Volume 2, Issue 1

Quarter 1 2017

Risk Management Newsletter

Data Protection

Data Protection Regulation is coming to the EU. This will have significant implications for Irish companies - not just to the likes of Apple, FaceBook and Google, but to all companies processing or storing personal data. In this issue we focus on what it will mean in practice for Irish companies and what they can do to be best prepared and to avoid potential fines and penalties.

Data breaches = bad news

Data breaches are happening already. Some are accidental, others are malicious; as far as clients and employees are concerned it doesn't matter, a breach is a breach and their personal information is out there. In one week in December we were notified of two separate data breaches affecting clients of our office and potentially affecting 3,500 individuals.

We don't yet have mandatory notification requirements as they do in other jurisdictions, yet the Irish Data Protection Commissioner (DPC) now deals with over 2,000 data breach notifications per year; that number has grown rapidly even in the absence of strong regulation.

The countdown is on

The EU's General Data Protection Regulation (GDPR) comes into effect on **25 May 2018.** It was drafted due to the fact that existing legislation is outdated and also in response to individuals being more aware than ever before of how their personal data is stored, secured and disposed of. Significant changes under GDPR will include:

- Mandatory notification to the DPC within 3 days of discovery of the breach
- Increased fines and penalties
- Obligations around correct requesting of, storage and disposal of personal data
- Those processing personal data of EU citizens will need to appoint designated Data Protection Officers (DPOs).

We gave a more detailed summary in our April 2016 newsletter, available here. We are attempting to establish what guidance various business associations will give to their members on the need to appoint DPO's and will include any responses received in a future edition of this newsletter.

With this in mind, we asked the Data Protection Commissioner what businesses can do to prepare for GDPR. The full interview is included in the following pages. At the back of the newsletter you will find some more examples of incidents we have come across in recent months.

We sat down with Dale Sunderland, the Data Protection Commissioners Deputy Commissioner with responsibility for Consultation, Corporate Affairs and Communications., to discuss GDPR and what it means for Irish businesses.

O'Leary Insurances: Most of us have an online presence of some form, often through social media accounts such as FaceBook or LinkedIn. As the large Yahoo data breach proved, a lot of our information is already available online, we have chosen to put it up there. What so are the DPC's concerns around data protection? What harm can come of it if a company has its clients' names, addresses etc. accidentally released or stolen?

DPC: As you rightly point out, much of modern living is transacted online and we voluntarily exchange large amounts of personal data in order to engage with those online services. As a regulator, our primary concern is always for the safe exchange, management and security of data. What we mean by that is that when you supply your personal data, you should be doing so under conditions of full knowledge of the identity of the other party (data controller) and purpose(s) for which it will be used. Personal data should be fairly obtained. That means that supplying your personal information should not be something you are coerced or tricked into providing. Organisations who hold personal data must ensure that they take all necessary safety measures to secure it. Obviously, this means that controllers need to be vigilant against hackers, but it also means that they must have retention and disclosure policies in place; they should encrypt, anonymise or pseudonimise the data where possible and they should be sure that they have adequate internal restrictions in place to ensure that only those people within their organisation who have legitimate need to access the data can do so.

"Accidents will always happen, but adequate preparation will certainly mitigate any potential risks arising out of them."

When personal data is breached, it presents a potential spectrum of implications for the data subject, ranging from embarrassment to real reputational or financial damage. It really depends on the type of data that has been breached and the form it was in when it was released. For example, the potential harm to individuals if a secured laptop containing encrypted data is stolen is significantly less that what might arise if that same laptop wasn't password protected and all the data was in its raw format. This is why we are so strong on the need for data controllers to have adequate internal systems for dealing with this. Accidents will always happen, but adequate preparation will certainly mitigate any potential risks arising out of them.

OLI: What kind of data are you concerned with in the new regulations? What is Personally Identifiable Information (PII)?

DPC: Personally identifiable information is information that can be used on its own, or in conjunction with other information, to specifically identify an individual. Under the new Regulation, we are concerned with all forms of personal data, in particular sensitive personal data such as health, racial, genetic and biometric data which is afforded a higher standard of protection. Businesses also need to be aware that IP addresses and other online identifiers are also types of information which are defined as personal data.

OLI: If the PII of one individual is lost, is that considered a breach? Or will there be a threshold below which mandatory reporting is not required.

DPC: The breach notification is mandatory, and any loss of data must be notified to the Data Protection Authority (DPA) within 72 hours, unless the breach is unlikely to result in a risk to rights of the individuals concerned. The Regulation does not provide for any minimum threshold.

On notifying breaches:

*"The Regulation does not provide for **any** minimum threshold."*

OLI: Are you seeing many data breaches at present? If so, what type of companies are most susceptible and what type of breach are most common (i.e. accidental or malicious)?

