GDPR Processor Security Controls

GDPR Toolkit Version 1

Implementation Guidance

(The header page and this section must be removed from final version of the document)

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

General Guidance

This document sets out the general levels of service provided by the processor and will need to be tailored around how your services are offered and the nature of the services offered e.g. cloud services such as IaaS, PaaS and SaaS.

The exact split of responsibilities should be covered in a contract that is likely to vary between customers; this document therefore simply provides a starting point for the kinds of areas that need to be addressed. You may wish to provide this information on your website or in response to specific customer questions.

The idea of this document is to pre-empt the kinds of questions your customers may want to ask about how you secure your services and meet the requirements of the GDPR.

Review Frequency

We would recommend that this document is reviewed annually.

Toolkit Version Number

GDPR Toolkit Version 3 ©Datagator Ltd.

Document Fields

This document may contain fields which need to be updated with your own information, including a field for Organization Name that is linked to the custom document property "Organization Name".

To update this field (and any others that may exist in this document):

1. Update the custom document property "Organization Name" by clicking File > Info > Properties > Advanced Properties > Custom > Organization Name
2. Press Ctrl a on the keyboard to select all text in the document (or use Select, Select All on the ribbon)
3. Press F9 on the keyboard to update all fields
4. When prompted, choose the option to just update TOC page numbers

If you wish to permanently convert the fields in this document to text i.e. so that they are no longer updateable, then you will need to click into each occurrence of the field and press Ctrl Shift F9.

If you would like to make all fields in the document visible then go to File > Options > Advanced > Show document content > Field shading and set this to "Always". This can be useful to check that you have updated all fields correctly.

Further detail on the above procedure can be found in the *Toolkit Completion Instructions* within the Project Resources folder.

Copyright notice

Datagator Ltd is a company registered in England and Wales with company number 11260399 and registered office at 23 Cardiff Street, Aberdare, CF44 7DP.

Licence terms

Disclaimer

Please Note: *Your use of and reliance on this document template is at your sole risk. Document templates are intended to be used as a starting point only from which you will create your own document and to which you will apply all reasonable quality checks before use. Therefore please note that it is your responsibility to ensure that the content of any document you create that is based on our templates is correct and appropriate for your needs and complies with relevant laws in your country. You should take all reasonable and proper legal and other professional advice before using this document. Datagator Ltd makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of our document templates, assumes no duty of care to any person with respect its document templates or their contents, and expressly excludes and disclaims liability for any cost, expense, loss or damage suffered or incurred in reliance on our document templates, or in expectation of our document templates meeting your needs, including (without limitation) as a result of misstatements, errors and omissions in their contents.*

Datagator

[Replace with your logo]

GDPR Processor Security Controls

Document Ref.	
Version:	**1**
Dated:	**[Insert date]**
Document Author:	
Document Owner:	

Revision History

Version	Date	Revision Author	Summary of Changes

Distribution

Name	Title

Approval

Name	Position	Signature	Date

Contents

1 Introduction

[Organization Name] is a successful service provider with customers in many countries and takes the protection of its customers' data very seriously. In order to provide an enhanced level of protection, [Organization Name] has invested in a high level of information security and has also adopted the best practice controls defined in a number of information security codes of practice.

A key component of these controls is the clear definition of the split of responsibilities between the service provider and customer. It is also important that the technical, procedural and physical controls implemented by [Organization Name] 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 a number of 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 in order 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 particular business, industry and 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

[Organization Name] information security policies are written to take account of the specific needs of providing cloud services including:

- Extensive use of virtualization
- The multi-tenanted nature of our services
- Risks from authorized insiders
- Protection of cloud 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 cloud 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 [Organization Name] and our suppliers, including cloud service providers that supply supporting services, is established and maintained.

[Organization Name] operates from several geographical regions and adopts a zone approach to the storage of customer data so that it will always be located in the country or countries required by the customer.

2.3 Human resource security

A comprehensive program of awareness training is delivered on an ongoing basis to all [Organization Name] employees to emphasize the need to protect customer cloud data appropriately. We also require our contractors to provide appropriate awareness training to all relevant employees.

2.4 Asset management

Functionality is provided where possible within our cloud 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 cloud 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 cloud environment by [Organization Name] employees is strictly controlled and audited on a regular basis.

Where we operate a multi-tenanted environment, cloud 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 TLS by default. Customer data is encrypted at rest using keys managed by [Organization Name].

Facilities are provided by which the cloud customer may implement its own encryption of data at rest if required, with encryption keys being managed by the customer. Under these circumstances it is a customer responsibility to provide adequate protection of the keys from loss or compromise.

2.7 Physical and environmental security

[Organization Name] has procedures in place for the secure disposal and reuse of resources when no longer required by the cloud customer. These procedures will ensure that customer data is not put at risk.

2.8 Operations security

[Organization Name] makes customers aware of planned changes that will affect the customer cloud environment or services. This information is published regularly on our website and 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 cloud environment is subject to regular monitoring by [Organization Name] engineers to ensure that our capacity obligations can be fulfilled at all times.

Encrypted backups of customer environments are taken to a frequency specified by the customer and are retained for a default period of three months. Backups are stored at a separate location to the main location of customer data at a distance which is considered sufficient to represent a reasonable business continuity precaution. Backup samples are verified on a regular basis to confirm their integrity. Restoration from backup can be requested by the customer on a next day basis.

Activity and transaction logs are recorded in the cloud environment and may be accessed by customer administrators. These include details of logins/logouts, data access and amendments/deletions.

All system and device clocks within the cloud environment are synchronized (via designated servers) to an external time source, details of which are available upon request.

The customer cloud 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. We also recommend that customer put their own procedures in place in these areas.

Documented service monitoring facilities are available to cloud customers to allow them 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, cloud customer networks are isolated from each other. The [Organization Name] internal network also operates in isolation from all customer networks and environments.

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 [Organization Name], including separation of development, test and production environments, secure coding techniques and comprehensive security acceptance testing.

2.11 Supplier relationships

In the delivery of certain services, [Organization Name] 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 [Organization Name] 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.

[Organization Name] 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 [Organization Name] 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

[Organization Name] 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 cloud service provided will depend upon the country in which the contract is made. Where the data of EU citizens is held, [Organization Name] 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 [Organization Name] as part of its provision of the cloud service will be subject to protection in accordance with our information classification scheme and asset handling procedures.

[Organization Name]'s cloud services are certified to the ISO/IEC 27001 international standard for information security and are audited on an annual surveillance basis. We also comply with the ISO/IEC 27017 code of practice for information security controls in the cloud and the ISO/IEC 27018 code of practice for protection of personally identifiable information in the cloud.