*Data Privacy Management Policy*

Table of Contents

[Purpose 1](#_Toc4058611)

[Scope 1](#_Toc4058612)

[Policy 2](#_Toc4058613)

[Privacy Governance Program 2](#_Toc4058614)

[Compliance Evaluation 2](#_Toc4058615)

[Privacy Roles and Responsibilities 2](#_Toc4058616)

[Policy and Procedures Requirements 2](#_Toc4058617)

[Personal Information Inventory and Data Flows 3](#_Toc4058618)

[Privacy Assessments 3](#_Toc4058619)

[Program Monitoring and Reporting 3](#_Toc4058620)

[Third Party Screening and Privacy Requirements 4](#_Toc4058621)

[Breach Management 4](#_Toc4058622)

[Privacy Training Requirements 4](#_Toc4058623)

[Internal System Design and Development 4](#_Toc4058624)

[Program Communication 5](#_Toc4058625)

[Third Party Transfer of Subject Information 5](#_Toc4058626)

[Privacy Sanctions Policy 6](#_Toc4058627)

[Violations 6](#_Toc4058628)

[Definitions 6](#_Toc4058629)

[References 7](#_Toc4058630)

[Related Documents 7](#_Toc4058631)

[Approval and Ownership 7](#_Toc4058632)

[Revision History 8](#_Toc4058633)

Purpose

This policy establishes the responsibilities and minimum requirements for the implementation and maintenance of a privacy program at CompanyX (the “Company”). The privacy program is designed to protect all personally identifiable information of employees and customers against accidental disclosure.

Note: This policy conforms to the minimum program requirements of the General Data Protection Regulation (GDPR) as is mapped to these requirements. You must determine if your organization must comply as either a “Controller” or “Processor”.

Scope

This policy applies to all employees, contractors and third-parties responsible for implementing a data privacy governance program.

Policy

### Privacy Governance Program

Formal Privacy Governance Program - CompanyX will establish a formally document a privacy governance program that will secure CompanyX employee and customer personally identifiable information (PII) against unauthorized use or disclosure. CompanyX will assign roles and responsibilities to support the program and communicate the program goals and activities to all personnel.

Privacy Program Contents – At a minimum, the CompanyX data privacy program must support a full set of *Data Subject Rights* that enable the organization to comply with international data protection laws.

**Privacy Sanctions Policy Required** - CompanyX will apply appropriate and consistent sanctions to any personnel or business partners who do not comply with information security and privacy policies. CompanyX sanctions may include disciplinary actions up to and possibly including termination and/or legal prosecution.

### Compliance Evaluation

GDPR Compliance Evaluation – CompanyX must determine if their business practices and current business status require compliance with GDPR. The organization must explicitly declare this decision in a formal management statement. [Ref: GDPR Article 2 and Article 3]

Note: Organizations can be exempt from GDPR provisions by analyzing their Material Scope and Territorial Scope.

Data Collection Analysis – CompanyX management must undertake a data analysis to determine if GDPR data protection is required for the types of data being collected. [Ref: GDPR Art. 11]

### **Privacy Roles and Responsibilities**

Assign Privacy Roles and Responsibilities - CompanyX must assign privacy responsibilities to personnel and incorporate privacy responsibilities into all positions that handle PII.

Designated Privacy Officer - CompanyX will appoint a Chief Privacy Officer to oversee and be responsible for all CompanyX information privacy initiatives, activities and incidents.

Specific Privacy Officer Duties – CompanyX must formally document specific duties of the Chief Privacy Officer as they relate to regulatory requirements. [Ref: GDPR Art. 38.]

Privacy Oversight Council – CompanyX will establish a privacy oversight council to provide input to the privacy governance program, in addition to providing visible support of privacy initiatives from business unit leaders.

Contact with Authorities – As part of the formal privacy governance program, the CompanyX Chief Privacy Officer (CPO) will establish formal contact information and share this information with *Supervisory Authorities*. [Ref: GDPR Art. 37(7), Art. 33(5)]

### Policy and Procedures Requirements

Data Privacy Policies - Policies must be written, implemented and enforced to assure the security, reliability, integrity, and availability of sensitive personal information (PII).

Data Privacy **Procedures** - Procedures must be implemented and enforced to enforce security policies and assure the security, reliability, integrity, and availability of sensitive personal information (PII).

Accidental or unauthorized events - Policies must be implemented and enforced to response to events that compromise the security or integrity of PII, including responding to a possible public breach of PII.

Harm Prevention Policies - CompanyX will establish a formally documented procedures to determine if personal data processes are lawful and do not cause harm according to the Data Privacy Standard. [Ref: GDPR Art. 6(1), Art. 6(4)]

Binding Corporate Rules – CompanyX must develop policies and procedures supporting the transfer of data according to any *Binding Corporate Rules* that apply to the organization. [Ref: GDPR Art. 47(2)]

### Personal Information Inventory and Data Flows

**Comprehensive PII inventory required -** CompanyX must define and document the PII CompanyX handles and communicate this information to personnel to ensure they know and understand what PII CompanyX is responsible for protecting.

