in adherence to Principles set out in article 6.1 of this Data Protection Policy. This includes (but is not limited to):

a. ensuring that the Staff understand their obligations in terms of processing Personal Data, are aware and comply with this Data Protection Policy and report potential Personal Data breaches when they occur,
b. determining the level of access to Personal Data be granted to specific individuals, controlling when and how it will be granted and promptly revoke it upon expiration of the access need,
c. Ensuring Staff have appropriate training about Personal Data processing and applicable requirements under General Data Protection Regulation.
d. Ensuring all members of the Staff know how to obtain Personal Data protection advice.

5.4. All Staff

Regardless of the position, all Staff is required to acknowledge and act upon this Data Protection Policy and to adhere to processes/procedures, instructions, guidance. Failure to do so might result in disciplinary actions at the Organization's discretion.

Personal Data protection shall be implemented in every process within the Organization and all Staff is responsible for conducting consultation with the DPO if necessary.

Executive Management ensures that all Staff have the opportunity to acknowledge with this document prior to granting the Authorization.

5.5. Authorization to process the Personal Data

1. Authorization shall be granted by the Executive Management or by the holder of the power of attorney appointed for this purpose.
2. The Authorization shall be granted to a Staff member on the date on which he/she signs a contract of employment or other agreement with the Organization under which the Staff member provides services.
3. No person shall be allowed to process Personal Data in the Organization unless an Authorization is first granted to that person.
4. The Authorization shall be attached to a copy of the employment contract or contract for the Authorized Person's provision of services,
5. Executive Management or appointed person shall conduct the registry of the Authorization granted in the Organization.
6. Unless otherwise indicated in the Authorization, the Authorization shall expire on the date of termination of the Authorized Person's employment contract or other legal relationship under which such Authorized Person provides services.
7. The Authorization may be amended in the event of a change in the necessity to change the Authorized Person's access to the Personal Data.

6. Policy Statement

6.1. Principles

To ensure obligations under General Data Protection Regulation are met, the Executive Management ensures that the processing of Personal Data must comply with following principles:

a. Processed lawfully, fairly and in a transparent manner in relation to the Data Subject,
b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes,
c. adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (‘data minimization’);
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay (‘accuracy’);

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data are processed ('storage limitation');
f. processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and against accidental loss destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality'). Technical measures are implemented in accordance with the Device Policy document,
g. ensure, that any access to the Personal Data shall be granted only for the Authorized member of the Staff.

6.2. Principle Details

Principles	Applicability within the Organization
Lawfulness of processing	All processing of Personal Data, where the Organization acts as Data Controller must meet one of the six lawful bases: 1) the consent of the data subject, 2) the performance of a contract concluded with the Data Subject or fulfilling pre-contractual obligations, 3) adherence to a legal obligation the Organization is subject to, 4) protection of someone's vital interests, 5) the performance of a task carried out in the public interest, 6) it is necessary for the purposes of the Organization's legitimate interest, that is not overridden by the rights and freedoms of the Data Subject.
Consent to processing	Personal Data can be processed following the consent given by the Data Subject. Before giving consent, the data subject must be presented with adequate information in accordance with the GDPR. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can also be given verbally. The granting of consent must be documented.
Processing of special categories of Personal Data	Any processing of special categories of Personal Data must be consulted and approved with the DPO prior to commencement of processing or with outside advisors.
Rights of the Data Subject	Under GDPR, Data Subject is entitled to exercise rights stated below: 1. Right of access and right to obtain a copy of the Personal Data undergoing processing, 2. Right to rectification of inaccurate Personal Data concerning the Data Subject, 3. Right to erasure of Personal Data concerning the Data Subject,

