GDPR EU Privacy and Data Protection Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, the European Commission, and Swiss Administration to provide organizations with a process to comply with privacy and data protection requirements when transferring personal data from the European Union and Switzerland to the United States.

# II. Purpose

Effective safeguards ensure that European Union (EU) subjects are protected from privacy and data breaches. The safeguards apply to all organizations processing the personal data of subjects residing in the EU regardless of the organization’s location.

# III. Scope

This policy applies to ABC Company Executive Management, Department Heads, the Chief Security Officer, Risk Management Officer, Data Protection Officer, and those responsible for information and physical security.

# IV. Policy

A. Privacy Principles

Organizations that meet Privacy Shield requirements are deemed to provide “adequate” privacy protection, a requirement for the transfer of personal data outside of the European Union (EU) under the EU Data Protection Directive and outside of Switzerland under the Swiss Federal Act on Data Protection. EU Member State requirements for prior approval of data transfers either are waived or approval will be automatically granted.

The Privacy Shield program is administered by the U.S. International Trade Administration (ITA). The Privacy Shield Principles (Principles) include notice, choice, accountability for onward transfer, security, data integrity and purpose, access, and recourse, enforcement and liability.

Notice. ABC Company shall inform individuals about its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List. Such notice shall identify:

* The types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles.
* ABC Company’s commitment to subject to the Principles all personal data received from the EU in reliance on the Privacy Shield.
* The purposes for which ABC Company collects and uses personal information.
* How to contact ABC Company with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints.
* The type or identity of third parties ABC Company discloses personal information, and the purpose.
* The right of individuals to access their personal data,
* Choices and means ABC Company offers individuals for limiting the use and disclosure of their personal data.
* The independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual.
* The possibility, under certain conditions, for the individual to invoke binding arbitration,
* ABC Company’s requirement to disclose personal information in response to lawful requests by public authorities, including national security or law enforcement requirements.
* ABC Company’s liability in cases of onward transfers to third parties.

Choice. ABC Company shall offer individuals a clear, conspicuous, and readily available mechanism to exercise the opportunity to opt out whenever their personal information is to be disclosed to a third party, or used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), ABC Company must obtain affirmative opt-in express consent if such information is to be disclosed to a third party or used for a purpose other than that for which it was originally collected or subsequently authorized by an individual through the exercise of opt-in choice. In addition, ABC Company should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

Accountability for Onward Transfer. When transferring personal information to a third party acting as a controller (determines the purpose and means of the processing of personal data), ABC Company must comply with the above Notice and Choice Principles. ABC Company must also enter into a contract with the third party controller that provides such data shall only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles. The controller shall notify ABC Company if it can no longer meet this obligation. Staff must:

* Transfer such data only for limited and specified purposes.
* Ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles.
* Take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the ABC Company’s obligations under the Principles.
* Require the agent to notify ABC Company if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles.
* Take reasonable and appropriate steps to stop and remediate unauthorized processing.

Security. Staff must take reasonable and appropriate measures to protect data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

Data Integrity and Purpose. Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing. Staff shall not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by an individual. To the extent necessary for those purposes, Staff must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. Staff must adhere to the Principles for as long as it retains such information per the Data Retention Policy.

Access. Individuals must have access and be able to correct, amend, or delete their personal information held by ABC Company except where the burden or expense of providing access would be disproportionate to the risks to the individual’s privacy in the case in question, or where the rights of persons other than the individual would be violated.

Recourse, Enforcement, and Liability. Effective privacy protection shall include robust mechanisms for assuring compliance with the Principles and recourse for individuals who are affected by non-compliance with the Principles. At a minimum such mechanisms must include:

* Readily available independent recourse mechanisms by which an individual’s complaint/dispute is investigated and expeditiously resolved at no cost to the individual.
* Follow-up procedures for verifying ABC Company privacy practice attestations and assertions are true and have been implemented as presented.
* Obligations to remedy problems arising out of failure to comply with the Principles.

Supplemental privacy considerations include sensitive data, journalistic exceptions, secondary liability, performing due diligence and conducting audits, the role of the Data Protection Authorities (DPA), self-certification, verification, access, Human Resources data, obligatory contracts for onward transfers, dispute resolution and enforcement, choice – timing of opt out, travel information, pharmaceutical and medical products, public record and publicly available information, and access requests by public authorities.

