Information Security Policies

Sample Privacy Policy - Stringent

Policy #	IS-00	Effective Date	MM/DD/YYYY	Email	contact@companyx.com
Version	1.0	Contact	Policy Contact	Phone	888.123.4567

Table of Contents

Purpose....1
Scope....1
Terms and Definitions....2
Specific Privacy Requirements....2
Information to be Given to the Individual....4
Individual's Right Of Access To Data....4
Individual's Right To Object....5
Disclosure Of Personal Data To Third Parties....5
Processing Confidentiality And Security....6
Monitoring Of Internal Activities....7
Violations....8
References....8
Related Documents....8
Approval and Ownership....8
Revision History....8

PURPOSE

Company X supports the right to privacy, including the rights of individuals to control the dissemination and use of personal data that describes them, their personal choices, or life experiences. In the course if its business, it is necessary for Company X to record, store, process, transmit, and otherwise handle private information about individuals. Company X takes these activities seriously and provides fair, secure, and fully-legal systems for the appropriate handling of this private information. All such activities at Company X are intended to be consistent with both generally accepted privacy ethics and standard business practices.

SCOPE

This policy applies to all Company X employees, contractors, temporaries, and consultants, and other workers. All of these people are expected to be familiar with and fully in compliance with these policies. Workers who are not in compliance are subject to disciplinary action up to and including termination.

This policy also applies to outsourcing organizations that perform information-processing services on behalf of Company X. Use of outsourcing organizations to process personal data

must always include a contractual commitment to consistently observe these policies and related Company X procedures and standards as specified by the Information Security department. All outsourcing organizations handling personal data provided by Company X must periodically issue certificates of compliance with this policy, and permit Company X to initiate independent audits to determine compliance with this policy.

Terms and Definitions

Personal data - Any information relating to an individual. Such data includes name, address, telephone number, address, social security number, driver's license number, and personal business transaction details. For example, such a person could be a purchaser of Company X products. The following policies do not apply to statistical reports or other collections of information in which specific natural persons are not identifiable.

Processing of personal data or "processing" - Any operation or set of operations performed on personal data, whether by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, combination, blocking, erasure or destruction.

Owner - The Company X manager or executive, who determines the purposes for processing personal data, and who makes decisions about the security mechanisms to be used to protect such personal data.

Custodian - The Company X manager, or third-party organization manager if processing is outsourced, who processes personal data according to the instructions provided by the Owner.

Third party - Any person, partnership, corporation, public authority, government agency, or any other entity other than the individual, Owner, Custodian, and the persons who, under the direct authority of the Owner or the Custodian, are authorized to process the data.

Recipient - The person, public authority, government agency, or any other entity to whom personal data is disclosed, even if the recipient is a third party.

Consent - Any freely-given informed indication of his or her wishes by which the individual signifies his or her agreement to have his or her personal data processed, which may include disclosure.

Partner – Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

User - Any Company X employee or partner who has been authorized to access any Company X electronic information resource.

Specific Privacy Requirements

1. All personal data must be processed fairly and lawfully, according to the laws and regulations of all jurisdictions where Company X does business.

2. Personal data must be collected for purposes communicated to the individual and not further processed in a way incompatible with those purposes. Further processing of such data for historical, statistical or other business purposes is not incompatible with the

original purpose provided the further processing includes adequate additional controls protecting the rights of the individual.

3. The amount of personal data collected must be adequate, relevant, and not excessive in relation to the purposes for which they are collected or for which they are further processed.

4. Personal data must be accurate and complete, and where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate or incomplete, keeping in mind the purposes for which it was collected or for which it is further processed, are definitively erased or corrected.

5. Individuals must be given an opportunity to examine, and issue complaints about, inaccuracies and in-completions in records containing their personal data. Investigations of complaints must be performed promptly, and must be answered with a letter informing the involved individuals about the courses of action that Company X will take. Any resulting erasures or corrections must be performed promptly and at no cost to the individuals. Reasonable steps to prevent reoccurrence of the same inaccuracies or in-completions must also be taken, for instance by adding an explanatory paragraph in the subject's file. An exception to the requirements stated in this paragraph is permitted for personal data in management succession planning records, criminal activity investigation records, and other legitimate business activities where disclosure to the individual would be highly likely to jeopardize the project underway.

6. Personal data must not be kept in a form that permits identification of individuals for any longer than is necessary for the purposes for which the data was collected or for which it is further processed. For example, this can be implemented with linked separate files respectively containing identification information and related sensitive information. Owners of personal data are responsible for ensuring that items in the preceding points are complied with.

