Data Privacy Governance Program

EU & UK GDPR

zanda

APRIL 24, 2023

Policies and Procedures

Information security policies (summary info)

Data Protection Impact Assessment (DPIA)

Data Protection Impact Assessment (DPIA) methodology implemented by the organisation to support efforts of ongoing compliance with GDPR and UK GDPR.

Data Protection Policy

This document sets out the general principles to be applied by the organisation when handling the personal data referred to as "Individuals" in this document.

Data Retention and Disposal

This policy is about the organisation's approach for data retention and secure disposal.

Data Subject Rights Procedure

This document explains the rights granted by GDPR and UK GDPR to European Union (EU) and United Kingdom based individuals or Data Subjects with their relevant obligations for the businesses and sets out a methodology for implementing these rights into business operations.

GDPR and UK GDPR Breach Notification

This procedure is intended to be used when an incident has occurred that has resulted in or is suspected of having resulted in a loss of personal data.

GDPR and UK GDPR Procedure for International Transfers of Personal Data

This document guides organisations on the process when transferring personal data protected by the EU General Data Protection Regulation (GDPR) and UK GDPR outside of the European Economic Area (EEA) and United Kingdom.

Information Security

Zanda utilises InfoSec Platform to manage policies, provide security awareness training, implement and document security controls, and track compliance with customers, third-party vendors, independent auditors and regulatory agencies.

Internal Privacy Policy

This document sets out the general principles to be applied by the organisation when handling the personal data of EU and UK-based individuals ("Data Subjects") or California residents ("Consumers")—collectively referred to as "Individuals" in this document. Demonstrate also the organisation's commitment to safeguarding and appropriately handling our employees' and contractors' personal information.

Privacy Policy for Websites

The Privacy Policy describing the generic use and disclosure of personal information that is collected from the individuals online, through websites. This is published on the Zanda website here: zandahealth.com/privacy-policy

Risk Assessment

The organisation institutes regular risk assessments and uses industry best practices in remediation.

Vendor Management

The organisation actively manages risks around third-party vendors and their access to the organisation's data.

Policy Implementation Controls

Data Breaches

G—Breach Risk Assessments

Data breach risk assessment is performed on the identified incidents following the discovery of a breach to determine the probability that personal data has been compromised and whether notifications are required.

GC—Breach Notifications to Data Subjects

Notifications are provided to data subjects regarding their personal data breach without unreasonable delay in cases where a personal data breach is likely to result in a high risk to their rights and freedoms.

GC—Breach Notifications to Supervisory Authority

Notifications are provided to supervisory authorities regarding personal data breaches without unreasonable delay and in no case later than 72 hours after the discovery of a breach.

GP—Breach Notifications to Controller

Notifications are provided to controller(s) regarding personal data breaches without unreasonable delay following the discovery of a breach. Data breaches are logged, tracked and resolved in a timely manner in accordance with organisational policies and procedures.

Data Privacy

C—Data Inventory

Organisations identify and maintain an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection. The documented inventory is reviewed by management on at least an annual basis or during significant changes to ensure it aligns with the organisation's privacy notice.

G—Awareness Training

Employees and contractors are required to complete an information security and privacy awareness training as part of the onboarding process and annually thereafter.

G—Data Protection Officer

Organisation has designated a Data Protection Officer (DPO) to oversee the development and implementation of privacy policies and procedures in compliance with applicable privacy laws.

G—Data Protection Policy

Data Protection policy is established and communicated to employees and contractors within the organisation. The policy is reviewed by management on an annual basis or in case of significant changes.

G—Employee Privacy Notice

The organisation has established a privacy notice for its employees and contractors which specifies their rights and the organisation's privacy obligations in accordance with applicable privacy laws and regulations. The policy has been communicated and acknowledged by the employees and contractors on at least an annual basis or during significant changes.

G—EU Representatives

Organisation has designated a representative in the European Union to represent the organisation regarding their obligations under the GDPR and to deal with any supervisory authorities or data subjects.

G—Privacy Policy

Organisation has a privacy policy published on its website which outlines privacy obligations and specifies data subject rights in accordance with applicable laws and regulations. The policy is reviewed by management on an annual basis.

