GDPR Risk Assessment – Documentation presented to the customer

As JDI-UK undertakes the GDPR Risk Assessment then we look at different aspects of your business. This includes the current Policies & procedures documents. As well as all aspects of your "Personal Data" collection, manipulation and removal. Where a company does not have the relevant policy and procedures documentation then JDI will create a version based on the information that has been made available to us. The customer requires to review whether the policy requires modification or is required by the company.

In the documentation that has been created it holds **two main areas**:

GDPR Risk Assessment Findings & Observations and Policies & Procedures

GDPR - Risk Assessment Report

This is the GDPR Risk Assessment report which looks at how a company complies with GDPR. The Risk Assessment is based on 119 questions covering 7 areas which are the same questions that the ICO requires all companies to review and understand whether they have implemented policies, methods and other strategies to comply with the expectations. Each question can have 4 potential answers (NON-Applicable, Not Yet Started, Partially Implemented and Successfully implemented). Where we detect risks to the business relevant to the question then we identify whether the company has started to amend the specific questions criteria, or not even looked at it yet. The Data Controller should be looking to have each question with the "Successfully Completed or Non-Applicable" answer defined. Where its not yet started / partially implemented then this high-lights that there is a risk to the company. JDI provides full descriptive text to cove the current situation and expectations so that the Data Controller can make changes (where required) in order to minimise the risks to the business.

GDPR - Data Mapping Report

This document looks at all aspects of "Personal Data" that the company holds. It asks **WHY** does the company have the data (Legal basis for processing the data), **WHOSE** data is it (Customers, Suppliers, Employees etc), **WHERE** is the data located (Physical format, electronic within local desktop device, applications etc), **WHAT** actual data is held (individual fields or database cells) and **WHEN** the data is added, manipulated and eventually removed. The idea is that the company understands exactly what "Personal Data" it holds, and all the attributes about that data. The document also gives clarity as to when "Personal Data" should be removed / destroyed.

GDPR - CCTV Policy Document

This document is only required where the Data Controller has CCTV installed in their premises and the data Controller is responsible for the collection & protection of the images. This document is created with generic wording (Retention period defined as 28 days). The customer is required to review the contents of the document and make changes where required. This document would be managed & controlled by the person (Generally the IT Manager) who is responsible for the CCTV equipment.

GDPR - Data Protection Policy

Every company should have a Data protection Policy. The document is generally managed by the IT Manager (Working in connection with HR and other departments). The document and the contents should be socialised with all staff as they are expected to adhere to the companies Data Protection Policy. We create a generic document that covers a wide aspect of Data protection. Should the customer require to make changes or have specific items (relevant to the data Controller) added then this is expected. The customer is expected to review the document and ensure that the statements are being made are relevant to their company (and make changes where required).

GDPR - Data Breach Policy Document

Every company requires to have tis document. By default, it would have no entries. The document is generally managed by the Data Protection Officer / Lead. It is used to record ALL data breaches (including ones where the data protection Authorities are not required to be informed of the breach) This document would require to be made available to the Data Protection Authority (upon request). The document includes a copy of the policy and a report template at the bottom theta requires to be completed where there is ANY type of Data Breach.

GDPR - Document and Record Management Policy

All companies require to have this document. The purpose of the document is to understand where all data resides, and how the company expects data to managed. This document looks at Data retention and depending on the network topology would define expectations on how data is stored, manipulated, replicated etc. This document is generally managed by the IT Manager.

GDPR - Information Sharing Agreement

This document is only required where your company shares large amounts of data with other companies. This could include the passing of Personal data to a Data Processor that you are using to carry out a specific task. The document would define the expectations on both parties. If the document is not required due to your current operating model, then you should keep the document so that should your operating model change then you can use it (as required). This document is generally managed by the IT Manager or Data Protection Officer.

GDPR - Marketing Policy

This document is only required where a company is proactively marketing its business. The Marketing could be Business-to-Business (B2B0, or business-to-Consumer (B2C). The document defines the expected approach by the company to ensure that all marketing principles consider GDPR, the Privacy and Electronic Communications Regulations and the GDPR - ICO - Direct Marketing Checklist documentation. This document would generally be managed by the Marketing Manager (or person in charge of the Marketing of the Company). Where companies only advertise using social media & their website then this document is not required as there is no requirement to have consent to market using those methods.

GDPR - Privacy Statement

This document forms the basis of the privacy statement which the company should have on their website. A version of the document should be kept in offline physical format so it can be shared with people who do not have Internet connectivity. The physical version might be different as it includes employees and data not stored on the company's website / applications. We build a generic document which will require the customer to review, modify and then issue (where applicable). If the company already has a Privacy Statement, then it should ensure that its current version includes all aspects of GDPR.

GDPR - Subject Access Request Form – Customer

Every company should have a method of requesting identification from a Data Subject, where they (or their representative) is requesting a copy of the data Subjects data. This form can be used but can not be enforced. GDPR requires that the Data Controller positively identifies the Data Subject prior to releasing the information. This document explains the process to the data Subject, and the data provided by the data Subject helps identify the data sources that should be reviewed in order to release the Data Subjects personal data. This document should generally be managed by the Data Protection Officer.

GDPR - Subject Access Request Form – Employee

Every company should have a method of requesting identification from a Data Subject, where they (or their representative) is requesting a copy of the data Subjects data. This form can be used but cannot be enforced. GDPR requires that the Data Controller positively identifies the Data Subject prior to releasing the information. This document explains the process to the data Subject, and the data provided by the data Subject helps identify the data sources that should be reviewed in order to release the Data Subjects personal data. This document should generally be managed by the HR Manager. This form would also be used by Ex-Employees of the company.

Sample DPIA Template documentation (ICO)

This is a sample document that the Information Commissioners Office (ICO) has produced in the UK. The purpose of this document is to manage and identify Data Protection risks where a change in the companies' applications, Databases or other concepts of personal data storage are being changed. Its important that this document is used for all major changes in the company's strategies so that Data Protection is at the forefront of the company's considerations in all major changes.

Information from JDI-UK.

As part of our service we continue to work with (and support) your company in all aspects of GDPT and IT Support. The Risk Assessment should be carried out on an annual basis so that regulation changes can be considered and included in the future reports, alongside any changes in the Data Controllers operating model. We invoice our customers once the final draft has been created, but this does not always mean that the Risk Assessment report is finalised as there can be remedial work being undertaken based on the findings or ongoing changes in the business which amend the situation. If you have any questions, then please do get in touch as we are here to help you in all aspects of your IT and GDPR requirements. Where remedial work has been identified then JDI-UK can assist in carrying out the remedial work, but the cost of this is generally not included within the Risk Assessment report quoted costs. Once the report has been finalised then JDI is there to support you and answer all GDPR questions / queries to ensure that you continue to minimise the risks to your business. We don't charge for answering a question and where there would be a potential cost for our involvement then we would have clearly communicated this prior to carrying out any work.