YourIT!
Your Logo Goes Here

GDPR Assessment

EU GDPR Policy and Procedures

Scan Date: 1/18/2018

Prepared for:
My Client Company
Prepared by:
YourIT Company

1/18/2018

TABLE OF CONTENTS

GENERAL PROVISIONS

ARTICLE 1 - SUBJECT-MATTER AND OBJECTIVES

The organisation and its relevant entities are committed to the protection of Personal Data collected and processed as part of its business operating activity for the provision or offer of goods or services to individuals.

Personal Data is defined as any information relating to an identified or identifiable natural person ('Data Subject').

This policy outlines the organisation policies and procedures relating to the protection of Data Subject rights with regard to the processing of Personal Data and rules relating to the free movement of Personal Data.

These policies and procedures do not cover every condition, clause or stipulation of the European Union General Data Protection Regulation (EU GDPR) or its Articles or EU Member State national law nor were they intended to do so.

The processes adopted by the organisation herein are designed to automate the documentation and reporting of Information Processing System Security and a number of EU GDPR compliance requirements and not, for example, tasks that involve administrative attention such as employee background checks, business sanction warnings, or complaint handling.

The following policies and procedures support the administrative and technical safeguards of the EU GDPR whether required or addressable, to the extent described below and identified by EU GDPR "Article" provisions as follows:

ARTICLE 3 - TERRITORIAL SCOPE

This Policy applies to the organisation and its entities located within and outside the European Union whereby the entity processes Personal Data:

1) in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the European Union (EU) or not.

2) of Data Subjects who are in the EU by a controller or processor not established in the Union, where the processing activities are related to:

a) the offering of goods or services, irrespective of whether a payment of the Data Subject is required, to such Data Subjects in the Union or

b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3) by a controller not established in the European Union (EU), but in a place where EU Member State law applies by virtue of public international law.

Compliance Verification Requirements: This policy must be enacted and enforced based upon an organisation entity's processing of Personal Data of Data Subject's whereby European Union (EU) or EU Member State national law requires the protection of Personal Data and Data Subject rights under the EU GDPR and its provisions. The organisation and its entities will assess an entity's Personal Data collection and processing practices to determine if this policy is applicable to a specific entity.

Training Considerations: Organisation and entity personnel will be trained on the necessary EU GDPR Applicability Assessment practices used to determine if an organisation entity located outside of the European Union is required to implement this policy in part or in full.

ARTICLE 4 - DEFINITIONS

Below are the terms referenced in this policy and their definitions:

Consent - of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her

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 European Union (EU) or EU Member State national law, the controller or the specific criteria for its nomination may be provided for by EU or EU Member State national law

Data Processor - means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the organisation when acting at a Personal Data controller

Data Protection Officer - is a position within the organisation that acts as an independent advocate for the proper care and use of Personal Data.

Data Subject - An Identifiable Natural Person, or a Natural Person that can be identified to which the Personal Data refers.

Encryption - A method by which plain text or any other type of data is converted from a readable form to an encode version of data using an encryption key that can only be decoded by another entity if that entity has access to a decryption key.

Filing System - means any structured set of Personal Data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis

International Organisation - means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries

Personal Data - means any information relating to an identified or identifiable natural person ('Data Subject') an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Personal Data Breach - means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed

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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Processor - means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller

Profiling - means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

Pseudonymisation - means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person

Special Categories of Data - Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, including genetic data, biometric data collected and processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

Supervisory Authority - means an independent public authority which is established by a European Union Member State.

Third Party - means a natural or legal person, public authority, agency or body other than the Data Subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process Personal Data

PRINCIPLES

Policy: The organisation will collect and process Personal Data in accordance with the following principles:

ARTICLE 5 - PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

PRINCIPLE 1 - LAWFULNESS, FAIRNESS, AND TRANSPARENCY

The organisation will process lawfully, fairly and in a transparent manner in relation to the Data Subject ('lawfulness, fairness and transparency')

PRINCIPLE 2 - PURPOSE LIMITATION

When the organisation collects Personal Data, the data will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

PRINCIPLE 3 - DATA MINIMISATION

Personal Data collected by the organisation shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

PRINCIPLE 4 - ACCURACY

Personal data collected by the organisation shall be accurate and, where necessary, kept up to date every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

PRINCIPLE 5 - STORAGE LIMITATION

Personal Data stored by the organisation shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed

PRINCIPLE 6 - INTEGRITY AND CONFIDENTIALITY

The organisation will process Personal Data in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

PRINCIPLE 7 - ACCOUNTABILITY

The organisation shall be responsible for Data Protection and maintain the necessary records in its filing system. Records created and stored in the organisation's filing system will be maintained in order to demonstrate compliance with EU GDPR.

