GDPR Processor Security Controls

Guidance
Purpose of this document This document describes the information security controls that are in place by an organisation acting as a processor in the context of the GDPR.
Areas of the standard addressed The following areas of the GDPR are addressed by this document: Article 28 – Processors Article 32 – Security of processing
Review Frequency It will be reviewed at least on annual basis and upon significant change to the organisation and relevant legislation.

Contents

1 Introduction 3
2 Processing Service Specifications 4
2.1 Information security policies 4
2.2 Organisation of information security 4
2.3 Human resource security 4
2.4 Asset management 5
2.5 Access control 5
2.6 Cryptography 5
2.7 Physical and environmental security 5
2.8 Operations security 6
2.9 Communications security 6
2.10 System acquisition, development and maintenance 6
2.11 Supplier relationships 7
2.12 Information security incident management 7
2.13 Information security aspects of business continuity management 7
2.14 Compliance 7

1 Introduction

FIDUS INVESTMENTS CYPRUS LTD is a licensed investment firm with customers in many countries and takes the protection of its customers' data very seriously. To provide an enhanced level of protection, FIDUS INVESTMENTS CYPRUS LTD has invested in a high level of information security and has also adopted the best practice controls defined in several information security codes of practice.

A key component of these controls is the clear definition of the split of responsibilities between the investment firm and customer. It is also important that the technical, procedural and physical controls implemented by FIDUS INVESTMENTS CYPRUS LTD as part of its services are understood by the customer so that an informed assessment of the risks to its personal data can be made.

This is particularly important in the context of the European Union General Data Protection Regulation (GDPR) which places several obligations on the processor of personal data which must be contractually required by the controller.

The purpose of this document is to describe in outline the controls that are in place, or are offered on an optional basis, within our processing environment.

Cloud computing is generally accepted to consist of the following types of services:

Software-as-a-Service (SaaS) – the provision of a hosted application for use as part of a business process. Hosting usually includes all supporting components for the application such as hardware, operating software, databases etc.

Platform-as-a-Service (PaaS) – hardware and supporting software such as operating system, database, development platform, web server etc. are provided but no business applications

Infrastructure-as-a-Service (IaaS) – only physical or virtual hardware components are provided

The exact combination of controls that apply to each of the above models will vary according to the agreed scope of processing services provided. This will be stated within the contract that is signed before the delivery of services commences.

2 Processing Service Specifications

The following information is provided to help our customers make an informed choice about the level of information security they believe is needed to protect the personal data they place with us, based on an assessment of risk for their set of circumstances.

The information provided is intended to reflect an appropriately useful level of detail about our security defences, without divulging specifics that may be of value to an attacker. Further detail may be available to authorized customers under a non-disclosure agreement on request.

2.1 Information security policies

FIDUS INVESTMENTS CYPRUS LTD information security policies are written to take account of the specific needs of providing hybrid services including:

- Extensive use of virtualization
- The multi-tenanted nature of our services
- Risks from authorized insiders
- Protection of customer data
- The need for effective communication with our customers

All policies are version-controlled, authorized and communicated to all relevant employees and contractors.

2.2 Organisation of information security

Roles and responsibilities for the management of the technology environment are clearly defined as part of contract negotiation so that customer expectations are aligned appropriately with the way that service will be delivered.

In addition, a clear split of responsibilities between FIDUS INVESTMENTS CYPRUS LTD and our suppliers, including technology service providers that supply supporting services, is established and maintained.

FIDUS INVESTMENTS CYPRUS LTD operates from several geographical regions and adopts European zone approach to the storage of customer data so that it is maintained within the European boundaries.

2.3 Human resource security

A comprehensive program of awareness training is delivered on an ongoing basis to all FIDUS INVESTMENTS CYPRUS LTD employees to emphasize the need to protect customer data appropriately. We also require our contractors to provide confirmation on the appropriate awareness training to all relevant employees.

2.4 Asset management

Functionality is provided where possible within our services to allow our customers to reflect their own information classification and labelling schemes.

An audited procedure is in place for the return and removal of customer assets when appropriate. This procedure is designed to assure the protection of customer data in general and particularly personal data.

2.5 Access control

We provide a comprehensive, user-friendly administration interface to authorized customer administrators that allows them to control access at the service, function and data level. User registration and deregistration and access rights management is achieved via this interface, access to which may be protected if required by multi-factor authentication.

Documented procedures for the allocation and management of secret authentication information, such as passwords, ensure that this activity is conducted in a secure way.

The use of utility programs within the customer environment by FIDUS INVESTMENTS CYPRUS LTD employees is strictly controlled and audited on a regular basis.