G—Processing Special Categories of Personal Data

Organisation maintains an inventory of special categories of personal data processed by the organisation as well as its purpose. The documented inventory is reviewed by management on at least an annual basis and provided to legal authorities on request.

G—Record of Processing Activities/Inventory

Organisation maintains a record of processing activities with respect to personal data collected from data subjects or processed on behalf of the controller. The documented inventory is reviewed by management on at least an annual basis and provided to legal authorities on request.

G—Retention of Personal Information

The organisation retains personal information consistent with its privacy commitments and as long as it is required for its intended purpose.

GC—Consent on Collection and Processing

Explicit consent is obtained and maintained from data subjects prior to collection and for any new uses or disclosure of their personal information. Data subjects are provided with a mechanism to modify or withdraw their consent.

GC—Data Protection Impact Assessment

The organisation assesses the need for and implements, where appropriate, a data protection impact assessment whenever new processing of personal data or changes to existing processing is planned.

GC—Lawfulness of Processing

Organisation determines, documents, and complies with the relevant lawful basis for the processing of personal data for the identified purposes in accordance with applicable privacy obligations.

GC—Periodic Assessments

Periodic assessments of the systems, tools and processes are performed to identify all locations where personal information is collected, processed and distributed. Deficiencies are tracked, resolved and reported to management in a timely manner.

GC—Withdrawal of Consents

The organisation responds promptly to data subjects' requests to modify or withdraw their consent at any time. Records of such requests are documented and retained in accordance with organisational policies.

Data Privacy

G—Security Measures and Assessments

Appropriate technical and organisational measures have been implemented by the organisation for the security and protection of personal information. These measures are assessed by management on an annual basis and deficiencies identified are remediated in a timely manner.

Data Subject Rights

GC—Access Requests from Data Subjects

Access requests from data subjects to obtain, amend or review their personal information is documented, retained, and acted upon within 30 days from the receipt of the request. Any denial on request is communicated to data subjects and handled in accordance with applicable privacy regulations.

GC—Data Subject Rights Procedure

Organisation has established a data subject rights procedure that specifies rights granted to individuals with respect to their personal data. These procedures are approved by management and communicated to employees and contractors.

GC—Request for Erasure of Personal Information

Access requests from data subjects for the erasure of their personal information are documented, retained, and acted upon without undue days. Such requests are communicated to third parties that are involved in the processing of personal information in a timely manner.

GC—Request for Restriction/Objection on Processing

Access requests from data subjects for restriction or objection on processing of their personal information are documented, retained, and acted upon without undue days. Any such request is communicated to other data controllers or vendors also processing that information in a timely manner.

GC—Right of Data Portability

Access requests from data subjects for transmission of their personal information to another controller in a structured format are documented, retained, and acted upon without undue days.

GP—Request on Data Subject Rights

Requests received from controllers regarding exercising rights of data subjects are documented, retained, and acted upon without undue days.

Data Transfers

G—International Transfer of Personal Data

The organisation identifies the relevant basis for the international transfer of personal data and implements a procedure that specifies processes and conditions on the transfer of personal data to third countries or international organisations. The procedure is approved by management and communicated to employees and contractors.

G—Procedure for International Transfer of Personal Data

The organisation has established and implemented a data transfer procedure that specifies processes and conditions on the transfer of personal data to third countries or international organisations. The procedure is approved by management and communicated to employees and contractors.

Vendor Management

GC—Vendor Management Process

A vendor management process has been implemented whereby management performs risk assessments of potential new vendors/ processors and evaluates the compliance of existing vendors (including processors) on an annual basis. Corrective actions are taken as required based on the results of the assessments.

GC—Contracts with Processors

Organisation maintains written contract with processors that it uses for processing personal data collected from data subjects. These contracts outline the security and privacy requirements that are required to be implemented by processors for the protection of personal data.

GP—Authorisation from Controller for Sub-Processing

Organisation obtains formal authorisation from the controller prior to engaging another processor (sub-processor) to support its processing activities. Arrangements between processor and subprocessors are supported by written contracts outlining the same data protection obligations as it has with the controller.

GP—Contracts with Controller

Organisation maintains written contract with controllers on behalf of whom it performs processing of personal data. These contracts outline the security and privacy requirements that are required to be implemented by processors for the protection of personal data.