Processing Contracts Procedure

Reference: PIMS-C DOC 7.2.6
DocumentKits Issue No: 1.0
Organisation Issue No:
DocumentKits Issue Date: 26/06/2020
Organisation Issue Date:

1. Scope

All contracts with third parties regarding the processing of personally identifiable information (PII) are within the scope of this procedure. This procedure supplements Managing Third Party Service Contracts and External Parties: Information Security and Privacy Procedure.

2. Responsibilities

2.1
"Legal"

is responsible for drawing up and/or reviewing all processing contracts where Organisation Name is acting as a controller, processor or joint controller.

2.2 The Data Protection Officer is responsible for ensuring that any privacy controls mandated in contracts are adequate to protect PII while under control of the third party.

2.3 The
"owners"

of third-party relationships are responsible for ensuring that all external data processing is contracted out in line with this procedure.

3. Procedure

3.1 Where there is a business need for working with external parties, Organisation Name ensures that the privacy of any PII is not reduced
"; access to organisational assets is not granted until a privacy impact assessment (PIA) or risk assessment has been completed, and appropriate controls identified and implemented (Privacy Impact Assessment Procedure, Risk Management)."

SAMPLE

3.2 Contracts with PII processors and joint controllers are governed by contracts drawn up by
"Legal"

using
"link to template"

as a basis.

3.3 Contracts require PII processors and joint controllers to implement controls
"identified by PIA or risk assessment, or otherwise identified – describe. "

3.4 PII processing agreements between Organisation Name and external parties set out the following:

3.4.1 Organisation Name's Information Security Policy and the Data Protection and Privacy Policy.

3.4.2 The controls identified as required in accordance with 3.3 above, and the responsibilities for implementing them.

3.4.3 A clear definition and/or description of the processing to be provided, and a description of PII to be made available.

3.4.4 The roles and responsibilities of each party in relation to the PII (i.e. PII controller, PII processor, joint controller).

3.4.5 Terms for PII retention and disposal.

3.4.6 Requirements for user and administrator education, training and awareness.

3.4.7 Provisions for personnel transfer, where relevant.

3.4.8 Description of responsibilities regarding software and hardware installation, maintenance and decommissioning as it relates to the PII processing.

3.4.9 Clearly defined reporting process, reporting structure, reporting formats, escalation procedures and the requirement for the external party to adequately resource the compliance, monitoring and reporting activities.

3.4.10 A specified change management process.

SAMPLE

<<3.4.11-3.4.20 removed for sample purposes>>

Document owner and approval

The Management System Owner (MSO) is the owner of this document and is responsible for ensuring that it is reviewed in line with the requirements of the management system.

The current version of this document is available to
"Specify which members of staff this document is intended for"

and is published
"Describe the location(s) - electronic and physical - where this document is available"

Its approval status can be viewed in the Master List of Document Approval.

SAMPLE