<Product Name> - Technical and Organizational Measures

1. General Considerations

This data protection policy outlines the technical and organizational measures implemented for secure and compliant processing of personal data. It takes into account the rights of data subjects and requirements of the articles 24, 25, and 32 GDPR to the extent applicable.

<enter company name> deals with three general categories of personal data:

1. (…)
2. (…)

The following description of technical and organizational measures will be differentiated, where applicable, according to these categories of data.

2. Organization

<enter company name> appointed a data protection officer (DPO) who provides advice on data privacy issues, updates the team about changes in regulations and standards and, if required, supports with reviews and improvement of the measures. The DPO can be reached via <enter email address>.

In the future, the company is going to create data privacy guidelines documented in the form of standard operating procedures (e.g. DPR-SOP) and templates.

> Reference here your Information-Security-Management-System (ISMS) in place.

3. Confidentiality

3.1 Entry Control

<enter company name> operates based on office premises that are not freely accessible. They are locked when employees are away. The company implemented the following measures:

- Locked building
- Locked office

<enter company name> does not maintain servers or server rooms. (…)

> If you operate your own server rooms, do your best at describing all security policies to prevent unauthorized people from entering here.
>
> If you use a third party cloud provider, their policies here. Typically, they should provide you with loads of material that is helpful for this exercise.

> If your users store data locally on their end devices - good for you. In that case, enter some description of that and outline that no data leaves the end device.

3.2 Access Control

The company has implemented the following measures for access to software systems:

(…)

> Describe your access restrictions. Those are measures not only to prevent unauthorized people from entering your offices, but also to prevent unauthorized (electronic) access. Some example measures:
>
> - For every employee, a personally assigned user is set up with a password bound to strict requirements (at least 14 characters long with special characters).
> - Passwords must be unique and may not be used for other accounts. Passwords must be changed annually.
> - Central authentication with username and password, incl. mandatory 2-factor authentication. Every user has to verify the account at least every 30 days.
> - Access is monitored and logged, including unsuccessful login attempts.
> - Access is automatically blocked by the system after XXX failed attempts.
> - Only employees get access to the majority of files and systems and the extent of access can be determined selectively.

3.3 Usage Control

The company has implemented following measures when working within software systems:

(…)

> What are your policies when working with your internal systems? Some typical examples:
>
> - The password rules for access control must also be followed for usage control.
> - Role-based authorization, administrative user profiles are kept to a minimum.
> - User-dependent authentication with username and password.
> - The use of personal data is limited, so that only authorized individuals can use the personal data necessary for their task (De Minimis Principle).
> - Logging of usage and changes.

- Paperless work by principle and compliant destruction of paper documents with a shredder where applicable.

3.4 Pseudonymization

(...)

> This is often an overshoot, but think of scenarios in which identifiable data is really not that necessary. One common example:
>
> - Customer data is pseudonymized so far as the connection to the individual is not absolutely necessary for the result.

3.5 Separation Control

(...)

> This typically applies to companies managing large amounts of data from various customers:
>
> - Separation of data is ensured for customer data based on software system management, e.g. through data storage in separate folders.

4. Integrity

4.1 Transfer Control

Transfer control shall ensure that only authorized individuals can inspect personal data. Employee mobile devices must be encrypted if personal data is stored on them.

(...)

> How do you keep data safe in transmission? Some example measures:
>
> - The use of single USB flash drives or related data carrier tools is not allowed. Information should only be printed out if absolutely needed. Printed copies must be shredded immediately as soon as they are no longer needed.
> - Home office policies (e.g. connect to VPN)

4.2 Input Control

The company has implemented the following measures for its software systems:

- Traceability of inputs, changes, and deletions by personalized users
- Traceability in assigning, changing, and deleting user authorizations

> This applies to most cloud working environments (e.g. Google Drive, MS Sharepoint, Confluence, JIRA etc.). Any other measures to add in your context?

4.3 Availability and Reliability

- Employees are provided equipment which is state-of-the-art. Example configuration: (...)
- Personal data is processed on data processing systems that are subject to regular and documented patch management. No systems may be linked on the network that are outside of the manufacturer's maintenance cycles (e.g. no Win95, XP, etc). Automatic updates are activated on the computers.
- Continuous availability of high-speed internet is ensured. (Cloud system services can be used with any internet connection.)
- Continuous availability of data is guaranteed by means of redundant storage media and backups of systems according to the latest technical standards.

  Again, if you are using a large cloud provider, you can add more extensive policies and measures here, such as for example:

  - Cloud provider data centers and server rooms are state of the art (temperature control, fire protection, water penetration, uninterrupted power supply (UPS) ensuring controlled shutdown without any loss of data).

4.4 Product Development

4.4.1 Development Tools (...)

As before, think about your own organizational setup. How do you ensure safe development? Some examples:

- Third party applications must be approved prior to use by (...) according to (...) to ensure compliance with quality management and data privacy requirements.
- Development tools must only be downloaded from secure sources (e.g., the manufacturer's servers).
- Where possible, single-sign-on authentication is used for third party applications to allow for a complete and compliant access administration within the organization.
- Less secure third-party applications are disabled by administrator default configurations.

4.4.2 Privacy-Friendly Settings (...)

- Product development must take into account giving users the option of entering only the information necessary for the purpose of processing. Input fields with additional, unnecessary information should be avoided or at least designed as non-mandatory.
- By default, privacy-friendly settings must be preselected.

4.6 Data Deletion

The company implemented the following concept for automatic data deletion:

Data category	Retention period	Responsible
User data	<This period typically should be specified as part of the informed user consent>	
Customer data	- Customer data after termination of contracts- Lead contact data after 10 years of paused communication	
Employee data	Until end of employment	
Applicant data	Until 6 months after hiring decision or longer in case of employment	
Website data	Deleted after every session	Automated

5. Employee Workplace

The company has implemented the following measures:

- Employees must encrypt their hard drives with state-of-the-art encryption, e.g. Apple FileVault 2 for mac OS or equivalent software for other operating systems.
- The email account provider applies a default virus, spam and phishing filter to detect malicious software and avert cyber attacks.
- Employees are required to set up a completely closed firewall for their home office internet network.
- Employees are obligated to clean their desk of any documents containing sensitive data, especially when accessible by others.
- The default option for screen savers must be set at the shortest time period until activation. When temporarily leaving the workplace and hardware, employees should always lock their devices.

6. Procedure for Regular Review, Assessment and Evaluation

Data protection and IT security within the company is reviewed regularly and, based on these assessments, continuously improved. Internal auditing may include data privacy requirements such as:

- Obligation of employees to maintain data secrecy, training and education.
- Regular auditing of data processing procedures.
- Procedures in case of data breaches and the protection of data subjects' rights

The company has implemented the following internal measures:

- Appointment of a data protection officer
- Regular auditing of procedures
- Regular review of technical advancements in accordance with Article 32 GDPR