DPC: To end November 2016, the DPC received a total of 2,150 breach reports, of which 65 cases (3%) were classified as Non-Breaches under the provisions of the voluntary Code of Practice. Of the 2,085 valid notifications received between 01 January and 30 November, a total of 1,034 breaches (just under 50%) had occurred in the financial sector (banks & credit unions). The highest category of these reported breaches are postal and email disclosures which, in the majority of cases, have occurred due to human error.

OLI: Do you see mandatory reporting increasing the number of notifications to your office?

DPC: It's inevitable that it will bring about an increase in breach notifications. At the moment, breach notification is only mandatory for the telecommunications sector. The Regulation will extend that obligation to all companies processing personal data.

January to November 2016:

2,150 data breaches notified
3% Non-Breaches
97% consider Breaches

Almost 50% - financial sector
Majority are due to **human error**

OLI: How is the office of the DPC preparing for GDPR in terms of staffing and resources?

DPC: Our budget has increased annually over the last four years and we have used this to increase our staff, in particular through targeted recruitment for specialist posts including technologists, lawyers, auditors and investigators. We are currently almost 60 staff and this will increase to almost 100 in 2017. We have also established a city centre base in Fitzwilliam Square in addition to our existing office in Portarlington. We are engaged in training for all staff and obtaining internationally recognised certification for them. The GDPR presents a challenge for the DPC, but we are definitely putting in the necessary foundations to meet that challenge in 2018.

OLI: The new legislation comes into force in May 2018. What can small to medium sized enterprises be doing in the interim around data protection, and what can they do to ensure they are best prepared for when it comes into effect?

DPC: We have published guidance on our website www.dataprotection.ie on preparing for the GDPR which we would recommend all businesses review and follow. On the whole, the rights individuals will enjoy under the GDPR are the same as those under the Acts, but with some significant enhancements. Organisations who already apply these principles will find the transition to the GDPR less difficult.

A central part of getting ready for the GDPR is preparing for its new accountability requirements. This will include maintaining a record of all processing activities carried out by the organisation. There are however some exemptions for organisations with fewer than 250 employees, unless the data they process poses significant risk to data subjects, or their core business involves processing personal data. Business should also review their procedures to ensure they cover all the rights individuals have, including how the organisation would delete personal data or provide data electronically and in a commonly used format. An important change of particular note is the reduction in the time allowed for complying with access requests from 40 days to one month.

OLI: Companies processing sensitive data will need to nominate Data Protection Officers. What will their role be?

DPC: The GDPR will require some organisations to designate a Data Protection Officer (DPO). Organisations requiring DPOs include public authorities, organisations whose activities involve the regular and systematic monitoring of data subjects on a large scale, or organisations who process what is currently known as sensitive personal data on a large scale. The Article 29 Committee comprising all of the EU's data protection authorities has published guidance on the DPO role which should be of assistance to businesses. The DPO will have professional standing, independence, expert knowledge of data protection and be "involved properly and in a timely manner" in all issues relating to the protection of personal data. He or she cannot be dismissed for performing their data protection officer tasks. The important thing is to make sure that someone in your organisation, or an external data protection advisor, takes responsibility for your data protection compliance and has the knowledge, support and authority to do so effectively. Therefore, you should consider now whether you will be required to designate a DPO and, if so, to assess whether your current approach to data protection compliance will meet the GDPR's requirements.

OLI: How will you ensure firms are notifying your office of data breaches?

DPC: We are developing an online portal which will simplify the process of reporting a breach to this office and make it easier for data controllers to act in a timely fashion. Reporting breaches will be a legal obligation and failure to do so may have serious consequences. The GDPR greatly enhances the power of the DPC to level penalties against data controllers who do not comply with this requirement. There will obviously be mitigating factors; for example, a company which incurs a breach despite taking adequate security measures will not be liable for the same penalties as a company who has neither secured their data nor reported the breach. The GDPR reflects a changing climate around citizens' understanding of privacy. It is increasingly becoming a priority for consumers, so it is very much in the reputational interests of data controllers to comply with the GDPR provisions and engage with their lead supervisory authority.

OLI: On the continent, data protection officers have a reputation for being heavy handed on those that have suffered data breaches. The Irish DPC is currently seen as more approachable, resolving most queries with a call or an email and only coming down hard on companies with particularly poor procedures in force. Will the impending harmonised EU legislation change this approach?