**PII Data Flow Assessment** - CompanyX must map the data flows and identify points during the flows where PII is most vulnerable, then create controls and protections as appropriate.

**Key Processing Activities** – As part of the privacy governance program, all key business processes that process PII must be identified and documented. These must be identified as key controls within the corporate Risk Assessment. [Ref: GDPR Art. 30(1)]

### **Privacy Assessments**

**Privacy Impact Procedures -** The Data Privacy Impact Assessment (DPIA) must be conducted according to specific procedures developed by the CPO. The DPIA must analyze the threats to PII and determine what the potential impact to the company in the event a related incident occurred. The Chief Privacy Officer must then calculate the actions and related costs to help prevent such incidents.

**Privacy Impact Assessments -** The CompanyX Chief Privacy Officer, or an approved delegate, must conduct a Data Privacy Impact Assessment (DPIA) before adopting new systems for collecting or processing PII of individuals. In the event that these systems have already been established, a DPIA must be conducted on the existing systems. [Ref: GDPR Art. 24(1), Art. 25(1)]

**Ad-Hoc Privacy Impact Assessments -** CompanyX must also conduct a Data Privacy Impact Assessment (DPIA) in specific situations when there is a material change in the data privacy processing of the business. [Ref: See GDPR Art. 35(1), Art. 35(2), Art. 35(3), Art. 35(6)]

### Program Monitoring and Reporting

**Monitoring of Security and Privacy Laws -** CompanyX must continuously monitor corporate information security and privacy legal compliance, new security and privacy laws and regulations, and update programs as necessary to help ensure compliance.

**Privacy Metrics –** CompanyX must evaluate the Data Privacy Program using industry-established metrics that facilitate comparison with other organizations.

**Data Subject Records –** CompanyX must provide reports to Data Subjects on their personal data history, including full copies of their person data in an acceptable format and notice of any possible data breaches. [Ref: GDPR Art. 17, Art. 19, Art. 20(1), Art. 20(2), Art. 34(2)]

**Privacy Assessment Reports -** The Chief Privacy Officer (CPO) must regularly (e.g., quarterly or biannually) submit a “State of the CompanyX Privacy Environment” to the CompanyX executives. [Ref: GDPR Art. 39(1)]

### Third Party Screening and Privacy Requirements

**Third Party Privacy Impact Assessment** - Satisfactory Privacy Impact Assessments (PIAs) must be performed for third parties, and the results approved by the CPO, before giving the third party processors access to CompanyX PII to manage, process, transfer, or otherwise handle in any other way. [Ref: GDPR Art. 22(4)]

Formal Third Party Contracts - CompanyX must not use third-party data processors unless these same organizations have provided assurances that the organization is in compliance with GDPR principles. [Ref: GDPR Art. 28(3), Art. 28(9)]

Subcontractor Arrangements – CompanyX contracts with third-party data processors must require that those same processors specific that privacy controls must also apply to any subcontractors. [Ref: GDPR Art. 28(4), Art. 28(5)]

Individual Contractors – CompanyX must ensure that any individuals that act on behalf of the organization in handling data subjects must also follow all policies and procedures of CompanyX, including any of those required by contract or Union law. [Ref: GDPR Art. 32(4), Art. 29]

### **Breach Management**

Breach Response Procedures – CompanyX must have written procedures for the handling of a possible breach of subject information. [GDPR Art. 33(1), Art. 33(2), Art. 33(3), Art. 33(4), Art. 34(1), Art. 34(3)]

### Privacy Training Requirements

**Annual Privacy Training Required -** All CompanyX personnel must complete annual privacy training and participate in targeted privacy training as requested.

**Documented privacy education program -** The CompanyX Chief Privacy Officer must ensure the corporate personnel and business partner privacy education program is documented and authorized by the Privacy Oversight Council.

**Targeted privacy training for personnel handling PII -** CompanyX must provide targeted privacy training to groups handling or using PII and provide ongoing awareness messages communicating how to protect PII.

**Regular training of privacy team personnel** - All privacy team members and privacy advocates must participate in regular training, including training for privacy incident response procedures.

### Internal System Design and Development

**Privacy Requirements in Systems Development -** CompanyX must incorporate privacy requirements into the CompanyX systems and applications development life cycle and systems and applications update procedures. [Ref: GDPR Art. 22(3)]

**PII Information Classification –** CompanyX must properly classify personal information (PII) of data subjects so that proper information security controls can be applied to protect the data.

**Personnel Access Limits to PII** - CompanyX must limit the number of people who have access to PII to only those who need it to perform business activities.

