AMO Consultancy

Tailor-made applications to do exactly what you want, exactly how you imagined it.

ISPMS Personally Identifiable Information Policy

Last updated 04/06/2024

1 Introduction

The Organisation needs to collect and use certain types of information about staff, clients and other individuals who come into contact with the company in order to operate. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, government agencies and other bodies.

This personally identifiable information (referred to as PII) must be dealt with properly, however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this is within the EU General Data Protection Regulation and the Data Protection Act 2018.

We regard the lawful and correct treatment of PII as very important to successful operations, and to maintaining confidence between those with whom we deal and ourselves. We ensure that our Organisation treats personal information lawfully and correctly. This PII Policy is intended to be used in conjunction with the Organisation's established ISO 27001 Information Security Management System (including the Data Protection Policy). It therefore assumes that the requirements of the ISMS have already been determined and implemented.

The PII Policy forms part of the Organisation's suite of ISMS Policies and is not intended to be used on a standalone basis. The Organisation verifies its support for and commitment to achieving compliance with applicable PII protection legislation and/or regulation and commitment to the contractual terms agreed between the Organisation and its partners, its subcontractors and its applicable third parties (customers, suppliers etc.), which should clearly allocate responsibilities between them.

2 Terms & Definitions

2.1 Personally Identifiable Information (PII)

Any information that (a) can be used to identify the PII Principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII Principal.

2.2 PII Principal

Natural person to whom the personally identifiable information (PII) relates.

2.3 Data Controller

A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any PII are or are to be processed.

2.4 Data Processor

In relation to PII, means any person (other than an employee of the data controller, and either alone or jointly or in common with other persons) who processes the data on behalf of the Data Controller.

3 Responsibilities

This policy relates to all information that is dealt with by all employees and may include contractors, sub-contractors and other third parties who have access to information as a result of being connected in any way to the Organisation network, applications, systems and data.

If you are not sure about any aspect of this Policy, please contact the ISMS Manager.

4 Objectives

The Organisation needs to collect and use information about staff, clients and other individuals who come into contact with the company. In addition, it may be required by law to collect and use information to comply with statutory obligations of Local Authorities, government agencies and other bodies.

We view the lawful and correct treatment of PII as very important to successful operations and to maintaining confidence between those with whom we deal and ourselves. Our primary objective is to ensure that our Organisation treats personal information lawfully and correctly.

In addition, the Organisation aims to ensure that information is dealt with in accordance with the EU General Data Protection Regulation and the Data Protection Act 2018.

5 PII Policies & Procedures

5.1 Data Controller or Data Processor?

In its contractual relationships with customers, the Organisation first establishes whether it is a Data Controller or Data Processor. The roles may not be the same across all contracts, so, where the Organisation acts in both roles (e.g. a PII controller and a PII processor), separate roles are determined, each of which is the subject of a separate set of controls. Please see 'Key Definitions' above to facilitate this determination of role.

5.2 PII Risk Assessment

ISO 27001 risk assessment processes are applied to PII in order to identify risks associated with the loss of confidentiality, integrity and availability. GDPR privacy risk assessment processes are applied in order to identify risks related to the processing of PII.

5.3 PII Point of Contact

Mr Bertrand Piquet has been appointed to fulfil the following responsibilities:

- Be independent and report directly to the Board of Directors in order to ensure effective management of privacy risks
- Be involved in the management of all issues which relate to the processing of PII
- Be expert in data protection legislation, regulation and practice
- Act as a contact point for supervisory authorities

- Inform top-level management and employees of the Organisation of their obligations with respect to the processing of PII
- Provide advice in respect of privacy impact assessments conducted by the Organisation.

5.4 Device applicability

No distinction is made between different types of device or physical media on which PII may reside.

5.5 PII Awareness

Measures are in place, including awareness of incident reporting, to ensure that relevant staff are aware of the possible consequences to the Organisation, to the staff member and to the PII Principal of breaching privacy or security rules and procedures, especially those addressing the handling of PII.

