1. Introduction

GDPR (General Data Protection Regulation) is one of the regulations affecting the way that organizations carry out their information-processing activities. It is the regulation that is designed to protect the personal data of European Union citizens. Fines are applicable for any form of breaching GDPR's rules and regulations. Hence, **[XYZ]** should ensure compliance with GDPR by establishing a Data Protection Policy (DPP).

2. Purpose

The purpose of this document is to describe **[XYZ]**'s responsibilities regarding the protection of personal data.

3. Principles of Processing Personal Data

GDPR is based under a number of fundamental principles, such as:

a) Personal data should be processed with fairness, lawfulness, and transparency toward the data subject
b) Personal data should be collected for specified and legitimate purposes
c) Personal data should be accurate and kept up to date
d) Inaccurate personal data should be erased or rectified without delay
e) Personal data should be processed and secured against any unlawful or unauthorized processing

[XYZ] shall ensure compliance with all of the abovementioned principles.

3.1 Rights of the Data Subject

The rights of the data subject under the GDPR are:

a) The right of being informed
b) The right to access
c) The right to rectification
d) The right to erasure
e) The right to restrict processing
f) The right to data portability
g) The rights related to automated decision-making and profiling
h) The right to object

Data subject rights are supported by appropriate procedures within **[XYZ]** that allow the required action to be taken within the timescales stated under the GDPR.

The timescales for data subject requests are shown in the table below.

Data Subject Request	Time scale
The right of being informed	Within one month (if the data is not supplied by the data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The rights related to automated decision-making and profiling	Not specified
The right to object	On receipt of objection

3.2 Lawfulness of Processing

[XYZ] 's policy specifies the appropriate actions that should be taken for documenting and processing a specific case of personal data. However, GDPR provides six alternative ways that can be used by **[XYZ],** depending on the case.

Consent: Except in specific reasons that are stated as allowable under GDPR, **[XYZ]** should obtain consent from the data subject, prior to collecting and processing their data. For example, any case that involves children below the age 16 requires parental consent.

Contract performance: Explicit consent will not be required in cases where the collected and processed data are required for contract fulfillment, like cases when the contract cannot be finalized without the personal data. For example, if an address is missing in the delivery of a package, the delivery cannot be completed.

Legal obligation: Explicit consent will not be required in cases when the collected and processed data are required in order to comply with law. Taxation and employment can be examples of such cases.

Data subject's fundamental interests: A certain amount of data processing can be lawful under certain conditions (especially in the public sector), like cases when the data is needed to protect the subject's main interests or social care.

Carrying out tasks of public interest: The data subject's consent is not requested in cases where **[XYZ]** needs to perform a specific task that is of public interest.

Legitimate interests: Data processing is considered lawful in cases when the processing of personal data does not significantly affect the rights and freedoms of the data subject. However, the taking of such actions should be justified properly and documented.

3.3 Data Protection by Design

[XYZ] should adopt the principle of data protection by design and ensure that the systems collecting personal data consider privacy issues. The systems should also successfully complete one or more data protection impact assessment.

The data protection impact assessment (DPIA) includes the following:

- Determine the purpose of processing the personal data
- Determine whether the processing of personal data is necessary
- Identify the necessary controls to address the risks and comply with the legislation

In order to respect personal data privacy and comply with GDPR, **[XYZ]** can use techniques, such as data minimization and pseudonymisation.

3.4 Processing Personal Data Contracts

Based on the requirements of GDPR, **[XYZ]** should ensure that all of the personal data used are subject to a contract, i.e., the GDPR Controller-Processor Agreement Policy.

3.5 International Transfers of Personal Data

Before transferring any personal data outside of Europe, **[XYZ]** reviews and ensures that they are in compliance with GDPR regulations.

Therefore, in order to regulate the intra-group international data transfers, the Binding Corporate Rules (BCR) provide enforceable rights for data subjects.

3.6 Breach Notification

In any case related to breaches of personal data, **[XYZ]** is responsible for considering actions that should be taken and inform the affected parties.

In accordance with GDPR, if a breach of personal data occurs, the relevant authority should be informed within 72 hours. These cases should be managed based on the Information Security Incident Response Procedure, which provides the process of handling information security incidents.

Annex A (Data Protection Policy Example)

Summary of the policy	The data protection policy ensures an adequate level of security in terms of confidentiality, availability, and integrity of information assets and personal data of **[XYZ]** against all threats they could face. The organization establishes, implements, operates, monitors, reviews, maintains, and improves processes and controls related to data processing and information security based on a risk approach.
Introduction	**[XYZ]** should ensure respect for the integrity, confidentiality, and availability of information generated within the processing of personal data. **[XYZ]** shall ensure the protection of their information assets against internal, external, accidental, or deliberate threats.
Objectives	Ensure continuity of critical business activities. Ensure that all information processed, stored, traded, and released by **[XYZ**] has complete integrity.

	Ensure that all information relevant to **[XYZ]** will be monitored and stored according to procedures for maintaining appropriate confidentiality. Provide choice of appropriate and proportionate security controls to protect the assets, and maintain interested parties' faith.
Principles	**[XYZ]** shall establish, implement, operate, monitor, review, maintain, and improve their data protection and privacy framework based on a documented approach to risk activity and compliance with all of GDPR's requirements. **[XYZ]** should take into account all legal, regulatory, and contractual requirements with regards to the processing of personal data in order to avoid breaching its legal statutory, regulatory, or contractual obligations, as well as its security requirements. **[XYZ]** shall establish and implement a risk management program documented in accordance with GDPR's requirements. The criteria for evaluation and acceptance of risk must be established, formalized, and approved by the management. The data protection policy has been approved by management and is subject to an annual review.
Responsibilities	The management has the responsibility to ensure that objectives and plans for compliance with GDPR are established and reviewed annually during the management review, the roles and responsibilities for the processing of the personal data and information security are defined, a security awareness program is implemented, an internal audit is conducted at least once a year, and the necessary resources to maintain and improve its compliance are provided. The head of information security/data protection has the authority to intervene in all aspects of information security at **[XYZ]**. The head of information security/data decides, in general, all the requirements for the effective compliance to GDPR by means of administrative directives, previously submitted to senior management.

	Each executive has a responsibility to ensure that persons working under their control will protect information in accordance with **[XYZ]**'s policies**.** **[XYZ] users** (management, employees, contractors, and third party users) should be aware of the risks to information security and processing of personal data, their responsibilities, and the need to respect the policies and to ensure adequate protection of information.
Expected results	Appropriate and proportionate controls will be implemented to protect assets and give confidence to interested parties. Decisions on matters of data protection will be based on an evaluation of risks faced by **[XYZ].** The legal, regulatory, and contractual requirements for **[XYZ]** will be met.
Related policies	Data protection policy Human Resource Management policy The policy on the personnel's training and skills development