Data Protection Policy

1. Introduction

Switch Product Group is committed to protecting the privacy and personal data of our customers, employees, and partners. This Data Protection Policy outlines our approach to ensuring compliance with relevant data protection laws and regulations, including the General Data Protection Regulation (GDPR). Our policy sets out the principles and procedures we follow to safeguard personal data and ensure its confidentiality, integrity, and availability.

2. Purpose

The purpose of this policy is to:

- Outline our commitment to protecting personal data and respecting individuals' privacy
- Ensure compliance with GDPR and other applicable data protection laws
- Define the roles and responsibilities for data protection within the organization
- Establish procedures for handling personal data securely and transparently

3. Scope

This policy applies to all employees, contractors, and third-party service providers of Switch Product Group. It covers all personal data processed by the organization, including data relating to customers, employees, and business partners.

4. Responsibilities

Management Team: The management team has ultimate responsibility for ensuring that Switch Product Group complies with all data protection regulations and has effective policies and procedures in place.

Head of IT (Initial Data Protection Officer): The Head of IT will initially serve as the Data Protection Officer (DPO), responsible for overseeing the implementation and maintenance of this Data Protection Policy, ensuring compliance with data protection laws, and managing data security measures.

Employees: All employees are responsible for adhering to this policy and for handling personal data in accordance with the principles and procedures set out herein.

5. Data Protection Principles

We are committed to processing personal data in accordance with the following principles:

Lawfulness, Fairness, and Transparency: Personal data will be processed lawfully, fairly, and in a transparent manner.

Purpose Limitation: Personal data will be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

Data Minimisation: Personal data will be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

Accuracy: Personal data will be accurate and, where necessary, kept up to date.

Storage Limitation: Personal data will be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.

Integrity and Confidentiality: Personal data will be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

Accountability: We will be responsible for and be able to demonstrate compliance with these principles.

6. Data Subject Rights

We respect and uphold the rights of data subjects, including the right to:

- Access their personal data
- Rectify inaccurate or incomplete data
- Erase personal data (the "right to be forgotten")
- Restrict the processing of their data
- Data portability
- Object to the processing of their data
- Withdraw consent at any time, where processing is based on consent.
- Lodge a complaint with a supervisory authority

7. Data Collection and Processing

Lawful Basis for Processing: We will identify and document the lawful basis for processing personal data, such as consent, contract, legal obligation, legitimate interests, or vital interests.

Data Inventory: We will maintain an inventory of personal data processed by the organization, including details of data categories, processing activities, and data retention periods.

8. Data Security

Technical Measures: We will implement appropriate technical measures to protect personal data, including encryption, access controls, and secure data storage.

Organisational Measures: We will establish organisational measures to ensure data security, such as regular staff training, data protection policies, and incident response procedures.

Third-Party Processors: We will ensure that third-party processors comply with data protection requirements and enter into data processing agreements where necessary.

9. Data Breach Management

Incident Reporting: All employees must report any data breach or suspected data breach to the Head of IT immediately.

Breach Response: The Head of IT will assess the breach, implement measures to contain and mitigate its impact, and determine whether the breach must be reported to the relevant supervisory authority and affected data subjects.

Record Keeping: We will maintain records of all data breaches, including details of the breach, actions taken, and decisions made.

10. Training and Awareness

Employee Training: All employees will receive regular training on data protection principles, legal requirements, and best practices for handling personal data securely.

Ongoing Education: We will provide ongoing education and updates to employees to ensure they are aware of any changes in data protection laws and practices.

11. Policy Review and Updates

Regular Review: This policy will be reviewed annually or more frequently if necessary to ensure it remains up-to-date with regulatory requirements and best practices.

Amendments: Any amendments to this policy must be approved by the management team and communicated to all employees and relevant stakeholders.

12. Conclusion

Switch Product Group is committed to maintaining the highest standards of data protection and privacy. By implementing this Data Protection Policy, we aim to protect the personal data of our customers, employees, and partners, ensuring compliance with GDPR and other relevant data protection laws.