The European Union (EU) adopted the General Data Protection Regulation (GDPR) in April 2016. When it comes into force in May 2018 it will consolidate rights for individuals who are resident in the EU (Data Subjects).

Most organisations that process personal data about EU residents (whether as customers, contractors or employees) will need to comply with the GDPR by mid-2018. Compliance will be a significant undertaking for most enterprises and failure to have a defensible approach to your responsibilities may result in substantial penalties. Are you going to be ready for it?

GDPR compliance is a wide-ranging task

It will drive changes in all aspects of the business architecture – people, processes, technology and data. To comply with the GDPR, organisations will have to:

Understand what personal data it holds, where, how it is sourced, how it is processed, and who accesses it.
• In a large organisation, personal data is typically handled in many systems (e.g. digital portals, CRM and billing systems, data warehouses, ad hoc extracts for reporting). It exists in structured and unstructured forms and may be accessible to employees in many departments. It may be sent to, or processed by, third parties (e.g. for physical fulfilment or direct marketing).
• It is recommended that these locations and processes are known and described (Article 30).

Ensure it can transparently demonstrate under what law or consent they are processing personal data.
• It may often require an explicit record of consent for personal data to be used for particular purposes (or obtain a responsible adult’s consent in the case of children (Article 8)).
• This must be respected across the organisation, and data subjects be given the ability to review and revoke consent effectively (Article 7).

Enable data subjects to exercise their rights under the GDPR.
• Data subjects will have the right to obtain a copy of the personal data you hold about them and to an in-depth description of how it is being processed (Article 15). They have the right to have inaccurate personal data corrected (Article 16) and in certain circumstances, to have it deleted (Article 17). They may also be able to demand an electronic copy of the data they have provided to you in a form suitable to move it to another service supplier.
• The GDPR requires that these processes happen “without undue delay and in any event within one month of receipt of the request”. Therefore, you need effective ways for data subjects to exercise these rights (Article 12)

Know how to handle data security ‘incidents’.
• In the event of a personal data breach that may result in a risk to individual’s rights, the GDPR (Article 33) stipulates that the controller must report the breach to the supervisory authority within 72 hours of discovery. This isn’t much
time, so processes to discover, investigate and report breaches need to be in place. Communications will also be necessary within the organisation and with external bodies (e.g. business partners and the media).

It’s not just your processing that needs to comply with the regulations, but also any processing carried out by third parties on your behalf (Article 28). There is also a need to make sure that the staff understand their responsibilities when processing personal data; and you will have to ensure that you can explain all of this.

Other things to consider will include:
- appointing a Data Protection Officer (DPO) to strengthen data governance, formulate policies and standards, and determine appropriate protection levels
- ensuring all future developments and system implementations incorporate the principles of ‘data protection by default’ and ‘data protection by design’
- creating a platform and environment capable of continuously demonstrating control of personal data
- working out a plan (including containment, rectification and communications), in case things go wrong.

Complying with the GDPR is serious and urgent

Organisations need to be able to demonstrate compliance by May 2018. Failure to do so may result in significant direct penalties. Article 83 of the Regulation requires that are “effective, proportionate, and dissuasive”. They can be up to €20,000,000 or 4% of global turnover, whichever is greater.

However, since GDPR gives people (such as customers) more control over their personal data, organisations that are making it clear they comply with it; are making it easy for individuals to exercise their rights under the Regulation, could dramatically increase their customers’ confidence and loyalty in their brand.

Organisations need to better understand what personal data they are holding on their customers, and how it’s processed. This can be achieved by identifying and fixing data and process quality issues, or getting a ‘golden view’ of the customers. GDPR compliance is a good reason for introducing good practice data governance processes, too.

All organisations need a defensible position on the GDPR

Since there’s potentially a lot of work to do, and not a lot of time to do it, there is a need to work out what the highest priorities are.

To help organisations comply with the GDPR, Cognizant Business Consulting has built on its established information management strategy assessment tool, EDGE, to create a GDPR Assessment. Based on a structured survey of key stakeholders, it produces a set of priorities to address to be ready for the May 2018 deadline.

About Cognizant

Cognizant (NASDAQ-100: CTSH) is one of the world’s leading professional services companies, transforming clients’ business, operating and technology models for the digital era. Our unique industry-based, consultative approach helps clients envision, build and run more innovative and efficient businesses. Headquartered in the U.S., Cognizant is ranked 230 on the Fortune 500 and is consistently listed among the most admired companies in the world. Learn how Cognizant helps clients lead with digital at www.cognizant.com or follow us @Cognizant.