B. Data Protection Officer

Executive Management shall ensure a role-based job description for a Data Protection Officer is implemented and maintained.

* The data protection officer shall be designated on the basis of professional qualities and expert knowledge of data protection law and practices.
* The data protection officer may be a Staff member of the organization or fulfil the tasks on the basis of a service contract.
* The organization shall publish the contact details of the Data Protection Officer and communicate them to the supervisory authority.

C. Data Protection technical and organizational measures

The Chief Security Officer (CSO), Risk Management Officer (RMO), and Data Protection Officer (DPO) shall ensure that ABC Company’s privacy and data protection risks are properly managed and mitigated to the extent possible.

Security measures shall include but not be limited to:

* Documents (e.g. agreements, disclosure) that specify the specific purpose for collecting personal data and the minimum amount of personal data to be collected and processed.
* An analysis is performed to determine if special categories (e.g. racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) of personal data are processed.
* Written procedures that ensure personal data remains accurate. Written procedures shall also ensure inaccurate data is corrected or deleted in a timely manner.
* Data flow diagrams document business processes that transmit, receive, create, modify, delete, and access personal data.
* Processes shall ensure that personal data remains secure throughout its lifecycle including data collection, processing, storage, transmission, and disposal.
* An analysis to determine when pseudonymization and encryption shall be used to protect personal data.
* Ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
* Restoring the availability and access to personal data in a timely manner in the event of a physical or technical incident.
* Regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
* Assessing the appropriate level of security, identifying risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored or otherwise processed.
* Ensuring that persons who have access to personal data do not process the data except on approved instructions.

The CSO, RMO, and DPO shall oversee the implementation and maintenance of formal policies including, but not limited to:

* Data classification – Data Classification Policy
* Access controls – Access Control Policy, Password Policy
* Business continuity – Business Continuity Policy
* Compliance – Compliance Policy
* Data retention – Data Retention Policy
* Disposal of sensitive information – Disposal Policy
* Incident management – Incident Response Policy
* Logging and monitoring – Logging Policy, Security Monitoring Policy
* Physical security – Physical Access Policy, Physical Security Policy
* Privacy – Data Privacy Policy, Privacy Policy
* Risk mitigation – Risk Assessment Policy, Risk Management Policy
* Security controls – Anti-Malware Policy, Backup Policy, Change Management Policy, Encryption Policy, Firewall Policy, Patch Management Policy, Ransomware Policy, Security Policy
* Security training – Security Awareness and Training Policy
* Service providers – Cloud Service Provider Policy, Third Party Service Providers Policy, Vendor Access Policy

D. Data Protection impact assessment

Staff shall seek the advice of the Data Protection Officer when carrying out a Data Protection Impact Assessment. A Data Protection Impact Assessment shall be required in the case of:

* A systematic and extensive evaluation of personal aspects which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the person or similarly significantly affect the natural person, or
* Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offenses, or
* A systematic monitoring of a publicly accessible area on a large scale.

The Data Protection Impact assessment shall contain at least:

* A systematic description of the envisioned processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the Controller.
* An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
* An assessment of the risks to the rights and freedoms of data subjects.
* The measures envisioned to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the General Data Protection Regulation (GDPR).

Where necessary, Staff shall carry out a review to assess if processing is performed in accordance with the Data Protection Impact Assessment at least when there is a change of the risk represented by processing operations.

# V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to ABC Company Executive Management, Department Heads, the Chief Security Officer, Risk Management Officer, Data Protection Officer, and those responsible for information and physical security.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM01.01, EDM03.02, APO01.11, APO13.07, APO14.01-02, APO14.07, MEA03.01

GDPR Article 25, 30, 32

HIPAA 164.308(a)(2), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D),

ISO 27001 A.5, A.7.2.2, A.8.1.3, A.8.2.1, A.9-14, A.16-18

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29

NIST Cybersecurity Framework ID.AM-5, ID.GV-3, ID.RA-6, PR.AC-1, DE.DP-2, RS.RP-1

PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8