	4. Right to restriction of processing, 5. Right to Personal Data portability, 6. Right to object to processing of Personal Data concerning the Data Subject. 7. Right not to be subject to automated decision-making. Any request in respect of the rights above, should preferably be made in writing and send directly to the DPO (e-mail: dataprotection@pxpshape.com). Every Employee or Contractor is obliged to accept the request submitted to them and forward it to the DPO without further delay. Information on action taken on the request shall be provided within thirty days of receipt of the request. That period may be extended by two further months where necessary, considering the complexity and number of the requests. Data Subject shall be informed of any such extension together with the reasons for the delay. The DPO is responsible for managing the process and ensuring that required actions are taken and that the appropriate response is handed in to the Data Subject within deadline. If the request is submitted regarding Personal Data processes, in which the Organization acts as the Processor, the DPO is obliged to send the request forward to the Data Controller within contractual deadlines.
Information about processing	Whenever the Organization acts as the Data Controller, the Data Subject shall be provided with the required information of processing. Every information of processing shall be consulted with the DPO prior to commencement of the processing.
Automated individual decision-making, including profiling	Automated individual decision-making, including profiling shall take place only when it is necessary to fulfil the Organization's contractual obligations upon the Client's request and under strict legal conditions resulting from GDPR.
Personal Data protection by design and by default	The DPO shall be informed about every new software, process, solution, or any other change within the Organization, that requires Personal Data processing. The DPO is obliged to analyse the request to ensure that, by default, only Personal Data which are necessary for each specific purpose of the processing will be processed.

	Additionally, the DPO may propose appropriate technical and organizational measures in order to meet the requirements of GDPR and to protect the rights of Data Subjects.
Data processing agreement	Every business relationship that the Organization steps into shall be verified whether performance of the contract requires Personal Data transfer to or from the Organization. When such transfer occurs, the DPO must be consulted, and the data processing agreement shall be concluded if necessary.
Records of processing activities	The Organization maintains a record of processing activities and a record of all categories of processing activities required under the GDPR. Records are updated under the supervision of the DPO on an annual basis.
Security of processing	The Organization implements appropriate technical and organizational measures to ensure maintaining the level of security appropriate to the Risk identified.
Personal Data breach management	Every Incident that can be identified as a potential Personal Data breach shall be logged using the Issue Type "Privacy Incident Report". Management of the Incident is processed in accordance with Data breach management procedure (described in section 6.6 of this Policy).
Data protection impact assessment	Every new type of processing is assessed whether it is likely to result in a high Risk to the rights and freedoms of the data subject. When a high Risk is identified, data protection impact assessment (AKA DPIA) shall be carried out under the supervision of the DPO or external competent advisors.
Transfer of Personal Data to third countries or international organizations	Any processing of Personal Data that requires transfer of Personal Data to third country or international organization must be consulted with the DPO prior to commencement of the processing.
Authorization for Personal Data	Each member of the Staff may process the Personal Data only after being granted the authorization from the Organization.

6.3. Privacy by default and by design. Data processing impact assessment

The Organization ensures that the following rules are complied with when developing new or existing products:

1) Whenever the Organization intends to create a new product or develop an existing product, the Organization shall ensure that, taking into account the state of the knowledge, the costs of implementation and the nature, scope, context and purposes of the data processing and the risk of violation of the rights or freedoms of natural persons of varying probability and severity arising from the processing, it shall implement appropriate technical and organizational measures, such as pseudonymization, encryption, designed to effectively implement data protection principles, such as data minimization, and to give the processing the necessary safeguards to meet the requirements of GDPR and protect the rights of Data Subjects.

2) Furthermore, the Organization implements appropriate technical and organizational measures so that, by default, only those personal data are processed that are necessary to achieve each specific processing purpose. This obligation refers to the amount of personal data collected, the extent of its processing, the period of its storage and its availability. In particular, these measures ensure that, by default, personal data is not made available to an unspecified number of individuals without the person's intervention.

