Daniels Silverman

Sally Brown

Daniels Silverman

20 April 2018



Trinity Management Systems Limited

GDPR Compliance Report

GDPR Compliance Report

# Foreword

This GDPR Assessment Report test was commissioned by Daniels Silverman for Trinity Management Systems to conduct a GDPR assessment on all information collections within the organisation. This report details the methodology employed by Trinity Management Systems, the Data Protection impact analysis and the controls that have been implemented for GDPR compliance.

# Table of Contents

Foreword 2

Table of Contents 3

Introduction 4

Information collection assessment 5

Daniels Silverman Information Collections 7

Information Collection Mapping 7

Data Protection Impact Analysis 8

Conclusion 8

# Introduction

Trinity Management Systems Limited was engaged to conduct the GDPR Compliance Assessment for Daniels Silverman.

This assessment report details the high level information required to show GDPR compliance, along with the controls that have been put in place to protect all data and its usage. The information collections are categorised using the following criteria: -

|  |  |
| --- | --- |
| **Type** | **Description** |
| Personal | Personal data that is used to identify individuals. This includes all personal details including contact details and any level of personal detail the organisation is required to retain |
| Customer | Customer data includes personal data that is utilised as part of the service or operations of the organisation that can be used to identify individuals. |
| Financial | Financial data that is used by the organisation for both internal and external utilisation. |
| Commercial | Commercial data that is protected through Intellectual Property Rights and is sensitive to the organisation. |
| Supplier | Supplier data that is used for management of suppliers, this can sometimes include personal data and is therefore required to be protected. |

From each identified information collection, the questionnaire was completed. This information, from each information collection is utilised to calculate the scoring level, impact status, generate the data flows, risk assessment and the impact analysis.

Information Collection Status and Scoring boundaries

|  |  |
| --- | --- |
| Critical Status | Calculated Score |
| Gold | Less than 840 |
| Silver | Less than 650 |
| Bronze | Less than 460 |

# Information collection assessment

|  |  |
| --- | --- |
| Status | Meaning |
| ✓ | Requirement completed |
| 🗶 | Requirement is to be completed |
| ? | Further actions required for completion of the requirement |