Where we operate a multi-tenanted environment, customer resources are subject to strict segregation from each other, so that no access is permitted to any aspect of another customer's environment, including settings and data.

Virtual machine hardening, including the closing of un-needed ports and protocols, is implemented as standard practice and each virtual machine is configured with the same degree of protection for malware as physical servers.

2.6 Cryptography

Transactions between the user (including administrators) and the cloud environment are encrypted using SSL 2048bit. Customer data is secured at rest using industry-standard encryption technology to address organizational security and compliance requirements.

2.7 Physical and environmental security

FIDUS INVESTMENTS CYPRUS LTD has procedures in place for the secure disposal and reuse of resources when no longer required by the customer. These procedures will ensure that customer data is not put at risk.

2.8 Operations security

FIDUS INVESTMENTS CYPRUS LTD makes customers aware of planned changes that will affect the customer environment or services. This information is published regularly on our website and/or via email to affected customer administrators and will include the type of change, scheduled date and time and, where appropriate, technical details of the change being made. Further notifications will be issued at the start and end of the change.

The capacity of the overall environment is subject to regular monitoring by FIDUS INVESTMENTS CYPRUS LTD engineers to ensure that our capacity obligations can be fulfilled always.

Encrypted backups of the environment are taken and are retained for a period of ranging from three months to 6 years. Operational backups are stored at a separate location to the main location or site resiliency. Backup samples are verified on a regular basis to confirm their integrity.

Activity and transaction logs are recorded and include details of logins/logouts, data access and amendments/deletions.

All system and device clocks within the environment are synchronized (via designated servers) to an external time source.

The environment is subject to regular vulnerability scanning using industry-standard tools. Critical security patches are applied in accordance with software manufacturers' recommendations.

Operational activities which are deemed critical and in some cases irreversible (such as deletion of virtual servers) are subject to specially controlled procedures which ensure that adequate checking is performed prior to completion.

Documented service monitoring facilities are available to monitor their environment for abuses such as data leakage and unauthorized control of servers etc. in conjunction with access to log information.

2.9 Communications security

Where a multi-tenanted environment is provided, networks are isolated from each other.

The configuration of virtual network resources is subject to the same level of control as that for physical network devices, according to our documented network security policy.

2.10 System acquisition, development and maintenance

Secure development procedures and practices are used within FIDUS INVESTMENTS CYPRUS LTD, including separation of development, test and production environments, secure coding techniques and comprehensive acceptance testing.

2.11 Supplier relationships

In the delivery of certain services, FIDUS INVESTMENTS CYPRUS LTD makes use of peer cloud service providers in a supply chain arrangement. These suppliers are subject to regular second party audit to ensure that they have defined objectives for information security and carry out effective risk assessment and treatment practices.

All supplier relationships are covered by contractual terms which meet the requirements of the GDPR.

2.12 Information security incident management

Where FIDUS INVESTMENTS CYPRUS LTD believes it is appropriate to inform the customer of an information security event (before it has been determined if it should be treated as an incident) we will do this to the nominated customer administrator or deputy. Similarly, the customer may report security events to our support desk where they will be logged, and the appropriate action decided. Information about the progress of such events may be obtained from the support desk.

FIDUS INVESTMENTS CYPRUS LTD will report information security incidents to the customer where it believes that the customer service or data has or will be affected. We will do this to the nominated customer administrator or deputy as soon as reasonably possible and will share as much information about the impact and investigation of the incident as we believe to be appropriate for its effective and timely resolution. An incident manager will be appointed in each case who will act as the FIDUS INVESTMENTS CYPRUS LTD point of contact for the incident, including matters related to the capture and preservation of digital evidence if required.

We prioritise incident management activities to ensure that the timescale requirements of the GDPR for notification of breaches affecting personal data are met.

2.13 Information security aspects of business continuity management

FIDUS INVESTMENTS CYPRUS LTD plans for and regularly tests, its response to various types of disruptive incident that might affect cloud customer service. The architecture of our cloud services is designed to minimize the likelihood and impact of such an incident and we will make all reasonable efforts to avoid any impact on customer cloud services.

2.14 Compliance

The legal jurisdiction of the service provided will depend upon the country in which the contract is made. Where the data of EU citizens is held, FIDUS INVESTMENTS CYPRUS LTD will comply with the requirements of the General Data Protection Regulation and/or the EU/USA Privacy Shield. Evidence of our compliance to these requirements is available on request.

Records collected by FIDUS INVESTMENTS CYPRUS LTD as part of its provision of the service will be subject to protection in accordance with our information classification scheme and asset handling procedures.