Data protection impact assessment

1) If a particular type of processing - in particular using new technologies - is, by its nature, scope, context and purposes, likely to involve a high risk of violation of the rights or freedoms of natural persons, the Data Controller shall assess the effects of the intended processing operations on the protection of personal data before the processing begins. For similar processing operations involving a similar high risk, a single assessment may be carried out,

2) The data protection impact assessment referred to in point 1) above shall be required in particular for:

    a) a systematic, comprehensive assessment of personal factors relating to natural persons that is based on automated processing, including profiling, and is the basis for decisions that produce legal effects on a natural person or similarly significantly affect a natural person;
    b) large-scale processing of special categories of personal data referred to in Article 9(1), or personal data relating to criminal convictions and offenses as referred to in Article 10; or
    c) large-scale systematic monitoring of publicly accessible sites.

3) At a minimum, the assessment shall include:

a) a systematic description of the intended processing operations and the purposes of the processing, including, where applicable, the legitimate interests pursued by the controller;
b) an assessment of whether the processing operations are necessary and proportionate in relation to the purposes;
c) an assessment of the risk of violation of the rights or freedoms of data subjects referred to in paragraph 1; and
d) the measures planned to address the risk, including safeguards and security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other affected persons.

6.4. Accountability

The Organization is responsible for and must be able to demonstrate compliance with the Personal Data protection principles and the collateral obligations arising from GDPR (in order to gain and maintain compliance with Accountability principle).

The Organization must ensure that it has adequate resources, systems, and processes in place to demonstrate compliance with the Organization's obligations including:

a. appointing a suitably qualified DPO and providing them with adequate support and resources, if it is required by the GDPR regulations;
b. integrating Personal Data protection into the Organization's internal documents and policies;
c. regularly training the Organization's Staff on the GDPR, this Data Protection Policy and the Organization's related policies and procedures, and maintaining a record of training completion by the Staff;
d. regularly testing the technical and organizational measures implemented by the Organization and conducting periodic reviews to assess the adequacy and effectiveness of this Data Protection Policy, and the Organization's related policies and procedures;
e. keeping full and accurate records of all Personal Data processing activities in accordance with GDPR requirements;
f. reviewing all the systems and processes to ensure that they are adequate and effective for the purposes of facilitating compliance with the Organization's obligations under this Data Protection Policy.

6.5. Policy Compliance

All individuals and systems across the Organization shall comply with the requirements outlined in this Data Protection Policy and the documents sitting beneath it.

All systems across the Organization shall comply with this Policy and other appropriate documentation and procedures created to comply with the GDPR regulations. All exceptions to the requirements specified in this document must be handled through the Risk management process, and ultimately be signed off by the DPO (or the Executive Management).

This Policy does not replace Data privacy law and/or any national laws. It supplements Data privacy law. These regulations and laws shall take priority if compliance with this Policy would result in a violation of Data privacy law or national law. The content of this Policy must also be observed in the absence of corresponding national laws.

If compliance with this Policy would result in a violation of national law, or if regulations that deviate from this Policy are required under national law, this must be reported to the DPO or the Executive Management for the purposes of Personal Data protection law monitoring. In the event of conflicts between national laws and this Policy, DPO will find a practical solution that fulfils the purpose of this Data Protection Policy.

6.6. Personal Data breach management procedure

The purpose of this procedure is to standardise the response to any reported incident regarding Personal Data breach, and ensure all Incidents are managed in accordance with legal requirements and best practices.

Following this procedure will ensure that all Incidents are reported and properly managed in a timely manner, operations are restored as soon as possible, Incidents are handled by the right person, impact is properly assessed, the right people notified, everything is tracked and documented accordingly.

