PSIL CONFIDENTIALITY OF PERSONAL INFORMATION

Category: Complying with Laws and Regulations
Policy: Confidentiality of Personal Data
Geographic Scope: Ireland
Issuing Organisation: Pramerica Systems Ireland Ltd.

POLICY

Pramerica Systems Ireland Ltd (PSIL) requires that all personal data about its customers, employees, vendors, and business partners must be kept secure and confidential. Access to personal data must be limited to employees who need the information or access to it to perform their job responsibilities. Employees may not access or disclose personal data for any purpose except as authorized for PSIL's business purposes.
(For the definition of "personal data" and "sensitive personal data" under this policy, refer to the "Additional Information" section below. "Sensitive personal data has additional protections at law, however we use the term "personal data to include both sensitive and non-sensitive data.)

PURPOSE

The purpose of this policy is to provide a framework to protect our customers', employees', business partners', and vendors' personal data, and keep it secure and confidential.

SCOPE

This policy applies to all PSIL officers and employees. At a minimum, the following should be in place.

Appropriate Security Measures

Measures must be implemented to ensure an appropriate level of security, considering both the nature of the data, and the harm that might result from unauthorised, accidental, or unlawful processing, destruction, loss, or damage. When personal data is transmitted over a public network, it should be encrypted.

Written Contract

A written contract is required when the services of a third-party are engaged to process personal data. Informal or ad hoc arrangements are not acceptable. The contract must provide that the third-party:

a) Executes processing only on PSIL's instructions and provides appropriate security measures.
b) Provides sufficient guarantees in respect to technical and organisational security measures.
c) Takes reasonable steps to ensure compliance with those measures
d) Will assist PSIL in the event of a data breach or investigation concerning the personal data.

Fair Processing

Data will not be seen as having been processed fairly unless the following is made available at the time the data is obtained:

a) PSIL is clearly identified as assuming responsibility for the data.
b) The purpose(s) for which the data is intended (data can be used for many purposes, what is key is transparency around that).
c) Any other relevant information so processing will be fair to the data subject, such as the existence of rights of access and rectification available to the data subject.

In any other case, the above information must be provided to the data subject not later than the first time the data is processed, or before disclosure of data to a third-party.

Additional Conditions

At least one of the following conditions must be met to process Personal data:

a) The data subject has given explicit consent. When the data subject by reason of physical or mental incapacity is unlikely to understand the effect of giving consent, another family member can give consent however such circumstances are rare and specific advice must be sought by you in such situations by contacting the Privacy Officer.
b) Processing is necessary for the performance of a contract to which the data subject is a party; or to take steps at the request of the data subject prior to their entering into a contract.
c) Processing is necessary to comply with a legal obligation.
d) To protect the data subject's vital interests.
e) Processing is necessary for the administration of justice.
f) Processing is necessary to perform a Government function, or other function of a public nature, or function conferred on an individual under an enactment.
g) Processing is necessary for the legitimate interests of PSIL, except where the processing is unwarranted due to prejudicing the rights, freedoms, and legitimate interests of the data subject.

Processing Sensitive Data

Additionally, to process sensitive data, at least one of the following conditions must be met:

a) The data subject has given explicit consent. When the data subject by reason of physical or mental incapacity is unlikely to understand the effect of giving consent, another family member can give consent.
b) Processing is necessary to comply with legal obligations connected with employment.
c) To protect the data subject s vital interests including damage to health or property where it is not possible to obtain consent; or where another person's health or property could be damaged when consent is unreasonably withheld.
d) Processing by a non-profit organisation with the appropriate safeguards as part of its legitimate activities. Processing must relate only to members of the non-profit or to individuals who have regular contact with the orginisation, and the processing does not involve disclosure to a third-party without the data subject's consent.
e) The data subject has made the information public.
f) Processing is necessary to perform a Government function, or a function conferred on an individual under an enactment.
g) Processing is necessary to obtain legal advice, connected with legal proceedings, or for defending legal rights.
h) Processing is needed for medical purposes undertaken by a health professional or another individual subject to a similar duty of confidence as the health professional.
i) Processing for purposes under the Statistics Act of 1993.
j) Processing is carried out by political parties, candidates, or office holders in the course of electoral activities for compiling data on political opinions.
k) Processing is authorised by a government Ministry.
l) The data subject provided data for assessment or payment of tax or duty owed.
m) Processing is necessary to determine entitlement to, or control of, state benefits.

RESPONSIBILITIES

Senior Management is responsible for establishing supervisory procedures to comply with this policy. Additionally, Senior Management is responsible for:

- Enforcing this policy and taking prompt, effective, corrective action to protect personal data upon notice of a violation; and
- Ensuring that personal data is not disclosed to a third-party vendor unless:
  a) An agreement with proper protections is in place and approved by the Law Department; or,
  b) The disclosure is required or permitted by applicable law without such an agreement.