5.6 PII Classification

The Organisation's information classification system explicitly considers PII as part of the scheme it implements. Considering PII within the overall classification system is integral to understanding what PII the Organisation processes (e.g. type, special categories), where such PII is stored and the systems through which it can flow.

5.7 PII Stored on Removable Media

It is the policy of the Organisation to not use removable media for any purpose.

5.8 PII Stored on Physical Media

It is the policy of the Organisation to not use physical media for any significant purpose.

5.9 User Registration and De-registration

The ISPMS Manager must be informed immediately if user access control for users who administer or operate systems and services that process PII has been compromised, such as the accidental or deliberate release of passwords. De-activated or expired user IDs for systems and services that process PII must never be reissued.

In pre-defined cases where PII processing is being provided as a service, it is permissible for the customer to be responsible for some or all aspects of user ID management. Such cases must be included in the documented information.

No authentication credentials related to systems that process PII are to remain unused. Regular checks are to be made to ensure that no unused credentials exist.

5.10 PII User Access Provisioning

The Organisation maintains an accurate, up-to-date record of the user profiles created for users who have authorised access to the information systems and the PII contained in them. This profile comprises the set of data about that user, including user ID, necessary to implement the identified technical controls providing authorised access.

Implementing individual user access IDs enables appropriately configured systems to identify who accessed PII and what additions, deletions or changes they made. As well as protecting the Organisation, users are also protected as they can identify what they have processed and what they have not processed. In the case where the Organisation is providing PII processing as a service, the customer can be responsible for some or all aspects of access management. Where appropriate, the Organisation should provide the customer the means to perform access management, such as by providing administrative rights to manage or terminate access. Such cases should be included in the documented information.

5.11 Cryptography

Some jurisdictions can require the use of cryptography to protect particular kinds of PII, such as health data, resident registration numbers, passport numbers and drivers' licence numbers.

The Organisation provides information to the customer regarding the circumstances in which it uses cryptography to protect the PII it processes. The Organisation also provides information to the customer about any capabilities it provides that can assist the customer in applying their own cryptographic protection.

5.12 Secure Disposal or Re-use of Equipment

The Organisation ensures that, whenever storage space is re-assigned, any PII previously residing on that storage space is not accessible.

On deletion of PII held in an information system, performance issues can mean that explicit erasure of that PII is impractical. This creates the risk that another user can access the PII. Such risks are avoided by specific technical measures.

For secure disposal or re-use, equipment containing storage media that can possibly contain PII is treated as though it does contain PII.

Note: The equipment hard disk drive is typically securely erased before equipment disposal.

5.13 Information Backup

The Organisation's information is backed up in accordance with the Backup Policy. Particular care is taken when backing up PII, ensuring that such backups are maintained in an encrypted environment.

The Organisation ensures that the customer has been informed of the limits of the service regarding backup.

Specific requirements regarding the frequency of backups of PII, the frequency of reviews and tests of backup, or regarding the recovery procedures for PII may be legally or organisationally defined. If applicable, the Backup Policy defines how the Organisation demonstrates compliance with these requirements.

Whenever PII needs to be restored, processes are in place to ensure that the PII is restored into a state where the integrity of PII can be assured, and/or where PII inaccuracy and/or incompleteness is identified, and processes put in place to resolve them.

The Organisation has a procedure for, and a log of, PII restoration efforts. As a minimum, the log contains:

- The name of the person responsible for the restoration
- A description of the restored PII.

Specific requirements regarding content of the logs of PII restoration efforts may be legally or organisationally defined. If applicable, the Backup Policy defines how the Organisation documents compliance with these requirements for restoration log content, along with the conclusions of any associated discussions.

5.14 Event Logging

Where possible, event logs record access to PII, including by whom, when, which PII principal's PII was accessed, and what (if any) changes were made (additions, modifications or deletions) as a result of the event.

