Risk Assessment Matrix for Personal Data breaches

PxP Shape sp. z o.o.

If a Personal Data breach occurred a Risk Assessment should be made immediately and recorded. List the threats and calculate the Risk associated. This will help on deciding the next steps to take.

All terms used in this Policy shall have the meaning determined in the Personal Data Protection Policy of PxP Shape Sp. Z o.o.

Approach

1. Analyse the threat events which can impact the confidentiality, accuracy, or availability of the Personal Data being collected, stored, or processed in the Organization.
2. Evaluate the likelihood and Impact of the event to happen according to the following tables:

Likelihood		
1	Highly unlikely	Almost no chance of it happening
2	Unlikely	Small chance of the event happening
3	Possible	The event may happen
4	Likely	The event is likely to happen
5	Highly likely	The event will certainly happen

Impact	
1	Disclosure of no more than two personal details, from name, address, emails, telephone number or date of birth of Data Subjects
2	Disclosure of name, address, emails, telephone number, date of birth, of some Data Subjects
3	Disclosure of some personal details, such as name, address, emails, telephone number, date of birth, undefined medical data, or personal contact of some Data Subjects
4	Disclosure of personal details, such as name, address, telephone number, emails, date of birth, gender, medical data, bank details, conversations, and any additional data, which could result in a small number of Data Subjects suffering harm, anxiety, or identity theft as a direct result of disclosure.
5	Disclosure of personal details, such as name, address, telephone number, emails, date of birth, gender, medical data, bank details, conversations, and any additional data, which could result in a large number of Data Subjects suffering harm, anxiety, or identity theft as a direct result of disclosure.

3. Assess the Risk score by multiplying Likelihood value by the Impact value.

4. Use the comment section to address additional topics like:
    - If the Personal Data was lost/stolen, were there any protections in place to prevent access/misuse? E.g., encryption of data/device
    - If the Personal Data was damaged/corrupted/lost, were there protections in place to mitigate the impact of the loss? E.g., back-up tapes/copies

- Who are the individuals whose Personal Data has been compromised? E.g., students, applicants, staff, customers, etc
- What could the Personal Data tell a third party about the individual? Could it be misused?
- Are there wider consequences to consider? E.g., a risk to public health or loss of public confidence?

Example:
A laptop has been left on unattended in a public place and someone from the public witness a stranger plugging an external data storage in the computer and copied some Personal Data and the laptop was not encrypted. There was a document on the desktop containing names, address, email address, telephone number and some comments of over 40 Data Subjects but no medical information or bank details.

Event	Likelihood	Impact	Risk Score	Comment
Personal Data has been stolen from the computer	5	3	5x3=15	Medium / High risk High enough to contact the DPO or Designated Person to deal with the Personal Data and the Data Subjects, if known should be contacted. The Supervisory Body has to be notified.

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