****

**Supplier GDPR**

**Assessment Procedure**

**Contents**

[1 Introduction 7](#_Toc493774645)

[2 Supplier GDPR Assessment Procedure 8](#_Toc493774646)

[2.1 Prerequisites 8](#_Toc493774647)

[2.2 Timing and Scheduling 8](#_Toc493774648)

[2.3 Procedure 8](#_Toc493774649)

[2.4 Error Handling 9](#_Toc493774650)

[2.5 Support and Escalation 9](#_Toc493774651)

[2.6 Auditing and Logging 9](#_Toc493774652)

[2.7 Monitoring 9](#_Toc493774653)

**List of Tables**

[Table 1 - Error handling 9](#_Toc493774654)

[Table 2 - Support contact information 9](#_Toc493774655)

# Introduction

The use of appropriate, secure and effective suppliers is key to [Organization Name]’s compliance with the General Data Protection Regulation (GDPR). Suppliers are used not only to help with the running of an effective company but in many cases to deliver services directly to the customer, such as in the case of web hosting. Other suppliers play a major part in whether [Organization Name] is successful in reaching its objectives, for example in attracting sufficient visitors to its website.

But suppliers must not only deliver good products and services but also do so in a secure way that doesn’t put [Organization Name] and its customers’ personal data at risk. This procedure is intended to ensure that sufficient actions are taken and research completed to reach a reasonable judgement about whether a supplier is meeting its GDPR obligations.

The following related documents are relevant to this procedure:

* Privacy and Personal Data Protection Policy
* Supplier GDPR Assessment Form
* Procedure for International Transfers of Personal Data

# Supplier GDPR Assessment Procedure

## Prerequisites

Before starting the procedure, the following prerequisites must be in place:

* Requirements for a product or service have been defined
* The supplier will be, or is already, storing and processing the personal data of our customers, employees or other stakeholders

## Timing and Scheduling

This procedure can be initiated at any time, but is particularly relevant to personal data mapping exercises.

## Procedure

A supplier GDPR assessment should be recorded using the Supplier GDPR Assessment form and retained as evidence of the assessment.

The following steps are required:

1. Use a fresh copy of the Supplier GDPR Assessment form and record the details of the assessment, including date/time, assessor name, company under assessment, product or service name and the classification of personal data that is or may be shared with the supplier.
2. Research the details of the company providing the product or service, including registered name, country of registration, approximate size and when they were formed
3. Document the commercial details of the offering under consideration, including contract terms including length, applicable law, renewal and termination.
4. Find out what information is available about the information security controls used by the supplier, including information security policy, certifications (e.g. ISO/IEC 27001, Cyber-Essentials), encryption etc.
5. Define what personal data is held or processed by the supplier and for what reason. This should include volumes and whether any special categories are involved.
6. Establish the physical location of the personal data i.e. the country or countries in which the hardware on which the data resides, is located. For GDPR purposes this will be within the European Union or in a country whose data protection framework has been deemed acceptable by the EU.
7. Find out what controls the supplier has in place to protect the personal data, such as encryption at rest and access control.
8. Ascertain whether the supplier uses any third parties to provide the service and whether they will have access to the personal data. If so, this procedure must be repeated for each one.
9. When all relevant information has been obtained and recorded, assess whether any further action needs to be taken to ensure compliance with the GDPR. Records these actions on the form and ensure they are communicated and progressed.

## Error Handling

The following common errors may occur during this procedure:

|  |  |  |  |
| --- | --- | --- | --- |
| Stage of Procedure | Error | Possible Cause | Recommended Action |
|  |  |  |  |

Table 1 - Error handling

## Support and Escalation

If an error occurs which cannot be corrected using this procedure, support should be obtained using the following information:

|  |  |  |  |
| --- | --- | --- | --- |
| Support Person | Role | Email | Hours of availability |
|  |  |  |  |

Table 2 - Support contact information

## Auditing and Logging

Supplier GDPR assessments and their outcomes are logged on the Supplier GDPR Assessment form and stored in the management system folder structure.

## Monitoring

Progress of assessments should be monitored at least weekly whilst ongoing, although many will be completed within a shorter timeframe.