Where multiple service providers are involved in providing services, there can be varied or shared roles in implementing this guidance. These roles are clearly defined and included in the documented information, and agreement on any log access between providers is addressed.

5.14.1 Implementation guidance for when the Organisation acts as a PII Processor:

The Organisation defines criteria regarding if, when and how log information can be made available to or usable by the customer. These criteria are made available to the customer.

Where the Organisation permits its customers to access log records controlled by the Organisation, the Organisation implements appropriate controls to ensure that:

- The customer can only access records that relate to that customer's activities
- Cannot access any log records which relate to the activities of other customers
- Cannot amend the logs in any way.

5.14.2 Protection of Log Information

Log information is held where possible as a system record with access restricted to those with appropriate administrator authorisation.

6 Information Transfer Policies & Procedures

The Organisation considers procedures on a case-by-case basis for ensuring that rules related to the processing of PII are enforced throughout and outside of the system, where applicable.

6.1 Confidentiality or non-disclosure agreements

The Organisation ensures that individuals operating under its control with access to PII are subject to a confidentiality obligation. The confidentiality agreement, whether part of a contract or separate, specifies the length of time the obligations should be adhered to.

When the Organisation acts as a PII processor, a confidentiality agreement, in whatever form, between the Organisation, its employees and its agents ensure that employees and agents comply with the policy and procedures concerning data handling and protection.

6.2 Securing Application Services on Public Networks

The Organisation ensures that PII which is transmitted over untrusted data transmission networks is encrypted for transmission.

Untrusted networks can include the public internet and other facilities outside of the operational control of the Organisation.

6.3 Secure Systems Development

Systems and/or components related to the processing of PII are designed following the principles of privacy by design and privacy by default, and to anticipate and facilitate the implementation of relevant controls for PII controllers and PII processors respectively, in particular such that the collection and processing of PII in those systems are limited to what is necessary for the identified purposes of the processing of PII.

For example, an organisation that processes PII should ensure that it disposes of PII after a specified period. The system that processes PII should be designed in a way to facilitate this deletion requirement.

The Secure Development Policy has considered the following aspects and includes appropriate requirements where deemed necessary:

- Guidance on PII protection and the implementation of the privacy principles (see ISO/IEC 29100) in the software development lifecycle
- Privacy and PII protection requirements in the design phase, which can be based on the output from a privacy risk assessment and/or a privacy impact assessment
- PII protection checkpoints within project milestones
- Required privacy and PII protection knowledge
- By default, minimise processing of PII
- By default, the collection of information must be limited to what is necessary for the identified purposes of the processing of PII.
- Systems and/or components related to the processing of PII must be designed in accordance with the principles of privacy by design and privacy by default.
- Outsourced systems and/or components related to the processing of PII must be designed in accordance with the principles of privacy by design and privacy by default.

If outsourced development is utilised, then the following is considered:

- Developer contracts
- Developer compliance with Organisation development methods and source code control
- Monitoring methods used for control and associated records.

6.4 Protection of Test Data

If genuine PII is used for testing purposes, a risk assessment must be undertaken and used to inform the selection of appropriate mitigating controls.

7 Addressing Security within Supplier Agreements

The Organisation specifies in agreements with suppliers whether PII is processed and the minimum technical and organisational measures that the supplier needs to meet in order for the Organisation to meet its information security and PII protection obligations.

Supplier agreements clearly allocate responsibilities between the Organisation, its partners, its suppliers and its applicable third parties (customers, suppliers, etc.) taking into account the type of PII processed.

7.1 Implementation guidance for when the Organisation acts as a PII Processor:

The organisation should specify in contracts with any suppliers that PII is only processed on its instructions.

7.1.1 Responsibilities and Procedures

As part of the overall information security incident management process, the Organisation has established responsibilities and procedures for the identification and recording of breaches of PII (documented in the Security Incident Reporting Policy).