7. Personal data may be processed only if:
    - The individual has given his or her consent unambiguously.
    - Processing is necessary for the performance of a contract to which the individual is party, such as completing an order for goods.
    - Processing is required to respond to a request made by the individual.
    - Processing is necessary for compliance with a legal obligation to which the Owner is subject.
    - Processing is necessary in order to protect the vital interests of the individual.
    - Processing is necessary to explore or provide new business products or services that may be of use to the Owner, as long as these new products or services do not override the fundamental rights or freedoms of the individual.

8. Processing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, criminal offenses, health, or sex life is prohibited unless:
    - The individual has provided explicit consent to such processing.
    - Processing is necessary for the purposes of carrying out the obligations and specific rights of the Owner in the field of employment law.
    - Processing is necessary to protect the vital interests of the individual or of another person where the individual is physically or legally incapable of giving his

or her consent. Custodians of personal data are responsible for ensuring that items in the preceding two points are complied with.

Information to be Given to the Individual

The Owner or his or her representative must provide individuals with the following information:

- The identity of the Custodian and of his or her representative, if any.
- The purposes of the processing for which the data is intended.
- The policies related to handling personal data, including material changes to these policies that have gone into effect since the personal data was collected.
- Any further information such as:
    - The recipients or categories of recipients of the data.
    - Whether replies to the questions are obligatory or voluntary, and the possible consequences of the failure to reply.
    - The existence of the right of access to and the right to correct the data concerning the individual.

Where personal data has not been obtained directly from the individual, the Owner or his or her representative must notify the individual at the time when personal data will be processed. If a disclosure to a third party is anticipated, the individual must be notified no later than the time when the data is disclosed. The Owner must provide the individual with at least the following information, except where the individual already knows it:

- The identity of the Custodian and the Custodian's representative, if any.
- The purposes of the processing.
- Any further information such as:
    - The categories of data concerned.
    - The recipients or categories of recipients.
    - The existence of the right of access to and the right to correct information concerning the individual.

Upon request, the Owner or his or her representative must provide all individuals with a brief written summary of the subject's rights to learn about, get copies of, lodge objections to, and correct personal data. Trained personnel who can explain an individual's rights must be available to subjects by telephone.

If Company X changes its privacy policy, an attempt to notify all individuals must be promptly initiated. As a part of this notification, Company X must provide individuals with a summary of the words that have changed and what these changes mean. Individuals also must be given an opportunity to be removed from Company X records.

Individual's Right Of Access To Data

Every individual has the right to obtain the following from the Custodian:

1. Without undue constraint at reasonable intervals and without excessive delay or expense:

- Confirmation as to whether data relating to him or her is processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data is disclosed.
- Details as to the source of information about the individual, if such information is recorded.
- Communication of the personal data to the subject in an intelligible form.
- Knowledge of the logic involved in any automatic processing of data concerning him or her at least in the case of the automated decisions affecting the individual.

2. When appropriate, an indication that his or her personal data has been corrected, erased, or blocked because it was incomplete or inaccurate.

3. Notification to third parties to whom the data has been disclosed of any correction, erasure, or blocking carried out in compliance with the prior paragraph, unless this proves impossible or involves a unreasonable effort or expense.

Individual's Right To Object

Individuals may object, free of charge, to the processing of personal data that the Owner anticipates will be processed for the purposes of direct marketing. Owners must provide prompt processing mechanisms that permit individuals who objected to be removed from direct marketing lists.

Individuals must be informed before personal data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing. Individuals must be expressly offered the right to object free of charge to such disclosures or uses. Owners must provide processing mechanisms that permit individuals who objected to block such a disclosure.

Disclosure Of Personal Data To Third Parties

Company X may provide third parties with personal data processed on its systems for generally accepted business purposes such as court orders, subpoenas, employment verification, governmental licensing, underwriting, and other reasons. All recipients of such information must definitively identify themselves, certify in writing the legal and customary purposes for which the information is sought and certify that the personal data will be used for no other purposes.

All disclosures to government agencies and other third parties must be preceded by written or other notice sent to the individual. A blanket, one-time approval of such disclosures is sufficient. Sufficient time must be provided between the receipt of such notice to the individual and the actual disclosure to the third party to permit the individual to object, should he or she so elect.

Processing Confidentiality And Security

The Owner must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss, unauthorized

alteration, and unauthorized disclosure or access. These measures must be consistent with the standards and procedures issued by the Information Security department.

