ViClarity

White Paper

Getting Ready For General Data Protection Regulation (GDPR)

ViClarity

General Data Protection Regulation (GDPR)

The May 2018 implementation date for the EU backed General Data Protection Regulation (GDPR) is still some months away yet findings from research by security broker Netskope has claimed more than 75% of business apps lack key capabilities to ensure compliance under EU General Data Protection Regulation (GDPR). This lack of movement towards adapting the necessary steps and requirements to meet the regulations demands is equivalent to an organisation burying their head in the sand. The General Data Protection Regulation (GDPR) has been 4 years in the making and at its core is a set of rules that dictate how organizations should collect, store and dispose of the personal data of EU residents. The GDPR received the green light as of 14 April 2016 and will come into play across all EU member states from 25 May 2018, replacing Directive 95/46 EC and Member State implementing legislation.

The GDPR will seek to strengthen and unify data protection for individuals within the EU while also addressing the exportation of personal data outside the EU. This new regulation is seen as the most ambitious and comprehensive changes to data protection rules globally in the last 20 years. The demands of a 21st-century business see customers expecting business to operate at all times. The increasingly global economy allows little room for downtime and it is not tolerated by customers as they can readily take their business elsewhere. Data protection strategies need to take into account these 24/7 expectations but also the changing legislation around such protection strategies. On top of these customer demands, data protection is important because of the increased usage and reliance on computers and computer systems in certain industries e.g. financial services and healthcare. This increased usage has resulted in the recognition that data is an important corporate asset that needs to be safeguarded and the loss of such information and failure to comply with the relevant legislation and regulations can lead to direct financial losses, such as lost sales, fines, or monetary judgments.

The new regulation is applicable to any company that processes EU user data, even if that processing or data storage occurs outside of the EU. The new regulation upon its initial implementation in Data Protection Directive (1995) and the newest version which it will supersede has at its core the primary objective of giving citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. The new regulations contains some key changes, 5 of which are highlighted below:

- **Accountability**
  - Requirement to be able to demonstrate how compliance with GDPR is achieved.
- **Consent**
  - Sees the introduction of a higher standard for the conformance with an individual's need to consent
- **International Data Transfer**
  - Data Transfer to non EEA countries is prohibited unless sufficient protection is in place.
- **Privacy Notices**
  - Information to be provided to individuals in an easy accessible form, using clear language.
- **Individual Rights**
  - Provides individuals with enhanced rights regarding the processing of their personal data.

(LEDP) Law Enforcement Data Protection Directive (2016/680)

Another important parallel part to the GDPR is the Law Enforcement Data Protection Directive (2016/680) known as the LEDP Directive. The LEDP has been proposed by the European Commission but has not attracted as much attention and debate as the GDPR, but both constitute a package and were adopted together. The Data Protection Framework Decision 2008 will be replaced by LEDP and is to be implemented into national law from the 6 May 2018. This directive focuses on the protection of any personal data processed for law enforcement purposes.

The failure of an organisation to comply with the regulations outlined above will have negative implications in a variety of different forms ranging from a loss of customer and market confidence in the company's product offering as a result of non-conformance through to the surrendering of custom to organisations observing the

regulation requirements.

Perhaps the biggest implication is the financial one which sees the introduction of severe fines being imposed on organisations of up to USD 22 million or up to 4% of annual worldwide revenue.

Although 2018 sounds far away, in reality the process of GDPR preparation needs to begin now. Less than one in five Irish Organisations regard themselves as well prepared. It's imperative for organisations to take the first step in preparation now by putting processes in place to deal with GDPR and when May 2018 comes they can refer back to the processes in place and show regulators such as The Central Bank Of Ireland that they are on top of the situation.

ViClarity is a trusted provider of Risk & Compliance monitoring solutions which offer a number of solutions within these key market spaces to help organisations structure their legislative and regulatory compliance requirements through an effective, easy to use Enterprise Risk Management (ERM) workflow tool. ViClarity have introduced a new GDPR solution which automates the processes involved with GDPR preparation and ongoing compliance. The ViClarity GDPR solution maps directly on to the incoming regulation and provides organisations with a live overview of their GDPR risks, controls and actions.

For more information on ViClarity's GDPR solution or any other solutions call 01 902 2859 or email info@viclarity.com. Chat to us live on our website at www.viclarity.com.