DPC: Given the many major international companies that locate here, we are very aware of the importance and visibility of our role in safeguarding the data protection rights of many millions of individuals across the EU. Equally, we are deeply conscious of the economic context in which we carry out our functions recognising, as the EU does, that processing personal data is necessary for the continuing advancement of enterprise and society. This is why we place such a huge emphasis on being open, engaged and balanced in our approach to dealing with business. For us, it is more effective to engage proactively with business to promote data compliance before something goes wrong which we believe best serves the interest of individuals and achieves the greatest systematic impact in terms of data compliance. However, we do handle several thousand complaints a year, 1,000 of which give rise to a statutory investigation. We also have very strong powers of inspection and powers to enforce compliance with the data protection acts which we do as and when necessary. The shared goal of all EU DPAs is to ensure the safety of citizens' personal data and we will be exercising our enhanced powers in cooperation with other EU DPAs as necessary in accordance with the Regulation. Clearly the consequences for organisations will be assessed in the context of the nature of an infringement and the organisation's efforts to comply with the law.

OLI: Companies have been put on notice about GDPR well in advance. Can we expect fines and penalties as soon as GDPR comes into effect? Do you envisage fines and penalties for those in breach of the regulations, or will there be warnings handed out first?

DPC: GDPR Article 83 is very clear in setting out the criteria to be considered when deciding whether to impose a fine and how to assess the appropriate level of fine that should be imposed. Issues such as the gravity of the infringement, whether it was intentional, whether any mitigating actions were taken by the data controller to reduce the impact on data subjects all need to be considered. The DPC will take all of these matters into account when investigating potential infringements. However, the important message for organisations remains; to take all necessary steps now to be ready to comply with the GDPR and avoid breaching your obligations.

OLI: Finally, have you any other words of advice for Irish SME's around data protection?

DPC: Follow us on Twitter @DPCIreland for information and guidance on data protection compliance and the GDPR! And remember, good data protection practices in your organisation involve doing what is right and fair, and indeed ethical, by your customers and employees. It will help you command client loyalty, protect your reputation, avoid becoming the subject of civil actions or dealing with breaches which side-tracks organisations from dealing with their main business. Therefore, we are saying that, in addition to being a legal obligation, it makes sound business sense to future-proof your organisation against GDPR implementation on May 25th 2018. Data protection is not a barrier to efficiency and innovation; it's a pathway to doing things in a sustainable, lawful and sound way.

Dale Sunderland joined the Data Protection Commissioner (DPC) in May 2016. He is Deputy Commissioner with responsibility for Consultation, Corporate Affairs and Communications.
T: 1890 252 231 E: info@dataprotection.ie W: www.dataprotection.ie

Risk Management Newsletter

Thank you for reading our newsletter. Below are links to our own social media pages. Follow these to keep abreast of important updates.

LinkedIn: https://goo.gl/u06ncG Twitter: @OLearyInsurance Facebook: https://goo.gl/DILziV

Below are a selection of cyber incidents that we have come across recently. As usual, these are all real-life Irish cases.

Cybercrime

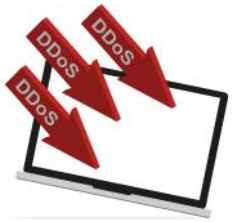
A **hotel** implements dual verification on bank transfers - that is they double check all email instructions by picking up the phone. However, a director was under pressure to respond to an email request for a transfer as he headed into an important meeting, so he authorised the transaction. The request was fraudulent and € 100,000 was lost.

Data breach

A **financial services** company based in Munster was running its month end reports. It uses a third party as its Customer Relationship Management software provider. The third party accidentally uploaded details of 3,000 of their clients to a Dublin competitor. Under GDPR, the financial services company would be responsible for the data breach despite not having instigated it.

Denial of Service (DoS)

A **solicitor** acted for a plaintiff in a case. The defendant in the case targeted her mobile phone in a DoS attack. Basically, they used multiple compromised systems to divert traffic towards their target's system and render it useless. This caused disruption to the business for three whole days.



An **architect** suffered a similar incident and the firm completely changed their systems as a result.

If you wish to discuss further please contact us. For new clients please contact cyber@oli.ie or 021 453 6860.

About O'Leary Insurances

Insurance Brokers & Consultants, Est. 1961

From an initial complement of three staff in 1961, originally founded by the late Archie O'Leary, O'Leary Insurances has successfully grown & developed into an Insurance Brokerage which specialises in providing a high level of customer service throughout Ireland.

With over two hundred employees now operating from nine locations nationwide, O'Leary Insurances provides a comprehensive insurance broking service to all sectors of the Irish Economy. As part of this insurance broker service, we have consistently maintained our strong emphasis on professionalism and personal attention through all of our products, buildings on our hard-earned reputation for dependability and commitment.

Our highly trained and experienced personnel would be delighted to be of service to you and would welcome the opportunity to discuss both your Personal Insurance and Business Insurance requirements with you. We are confident that our knowledge and expertise can assist you in the management of your insurance needs and can assure you of our very best attention in meeting the challenges of the future.

Disclaimer – as insurance brokers we cannot provide legal or risk management advice.

Thank you for reading.