



COMPLY TODAY

GDPR Processor Security Controls



Guidelines

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	ACCESS CONTROL	5
2.5	CRYPTOGRAPHY.....	5
2.6	PHYSICAL AND ENVIRONMENTAL SECURITY	5
2.7	OPERATIONS SECURITY	5
2.8	SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE	6
2.9	SUPPLIER RELATIONSHIPS	6
2.10	INFORMATION SECURITY INCIDENT MANAGEMENT.....	6
2.11	INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT	6
2.12	COMPLIANCE.....	6



1 Introduction

COMPLY TODAY to provide an enhanced level of protection, 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 organization and customer. It is also important that the technical, procedural and physical controls implemented by COMPLY TODAY 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.

Even though currently COMPLY TODAY does not utilize any cloud services, nevertheless and when adopting this usage then the Cloud computing will 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 to apply to each of the above models will vary according to the agreed scope of processing services provided. This will be stated within any engagement 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 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

COMPLY TODAY information security policies are written to take account of the specific needs when 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 **COMPLY TODAY** and our suppliers, including cloud service providers that will supply supporting services, is established and maintained.

2.3 Human resource security

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

2.4 Access control

We provide a comprehensive, user-friendly administration interface to authorized 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 used 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.

2.5 Cryptography

Any data communication between the users and administrators and the cloud environment will be encrypted using SSL 2048bit. Customer data will be encrypted at rest using private keys managed by the company.

2.6 Physical and environmental security

COMPLY TODAY 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.

2.7 Operations security

COMPLY TODAY will make customers aware of planned changes that will affect the customer cloud environment or services. This information, upon any amendment, is published on our website and via email to affected customer 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 will be subject to regular monitoring by **COMPLY TODAY** to ensure that our capacity obligations can be fulfilled always.

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.

2.8 System acquisition, development and maintenance

Secure development procedures and practices are used within **COMPLY TODAY**, including separation of development, test and production environments, secure coding techniques and comprehensive security acceptance testing.

2.9 Supplier relationships

In the delivery of certain services, **COMPLY TODAY** will make 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.

2.10 Information security incident management

COMPLY TODAY 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 **COMPLY TODAY** 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.

2.11 Information security aspects of business continuity management

COMPLY TODAY plans for and regularly tests, its response to various types of disruptive incident that might affect customer service. The architecture of our 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 services.

2.12 Compliance

Where the data of EU citizens is held, **COMPLY TODAY** will comply with the requirements of the General Data Protection Regulation. Evidence of our compliance to these requirements is available on request.

Records collected by **COMPLY TODAY** as part of its provision of the service will be subject to protection in accordance with our information classification scheme and asset handling procedures.