Transfers of private information to another country, no matter what technology is employed, must not take place unless prior approval of the Information Security manager has been obtained. An exception is made in those cases where the individual is, was, or will be located in the destination country, or when the individual has specifically requested such a transfer.

Company X information systems or staff must not link anonymous information about individual behavior or activities with personally-identifiable information unless the involved individuals have given their consent. For example, such a linkage could tie Internet shopping purchase information with web browsing logs.

The Owner or his or her designated representative must prepare a documented risk assessment to determine the privacy implications of all significantly new or different uses of personal data. Such a risk assessment must be completed before these uses take place, and must include all steps in the proposed processing, including access, storage, transmission, and destruction. Such a risk assessment must include not only consideration of the risks, but also the security measures to be employed such as access controls, encryption, logs, data retention schedules, and data destruction procedures.

When building, testing, enhancing, and maintaining processing systems, developers must not use actual personal data. Instead, they must use fictional or sanitized personal data that preserves the essential characteristics of the data, but that does not relate to identifiable individuals. In emergency situations where processing with actual personal data is required, use of such information is permitted under strict security procedures defined by Information Security.

All user access to processing systems and networks containing personal data must be logged so that every recent access to personal data can be traced to a specific user. Custodians of these systems and networks are responsible for the routine monitoring of such logs and the follow-up on potential security-relevant events.

When not in use, personal data must be stored in encrypted form if held in a computer or network, or in locked or similarly secured containers if held in paper, microfiche, or other non-computerized form. When sent over public computer networks such as the Internet, personal data must be protected by encryption. Procedures and standards issued by Information Security provide additional details on these topics.

When they are no longer needed, all copies of personal data, including those on backup tapes, must be irreversibly destroyed according to standards and procedures defined by the Information Security department. A document describing the personal data destroyed and the reasons for such destruction must be prepared for each destruction process, and promptly submitted to the relevant Owner. Permission to destroy personal data may be granted by only the Owner, and only if all legal retention requirements and related business purposes have been met.

The use of cookies, web bugs, images, and other techniques to covertly gather information about individuals who use the Internet is incompatible with this policy. Whenever Company X gathers information about individuals, these same subjects must have agreed upon the collection effort in advance. For this same reason, Company X does not deposit cookie files on

individual hard drives or does not perform any other covert recording of the Internet activity in which individuals have engaged.

Company X streamlines and expedites all of its computerized business interactions with individuals, but at the same time to be forthright and clear about its privacy policies. To support these objectives and to encourage individuals to use Internet commerce sites and other computerized business systems, Company X adopts and supports all generally-accepted standards for web content rating, web site privacy protection, and Internet commerce security, including third-party seals of approval.

Company X does not use externally-meaningful identifiers as its own internal individual account numbers. For example, to prevent identity theft, Company X customer account numbers must never be equivalent to social security numbers, driver's license numbers, or any other identifier that might be used in an unauthorized fashion by a third party.

Monitoring Of Internal Activities

In general terms, Company X does not engage in blanket monitoring of internal communications. It does, however, reserve the right at any time to monitor, access, retrieve, read, or disclose internal communications when a legitimate business need exists that cannot be satisfied by other means, the involved individual is unavailable and timing is critical to a business activity, there is reasonable cause to suspect criminal activity or policy violation, or monitoring is required by law, regulation, or third-party agreement.

At any time, Company X may log web sites visited, files downloaded, and related information exchanges over the Internet. Company X may record the numbers dialed for telephone calls placed through its telephone systems. Department managers may receive reports detailing the usage of these and other internal information systems, and are responsible for determining that such usage is both reasonable and business-related.

All files and messages stored on Company X processing systems are routinely backed up to tape, disk, and other storage media. This means that information stored on Company X information processing systems, even if a worker has specifically deleted it, is often recoverable and may be examined at a later date by system administrators and others designated by management.

At any time and without prior notice, Company X management reserves the right to examine archived electronic mail, personal computer file directories, hard disk drive files, and other information stored on Company X information processing systems. This information may include personal data. Such examinations are typically performed to assure compliance with internal policies, support the performance of internal investigations, and assist with the management of Company X information processing systems.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Company X reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

Company X does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Company X reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner 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.

References

ISO 27002 – 15.1.4 Data protection and privacy of personal information.

Related Documents

Sample Privacy Policy - Lenient

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	MM/DD/YYYY	MM/DD/YYYY	