General Data Protection Regulation (G.D.P.R) Risk Assessment Overview

Presented by: -
Paul Johnson (D.Sc.)
JDI-UK Limited

- All companies require to carry out a specific investigation and implementation exercise: there is no ‘off the shelf’ solution to GDPR. This was the intention behind the regulations, so engagement by all concerned is critical to becoming and remaining compliant. This should have been completed ***prior*** to **25th May 2018.**
- The above statement can be addressed by the carrying out of a GDPR Risk Assessment
- JDI-UK are here to help simplify and assist your company to understand the GDPR implications. We also help you prepare for the changes your business required to adapt to become and remain compliant with the regulations. Our GDPR Risk Assessor has over 35 years IT experience, including 20 years working with various Data Protection Acts so we bring knowledge & experience in what we deliver.

- **Preparing for the day of the Risk Assessment**
  - We will expect that a **Non-Disclosure agreement is signed prior** to the start of the Risk Assessment. This will be sent out with the information prior to the Risk Assessment date.
  - Do you Process Personal Data as a **'Controller' or also as a 'Processor'?** A processor will process personal information that was not given to them directly by the 'Subject'.
  - We will be looking to **review any Policies & Procedures which you already have**. These include Data Breach Register, CCTV, Data Protection Policy, Documentation & Record Management Policy, IT Data Processing & Security Policy, Information Sharing Agreement, Subject Access Request Forms, Marketing Policies, Legitimate Interests & Data Protection Impact Assessment (DPIA) documentation. Don't worry if you don't have these as we can build you copies.
  - Does your company own & manage any form of CCTV?
  - **Your ICO Registration Details** (Including Registration Number) if you have registered already. Not all companies require to be registered, but we validate this for you.
  - We will be looking at all of the systems, applications, devices & locations that would hold personal data on – So we could do with you identifying the relevant applications & locations. This includes Employee, Supplier, Business & consumer customers (as applicable).
  - If you have a **HR handbook** for your employees / Sub Contractors, then can you make this available as well?

- **Preparing for the day of the Risk Assessment**
  - What **training you give to your staff**? New Starters, refresher training etc. This is relevant to all aspects of Data Protection, Marketing, Records Management, CCTV & information sharing (where applicable)
  - A High-level understanding of your **Marketing strategies & the applications** / resources used. This includes Email, Phone, Text, Physical mail etc. (as in what type of marketing do you do). We also require to understand the audience – Business-to-Business (B2B), Business-to-Consumer (B2C) and whether you target any 'Sole-trader' businesses.
  - What companies process your personal data for you (E.G Accountants, Mailing Companies)
  - What companies you outsource to (where they would have access to manipulate your personal data). Examples would be a payroll company, Cleaning & Security companies, Confidential Waste companies, IT Companies,
  - An understanding of your IT Topology.
    - Does your company use a 'Domain Controller' environment, or a standalone design. The easiest way to understand this is that a Domain Controller environment allows an individual to use their username & password on any device.
    - Do you have applications hosted on system within your local intranet, or are your applications facilitated from the internet (Cloud solutions) or a blended
    - An understanding of where (location – Europe, USA or rest of the world) you house personal data.
    - Username & Password facilitation. How are they issued / managed etc.
    - What email system do you use (E.G Outlook), and who is the subscription procured through / where is it hosted from etc.
    - What IT Asset Management Facilities you have (E.G Excel Spreadsheet) to record the characteristics to your Server & client devices.
    - What versions of Windows operating system software you run on your Servers , Desktop & laptop devices – We run a script on all devices in order to build a complete picture (if you do not already do this). We identify Operating System versions that do not include Security enhancements including Bitlocker encryption.

- # The Day of the Risk Assessment
  - We will be working through a series of questions that are divided into 7 sections. You may feel its better to have different people available for each Section.

    - **Data Controller**: This includes IT, HR and General Management Staff
    - **Data Processor**: This includes IT, HR and General Management Staff (May not be applicable to your business)
    - **Marketing**: Marketing team, or anyone who is involved in marketing your company to others
    - **Information Security**: IT staff or external representatives (on the phone)
    - **Records Management**: General Supervisory staff – People who understand where data is housed & how its used.
    - **Data Sharing & Subject Access**: Data Protection Lead, HR and General Management Staff.
    - **CCTV**: Security / Who ever is tasked with this. (May not be applicable to your business)

  - We will require a desk and access to a few cups of coffee, Don't worry about Internet access (we use own connectivity).
  - We will build answers to the 119 questions and highlight any points of concern. The draft report is written up and presented a few days later. Any points of concern we will walk you through and agree a remedial solution to resolve the specific issues. Where remedial work is required, we will present a quote for consideration & carry out the work in an agreeable timeframe – Any remedial work that we complete will be written into V2 of the compliance report.
  - Where remedial work is carried out within a few days of the initial Risk Assessment, then we update this into version 1 of the Compliance Report and then submit for signoff with your company.
  - We don't invoice for the work until after the final compliance report has been submitted.

Contact Information

- **Address**
  - Registered Office: JDI House, 5 Church Walk, Preston, Lancashire. PR2 6SZ
  - Telephone: 01772 802702 / 07889 948484
  - Business Hours: Monday – Friday (8:30am – 6pm), Saturday – By Appointment.
  - Email: gdpr@jdi-uk.com

- **Barbara Kenny**:-
  - Email: - Barbara.Kenny@jdi-uk.com

- **Paul Johnson**
  - Email: - Paul.Johnson@jdi-uk.com

- **Company Websites**:-
  - Main Website: - jdi-uk.com
  - GDPR Website: - everything-gdpr.com

Our Aim: - To ensure our customers maximize their investment in IT, whilst reducing their overall spend. Being a trusted partner for our customers.