Senior Management is further responsible for providing the structure for controlling the content and use of personal data in compliance with the following seven data protection principles:

- Personal data must be obtained and processed fairly. An employee should be told how the data will be used and that it should not be used outside that reason.
- Data should be accurate, complete, and up to date.
- Personal data should be obtained for legitimate purposes only. Use of Personal data beyond these may result in prosecution under Irish data protection laws.
- Personal data shall not be further processed in a manner other than its legitimate purpose.
- Ensuring Personal data collected is adequate, relevant, and not excessive in relation to the purpose for which it was legitimately collected.
- Personal data shall not be kept for longer than is necessary.
- Appropriate security measures must be taken against unauthorized access, or alternation, disclosure, destruction, or accidental loss of Personal data.

The Compliance Department is responsible for setting and maintaining the Company Privacy Policy in the United States, which also provides assistance to Prudential International businesses (including PSIL) to help them fulfill their obligations under this policy and applicable law.

The Privacy Officer is responsible for administering the Privacy Program and appointing and monitoring the privacy activities of the roles described below.

The Business Information Security Officer (BISO) is responsible for overall information security management.

Records Information Management Specialists (RIMS) are responsible for records retention.

Law Department is responsible for providing legal assistance and guidance to businesses (including PSIL) with the drafting of contracts where disclosure of personal data to a third-party vendor may be necessary.

All Employees are responsible for protecting the security and confidentiality of Personal / Sensitive Personal data in compliance with the requirements of their business. As part of this policy, employees are responsible to:

- Limit access to Personal / Sensitive Personal data to authorized employees whose work requires use of the information;
- Not accessing or disclosing Personal / Sensitive Personal data for any purpose except as authorized for PSIL's business purposes;
- Notifying management and your privacy officer of any unauthorized access or disclosures they believe may have occurred; and,
- Not disclosing Personal / Sensitive Personal data after the termination of employment unless permitted or required by law.

In any situation in which an employee is unsure what action to take (or refrain from taking), s/he is responsible for seeking guidance from his/her manager, the Privacy Officer, local business ethics contact or Global Business Ethics & Integrity.

ADDITIONAL INFORMATION

Definition of Personal Data

Data relating to a living individual who is, or can be, identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of PSIL. This data may include, but is not limited to:

Name, home and work address, date of birth, gender, age, nationality/citizenship, highest level of education, work e-mail address, home and work telephone number, and marital status.

Job title, job status, performance ratings, job history, training, date of hire, promotions and promotion dates, employment termination date, reason for employment termination, salary, bonuses, pay grade, pay or compensation plan, exchange rates, and equity plan awards and grants.

Personal bank, brokerage, and securities account information, tax related information and tax identification number.

Data relating to the investigation of employee complaints and violations of company policy.

Sensitive Personal Data

In addition, Personal data is regarded as Sensitive when it includes the subject's :

a) Racial or ethnic origin, political opinions religious or philosophical beliefs;
b) Trade union membership;
c) Physical or mental health or condition, or sexual life;
d) Commitment, or alleged commitment, of an offence or any proceedings for an offence committed, or allegedly committed, by the data subject, the disposal of such proceedings, or the sentence of any court in such proceedings.

Disclosure

PSIL will, upon request from an individual, the Data Protection Commissioner, or other regulatory authority, reply to any inquiries on a timely basis and disclose sensitive personal data without delay as long as it does not violate any local Irish/ and guidelines issued by the Data Protection Commissioner ordinances.

Complaint Handling

The Company shall do its best to appropriately and promptly handle complains about personal information. The Privacy Officer shall handle any complaints and respond to Irish or other authorities or as to any inquiries regarding personal information. If necessary, the Privacy Officer will seek outside counsel expertise if Pramerica receives a data protection law request from non Irish regulators as they may not have jurisdiction, but can be difficult to disengage. from if an engagement commences.

Handling Privacy Information Leaks

In case of personal information leaks, PSIL must follow the GBTS Privacy Leakage Program procedures. This includes reporting to supervising regulatory agencies immediately. Additionally, an announcement regarding the details and preventive measures against reoccurrences should be made and the details must be notified to relevant parties.

Rights of Data Subjects

If an individual believes their personal data is being maintained by PSIL and provides a written request to determine whether that is the case, PSIL will respond within 21 days. The response will include a description and purposes in the event PSIL is maintaining the individual's data. In addition, further rights related to the following are relayed to data subjects under Irish and European Union Data Protection laws:

a) Access (with certain restrictions)
b) Recertification/Erasure
c) Processing that may cause damage or distress
d) Automated decision making
e) Direct marketing

Refer to the Irish Data Protection Acts of 1988 and 2003 and EC Directive 95/46/EU as to data privacy requirements). Note that EU data privacy law is expected to undergo a major transformation in the next 18/24 months, and so this policy is as a result under constant review.