Additionally, the Organisation establishes responsibilities and procedures related to notification to required parties of PII breaches (including the timing of such notifications) and the disclosure to authorities, taking into account the applicable legislation and/or regulation.

8 Response to Information Security Incidents

8.1 Implementation guidance for when the Organisation acts as a PII Controller:

An incident involving PII triggers a review by the Organisation, as part of its information security incident management process, to determine if a breach involving PII requires a response.

An event does not necessarily trigger such a review.

N.B. a breach involving PII which could result in a risk to the rights and freedoms of natural persons must be notified to the ICO without undue delay and within 72 hours.

When a breach of PII has occurred, response procedures include relevant notifications and records. Notifications are clear and contain such information as:

- A contact point where more information can be obtained

- A description of the breach including the number of individuals concerned as well as the number of records concerned
- Measures taken or planned to be taken.

Where a breach involving PII has occurred, a record is maintained with sufficient information to provide a report for regulatory and/or forensic purposes, such as:

- A description of the incident
- The time period
- The consequences of the incident
- The name of the reporter
- To whom the incident was reported
- The steps taken to resolve the incident (including the person in charge and the data recovered)
- The fact that the incident resulted in unavailability, loss, disclosure or alteration of PII.

In the event that a breach involving PII has occurred, the record also includes a description of the PII compromised, if known; and if notifications were performed, the steps taken to notify PII principals, regulatory agencies or customers.

8.2 Implementation guidance for when the Organisation acts as a PII Processor:

Provisions covering the notification of a breach involving PII form part of the contract between the Organisation and the customer. The contract specifies how the Organisation will provide the information necessary for the customer to fulfil their obligation to notify relevant authorities. This notification obligation does not extend to a breach caused by the customer or PII principal or within system components for which they are responsible. The contract also defines expected and externally mandated limits for notification response times.

N.B. a breach involving PII which could result in a risk to the rights and freedoms of natural persons must be notified to the ICO without undue delay and within 72 hours. The PII Controller must also be notified.

Where a breach involving PII has occurred, a record is maintained with sufficient information to provide a report for regulatory and/or forensic purposes, such as:

- A description of the incident
- The time period
- The consequences of the incident
- The name of the reporter
- To whom the incident was reported
- The steps taken to resolve the incident (including the person in charge and the data recovered)
- The fact that the incident resulted in unavailability, loss, disclosure or alteration of PII.

In the event that a breach involving PII has occurred, the record also includes a description of the PII compromised, if known and, if notifications were performed, the steps taken to notify the customer and/or the regulatory agencies.

9 Identification of Applicable Legislation and Contractual Requirements

The Organisation identifies any potential legal sanctions (which can result from some obligations being missed) related to the processing of PII, including substantial fines directly from the local supervisory authority.

The contract defines their respective security, privacy and PII protection responsibilities. The terms of the contract may provide a basis for contractual sanctions in the event of a breach of those responsibilities.

10 Protection of Records

Review of current and historical policies and procedures may be required (e.g. in the cases of customer dispute resolution and investigation by a supervisory authority).

The Organisation retains copies of its privacy policies and associated procedures for a period as specified in its retention schedule. This includes retention of previous versions of these documents when they are updated.

11 Independent Review of Information Security

Where the Organisation is acting as a PII processor, and where individual customer audits are impractical or can increase risks to security, the Organisation makes available to customers, prior to entering into, and for the duration of, a contract, independent evidence that information security is implemented and operated in accordance with the Organisation's policies and procedures.

Evidence of certification to ISO 27001: 2013 is normally sufficient for this purpose.

12 Technical Compliance Review

As part of technical reviews of compliance with security policies and standards, the Organisation includes methods of reviewing those tools and components related to processing PII. These can include:

- Ongoing monitoring to verify that only permitted processing is taking place; and/or
- Specific penetration or vulnerability tests (for example, de-identified datasets can be subject to a motivated intruder test to validate that de-identification methods are compliant with organisational requirements).