**Privacy review of data mining activities -** All CompanyX data mining activities must be authorized and approved by the Chief Privacy Officer to avoid potential violations of CompanyX privacy policies.

**Privacy procedures for CRM activities** - CompanyX will implement procedures to incorporate privacy practices into all customer relationship management (CRM) activities.

### Program Communication

**External Privacy Policy Required** - CompanyX must post a website privacy policy, approved by the Chief Privacy Officer, on the corporate websites. Each page on each website must provide an easy-to-find link to the privacy policy.

**Employee Notice of Privacy Policies** – All CompanyX personnel who handle PII in any manor must be made aware of the privacy policies that apply to them, as well as the sanctions for not complying with policies.

**Clear Notice of PII Privacy Policies -** Whenever CompanyX collects PII, in any location and in any way, clear notice must be given to the individuals from whom it is collected that (1) their information is being collected, and (2) the details of company privacy policies.

### Third Party Transfer of Subject Information

**Approved “Adequate” Data Transfer** – CompanyX must only transfer personal data to a third country or international organization after certain conditions have been validated in accordance with the *Private Data Transfer Procedure*. [Ref: GDPR Art. 44, Art. 45, Art. 46(1), Art. 48]

*(Note: This procedure contains the details for all onward-transfer requirements within the GDPR, including: adequacy, international agreement, verified existence of appropriate safeguards, enforceable data subject rights, and available effective legal remedies. [Ref: GDPR Art. 44, Art. 45, Art. 46(1), Art. 48]* In the event that “transfer adequacy” cannot be achieved, transfer of personal data can only be done if one of the seven GDPR conditions are met. [Ref: GDPR Art. 49(1)]

**Secure Transfer Safeguards (Controls)** – CompanyX must implement specific management and technical controls for the secure transfer of this subject data to third parties. [Ref: GDPR Art. 46(2)]

**Transfer for Lawful Processing**– CompanyX may transfer public data if the subject has opted out (“objected”) in the case where the transfer supports legitimate and documented public-interest, official authority, scientific, and historical-research purposes. [Ref: GDPR Art. 6(1), Art. 21(6)]

### Privacy Sanctions Policy

**CompanyX privacy sanctions policy**

The CompanyX Privacy Sanctions Policy protects the confidentiality, availability and integrity of personally identifiable information as required by law, regulations and the CompanyX ethics policy. All CompanyX employees, business associates and agents must protect the integrity, availability and confidentiality of PII.

Any employee, business associate or agent of CompanyX who believes another employee, business associate or agent has violated any of the CompanyX privacy policies must immediately report such violation to the Corporate Privacy Officer.

An employee, business associate or agent will receive disciplinary action up to and possibly including termination and/or criminal prosecution for not complying with the privacy policies, for a willful or grossly negligent violation of privacy, for breaking privacy-related laws, or any other action in violation of the CompanyX privacy policies, procedures and practices.

All sanctions will be documented and retained for six years.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. CompanyX reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. CompanyX does not consider conduct in violation of this policy to be within an employee’s or Third-Party’s course and scope of employment, or the direct consequence of the discharge of the employee’s or Third-Party’s duties. Accordingly, to the extent permitted by law, CompanyX reserves the right not to defend or pay any damages awarded against employees or Third-Parties that result from violation of this policy.

Any employee or Third-Party who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

Definitions

**Binding Corporate Rules** - A set of agreed-upon rules for the security transfer of data between organizations within the same business type or joint economic activity. [Ref. GDPR Recital 110]

**Data Controller –** ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. [Ref: GDPR Art.4-7]

**Data Processor** – The term ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; [Ref: GDPR Art.4-8]

**Data Subject –** Refers to any consumer that falls under the scope of GDRP and would be providing personal information directly to a *Data Controller*.

**Data Subject Rights** – This refers to the set of specific rights that an individual had with respect to the control of their personal information. [Ref: GDPR Art.12-23]

**Information Asset –** Any CompanyX data in any form, and the equipment used to manage, process, or store CompanyX data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

**Personally Identifiable Information (PII)** – Information that alone, or when combined with other personal or identifying information can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

**Processing** – The term ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. [Ref: GDPR Art.4-2]

**Privacy Program** **-** The guidance provided that will enable CompanyX to maintain information about individuals while protecting the right of the individuals against unwarranted or illegal invasions of their privacy.

**Third Party Processor -** Any non-employee of CompanyX who is contractually bound to provide some form of service to CompanyX.

**User -** Any CompanyX employee or Third-Party who has been authorized to access any CompanyX electronic information resource.

References

ISO 27002: 18.1.4 Privacy and protection of personally identifiable information

NIST: Appendix J: Privacy Controls (800-53 V5 P Controls)

US-CSF: PR.DS-9: Privacy of individuals and (PII) is protected

GDPR: General Data Protection Regulation

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | 10/05/2019 | MM/DD/YYYY |  |
|  |  |  |  |  |