|  | Requirements | Information | Assessment | Status |
| --- | --- | --- | --- | --- |
| 1 | C:\Users\sally\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Step 1.png | **Raise GDPR Awareness**  GDPR awareness presentation, detailing the changes to legislation and your responsibilities | GDPR Awareness presentation to all key stakeholders and all members of staff has been completed. | ✓ |
| 2 | C:\Users\sally\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Step 2.png | **Know your information**  Carry out an information collection audit using the "Information Collection Questionnaire" | All information collections have been identified and the default questions on each collection have been completed | ✓ |
| 3 | C:\Users\sally\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Step 3.png | **Privacy communications**  Review of privacy statement and Data Protection Policy.  Creation of template Privacy statement to use for all your communications - internet, email, marketing and contractual communications. This privacy statement is to be written in plain language and not "legal speak" | The Privacy Statement has been created and published to our website. Links within all correspondence to the Privacy statement have been implemented | ✓ |
| 4 | C:\Users\sally\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Step 4.png | **Individual Rights**  Ensuring processes are updated to reflect how you delete individual’s information within the remit of all legislation. Review how information is provided to individuals in a common format | The Privacy Statement has been created and published to our website. Links within all correspondence to the Privacy statement have been implemented | ✓ |
| 5 | C:\Users\sally\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Step 5.png | **Subject Access Request (SARs)**  Implement a plan for handling SARs and providing required information within the 30 day notice period. Communicate the parameters of SARs | A Subject Access Request Policy is required to be created and implemented | ✓ |
| 6 | C:\Users\sally\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Step 6.png | **Be legal**  Understanding the different types of data processing your organisation performs. Identify the legal basis for carrying out such tasks and document each separately | All information collections have been identified and the type of data being held assigned within the Information Collection questionnaire. The types of data are detailed within the flow charts for each information collection. | ✓ |
| 7 | C:\Users\sally\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Step 7.png | **Consent**  How you seek, obtain and determine consent for individual’s data to be used and/or shared | For each information collection a determination has been made on whether formal consent is required to be asked for. Where consent for an individual’s information is to be shared outside our organisation this has been requested. | ✓ |
| 8 | C:\Users\sally\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Step 8.png | **Protecting children's data**  Design and implement systems that can be used to verify ages and to seek consent from a guardian for a data processing activity relating to a child | Daniels Silverman have determined that the processing and control of children’s data/information is part of our operations | ✓ |
| 9 | C:\Users\sally\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Step 9.png | **Data breaches**  Implement process for detecting, investigating and reporting data breaches to customers and regulatory body | Daniels Silverman have in place a Security Incident Management Policy | ✓ |
| 10 | C:\Users\sally\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Step 10.png | **Privacy by Design**  Privacy impact assessment (PIA) to be detailed within the GDPR assessment report about the risk assessment of all information collections identified in 2. Know your Information | An impact analysis as well as a risk assessment has been conducted on all identified information collections. This is detailed within Appendix A of this report. | ✓ |
| 11 | C:\Users\sally\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Step 12.png | **Data Protection Officer (DPO)**  Assign a DPO if your organisation processes large scale data and information as part of your main operations. It is your decision on whether you require a DPO or not | Daniels Silverman have assigned a Data Protection Officer. | ✓ |
| 12 | C:\Users\sally\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Step 11.png | **International?**  Within 2. Know your Information ascertain if any data is held or processed internationally. Any data held or processed outside the UK/EU is required to be identified and detailed within your privacy statement | Daniels Silverman hold, process and manage the information collections used for our operations outside of the UK/EU geographical area. The Privacy Statement reflects where information is held and managed. | ✓ |

Policies and/or Processes

The following documentation and activities have been implemented to, not only show compliance to the regulations but also, to implement “industry best practice” for the protection of information and IT infrastructure.

|  |  |
| --- | --- |
| Status | Meaning |
| ✓ | Implemented |
| 🗶 | Not implemented |
| ? | Requires to be updated |

|  |  |
| --- | --- |
| Document | Status |
| Privacy Statement | ✓ |
| Data Protection Policy | ✓ |
| Backup Policy | ✓ |
| Malware Protection Policy | ✓ |
| Encryption Policy | ✓ |
| Subject Access Request Policy | ✓ |
| Data Removal Request Policy | ✓ |
| Security Incident Management Policy | ✓ |
| Information Audit Policy | ✓ |

## Daniels Silverman Information Collections

We have identified the following types of information collections we utilise within our operations. The specific names of the information collections are confidential to our operation’s; therefore, this table shows the number of each type of information collection only.

|  |  |
| --- | --- |
| Type | Total |
| Personal | 16 |
| Customer | 1 |
| Financial | 1 |
| Commercial | 2 |
| Supplier | 1 |
| TOTAL | **21** |

## Information Collection Mapping

Daniels Silverman have conducted an information collection mapping exercise. From this information flowcharts have been generated so we can visually ascertain the flow of information and the protections throughout all our operations.

## Data Protection Impact Analysis

The Data Protection Impact Analysis (DPIA) is based on the level of risk and the critical status of the Information Collection. The overall results of DPIA are: -

|  |  |
| --- | --- |
| **Impact Analysis** |  |
|  |  |
| **Impact Level** | **Total** |
| Very High | 9 |
| High | 3 |
| Medium | 5 |
| Low | 4 |
| Grand Total | 21 |

The overall risk level of the Information collections is calculated at a level of **MEDIUM**

## Conclusion

Daniels Silverman have completed the GDPR Compliance exercise and have implemented all necessary controls and protections for all information collections. The recommended treatment plan from the initial report has been fully implemented within our organisation.

All personnel have received GDPR awareness training.

All implemented documents and activities are to be reviewed on an annual basis, as per our Internal Audit Process.