

## Introduction

The EU General Data Protection Regulation (GDPR) comes into force on 25 May 2018 and will supersede the current Data Protection Act 1998. GDPR will apply despite Brexit, and will impact all organisations that control or process personal data. It will grant data subjects a range of new rights, giving them more control over how their data is used. Organisations will be subject to new responsibilities and obligations, including the need to demonstrate compliance.

## What are we doing to ensure compliance?

At Impact, we are committed to protecting and respecting the privacy of individuals, and take our obligations under data protection legislation seriously. We already manage personal data in accordance with the industry standards for ISO 90001, ISO 14001 and OHSAS 18001. We understand and welcome the high standards that GDPR will promote and encourage across all organisations that process personal data on behalf of third parties.

Members of the Impact GDPR team are:

- Terry Kendrew, Managing Director, overall responsibility for Employee data
- Robin Harris, Finance Director, overall responsibility for Supplier and Customer data
- Angela De Klerk, Business Development Manager, responsible for Marketing data
- Elaine Smith, HR Manager, responsible for Employee data
- Nigel Gregg, IT Manager, responsible for IT/Software security
- Yvonne MacMillan, Credit Control Manager, responsible for Customer data

In order to ensure our readiness for GDPR, we have in place a multidisciplinary project team which, informed by an internal GDPR gap analysis assessment and specialist external advice, has the following key priorities:

- Modify and fine tune our existing management systems, processes and policies to ensure that we are GDPR-compliant.
- Ensure that our employees are fully aware of the new obligations that GDPR will introduce, and ensure that there is accountability and shared responsibility for ensuring compliance, from Board level and throughout the Group.
- Our Thirteen business units process personal data on behalf of our customers. We understand the importance of good data practices to our customers.

Some of the specific initiatives that we are currently progressing include:

**Data Review** – An extensive review of all personal data we hold, as we prepare a detailed data roadmap which outlines where this data is held, why we hold it and for how long.

**Contractual Updates** – A full-scale analysis of third parties who process data on our behalf, and updates to contractual positions to ensure that we (and our customers) are protected as best as is possible. In addition to this, we are updating our current business terms and conditions to give our customers the assurances required under GDPR.

**Process Updates** – Updates to our existing procedures to ensure we have the tools to maintain compliance with GDPR. This includes the appointment of a new Data Protection Officer, and a review of our existing policies such as our data security and incident response plans.

**Improved Subject Access** – Updates to our existing subject access request processes to ensure that it is easier and quicker for data subjects to exercise their rights.

**Review of consents** – Review of our existing marketing practices, and associated consents, to ensure that these are transparent, fair and GDPR-ready.

#### **What are the implications for our Employees and Customers?**

We understand the time and resource that is required to ensure that organisations are GDPR compliant. In supporting our customers to manage their risk-exposure and abide by the legislation, we are developing a number of measures and enhancements, through standard features, toolkits and added value solutions.

These include:

- Realtime protection of anti-virus, anti-malware and anti-spyware software.
- Improved security requirements (e.g. introduction of data encryption at rest).
- Encryption of all portable devices, protecting data in transit, this may include Secure Socket Layer (SSL) and Internet Protocol Security (IPsec) VPN connection, this will expand to include mobile phones.
- Development of data governance modules to our software solutions.
- Provision of template data protection impact assessments, with user-friendly guidance.
- Advice on data retention and deletion.
- Many more data protection enhancements are planned which may include multi-factor authentication, in addition to enhanced web-filtering preventing access to hazardous website URL's.

Over the coming months, we will be in contact with all our Employees, and Customers, to progress our GDPR readiness project.



Terry Kendrew  
Managing Director