The process flowchart should go through the following steps:

Report > Validate > Control > Assess > Communicate > Evaluate

6.6.1. Breach Management Process

- It is vital that Personal Data breaches are immediately (within 24 hours where feasible) reported, preferably made in writing, and sent directly to the DPO (e-mail: dataprotection@pxpshape.com) so that the impact of the breach and further notification requirements can be assessed as soon as possible. Depending on the complexity and size of the breach, a dedicated team (with adequate skills) may be assembled in order to provide an effective response.
- Once a Personal Data breach has been reported, its management should follow the steps:
    - Validate if the reported Personal Data breach has effectively occurred;
    - Control the impact as much as possible;
    - Assess the breach and the Risks in order to determine the best remedial approach and communication - Risk Assessment Matrix for Data Breaches;
    - Communicate the breach to relevant entities (individuals need to be informed in case the breach is likely to result in a high risk to their rights and freedoms, Supervisory Body, or the data controller). The following information should be made available to individuals when telling them about a breach: name and contact details of the DPO, a description of the likely consequences of the breach, the measures taken or proposed to deal with that breach and, where applicable, the measures taken to mitigate any possible adverse effects;
    - Evaluate the root cause of the breach, the response provided and what can be improved/learnt;

- Any discussion of a Personal Data breach (including the fact that it happened) must be restricted to the ones directly involved in the investigation (unless otherwise required).
- Any third-party processor providing services on the Organization's behalf, is legally obliged to notify the Organization about the breach under the General Data Protection Regulation. This notification must happen as soon as the processor becomes aware of such breach.

The following circumstances are indicated by way of example, which may indicate a breach of Personal Data security and the occurrence of which obliges the user to take the actions specified in this Personal Data Protection Policy:

- unannounced changes in the functionality or appearance of applications for processing Personal Data,
- unexpected and unexplainable changes in the contents of the database,
- unannounced presence of new applications in the computer system or other changes in the configuration of software used for processing personal data,
- traces of violation of the integrity of the physical security of the premises, where Personal Data are being processed.

6.6.2. Personal Data breach review

A Personal Data breach may expose the need of improvements regarding IT systems, Employees or Contractors training or procedures and policies. These improvements together with due dates, will need be specified in the Incident report.

The DPO or member of the Executive Management will draft the Incident report and ensure that the improvement actions are applied and in case those actions have not been applied, escalate it. Any lessons coming from these actions will need to be applied to the learning material available.

7. Record of processing activities and record of all categories of processing activities

1. The Data Controller shall keep a register of processing activities of Personal Data.
2. The following information regarding Personal Data shall be placed in the register of processing activities:
   (a) Contact details of the Data Controller and other co-controllers,
   (b) The purposes of the processing,
   (c) Description of categories of data subjects and categories of Personal Data,
   (d) Categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations,
   (e) When applicable, information about the transfer of Personal Data to a third country or international organization, including the name of the third country or international organization and documentation of the relevant safeguards,
   (f) If applicable, the planned deletion dates for each category of data,

(g) If possible, a general description of the technical and organizational security measures referred to in Article 32(1) of the Regulation. Hereinafter, as "Register of Processing Activities"

3. With respect to Personal Data for which the Organization is a Data Processor, the Executive Directors or its designated person shall maintain a register of categories of processing activities, including:
   (a) the name and contact details of each controller on whose behalf the Processor acts,
   (b) the categories of processing performed on behalf of each Controller,
   (c) where applicable, information about the transfer of Personal Data to a third country or international organization, including the name of the third country or international organization and documentation of the relevant safeguards,
   (d) If applicable, a general description of the technical and organizational security measures referred to in Article 32(1) of the Regulation, hereinafter as the "Register of categories of processing activities" The registers indicated in items 2 and 3 above shall be maintained by the Administrator's Management Board or a person designated by it, in electronic form within the meaning of Article 30 (3) of the GDPR.

8. Document Control

Document Details

Document Type	Policy
Owner	Bruno Pimenta
Approvers	See below
Date First Published	02/01/2023
Date of Next Planned Review	31/12/2025
Classification	INTERNAL

Version History

Version	**Date**	**Description of Change**	**Edited By**	**Reviewed and Approved? (Y/N) / Approver**
1.0	02/01/2023	Document created	Bruno Pimenta	Yes / Arthur Pfister
1.1	09/07/2024	Document reviewed	Bruno Pimenta	Yes / Arthur Pfister
1.2	27/06/2025	Document updated	Bruno Pimenta	Yes / Maria Pfister