The demonstration of compliance shall include the ability for the organisation to show that the six Data Protection Principles one (1) through six (6) above are met by the organisation.

Procedure: The organisation will use automated assessment and reporting tools to assess Personal Data collection, processing, and use including:

a) lawfulness, fairness, and transparency is maintained in relation to the Data Subject

b) verify that the data collected is for a specified, explicit, and legitimate use and not further processed

c) a verification that the data collected is minimised by being adequate, relevant, and limited to its processing purpose

d) a determination that the data is accurate and kept up to date

e) a determination that the data is kept in a form which permits identification of the Data Subject for longer than what is necessary

f) a verification that the data is processed in a secure manner in order to ensure protection of unauthorised or unlawful process and accidental loss

Compliance Verification Requirements: Documentation containing the terms of the organisation's Data Retention policy. An annual audit of the records detailed above will be carried out by the organisation to verify that systems and processing are creating, updating, and storing records in compliance with this policy. A Data Retention Schedule will be created and maintained by the organisation.

Training Considerations: Employees and third parties should be trained on organisation information security policies and procedures related to Personal Data security, the organisation's code of ethics, organisation practices involving the collection and processing of Personal Data, and organisation policies and procedures designed and implemented to protect the rights of Data Subjects.

ARTICLE 6 - LAWFULNESS OF PROCESSING

Policy: The organisation will implement data collection, processing, and verification procedures to ensure that its Personal Data processing activity is lawful based upon one of the existence of at least one of the following conditions:

1) the Data Subject has given consent to the processing of his or her Personal Data for one or more specific purposes

2) processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract

3) processing is necessary for compliance with a legal obligation to which the controller is subject

4) processing is necessary in order to protect the vital interests of the Data Subject or of another natural person

5) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the organisation when acting as the controller

6) processing is necessary for the purposes of the legitimate interests pursued by the organisation when acting as the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

Procedure: The organisation will use automated assessment and reporting tools to assess Personal Data collection, processing, and use including:

1) a description of the Personal Data collected

2) the purpose of the Personal Data's processing

3) a verification that the data collected is minimised

4) a determination if consent is provided during collection

5) the method used to secure consent

Compliance Verification Requirements: The following records are to be created, filed, and archived in compliance with policy and its audit requirements:

1) Data Subject consent records

2) record of contracts between the organisation and the Data Subject

3) records demonstrating that processing is in compliance with organisation legal obligations

4) when applicable, records demonstrating that processing is necessary for the carrying out of tasks in the public interest

5) records demonstrating that processing is for the purpose(s) of the legitimate interests pursued by the organisation.

Training Considerations: Employees and third parties should be trained on the execution of the processes designed to create, maintain, and analyse records to assess if the policies outlined above are in compliance with this policy's lawfulness of processing requirements.

ARTICLE 7 - CONDITIONS FOR CONSENT

Policy: The organisation will obtain Personal Data with the consent of the Data Subject, or the Data Subject's representative.

In instances where Consent is to be requested and received from an individual prior to data collection, data use, or disclosure of Personal Data, the organisation will seek such Consent.

The organisation shall establish a system for obtaining and documenting Data Subject consent for collection, processing, and/or transfer of the subject's Personal Data. The system must meet the following requirements:

1) Where processing is based on consent, the organisation, when acting as a "controller" shall be able to demonstrate that the Data Subject has consented to processing of his or her Personal Data.

2) Ensuring that the request for consent is presented to the Data Subject in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

3) Ensuring that a simple method is employed to enable the Data Subject to easily withdraw the subject's consent at any time.

4) Ensuring that when assessing whether consent is freely given, that the performance of a contract, including the provision of a service, is not conditional on consent to the processing of Personal Data that is not necessary for the performance of that contract.

5) Documenting a record of the consents made to the Data Subject, and the date and methods used by the Data Subject to grant consent to for the organisation to enable it to collect, process, and/or transfer the subject's Personal Data.

The organisation will perform a periodic review of the enforcement of the above policy and review the accuracy of the records maintained as referenced in item 5) above.

Procedure: The organisation will use automated assessment and reporting tools to assess Personal Data collection, processing, and use including:

1) a description of the Personal Data collected

2) the purpose of the Personal Data's processing

3) a verification that the data collected is minimised

4) a determination if consent is provided during collection

5) the method used to secure consent

Compliance Verification Requirements: Compliance verification requirements shall include a review of contents of record, the date and methods that Data Subjects use to grant consent for the organisation to collect, process, and/or transfer Data Subject Personal Data. Verification process will include a review of the organisation's Data Subject Consent form and the Data Subject Consent Withdrawal form.

Training Considerations: The organisation's employees, contractors, and third parties will be trained on the implementation and use of the processes and any related systems utilised to enforce the above policy.

Truncated Sample Report