Development and Enforcement of the GDPR Regulation

Background

European data protection law has not undergone a significant update since the EU adopted the European Union Directive (95/46/EC) in 1995. It was implemented in 1998 after a "grace period" of more than two years. Now, 23 years later, on 25th May 2018 the new law known as the General Data Protection Regulation (GDPR) will replace the aged 1995 Directive in a move that, according to the Office of the Information Commissioner in the UK, signals an **evolution** rather than a **revolution** for data protection. It was adopted in 2016 with a "grace period" of two years. GDPR is intended to strengthen and unify data protection law in the digital age. It means that any organisation, large or small, processing or controlling data in the EU must comply with the Regulation which will be transposed into the national laws of each member state.

At this point in time most people are familiar with the sanctions (fines and penalties) which can be imposed for breaches of the terms of the Regulation. The fines, which can amount to €20 million or 4% of annual turnover, whichever is higher, can be significant for any Company found to be in conflict with the Regulation. While such facts are useful in attracting attention, in reality it is very unlikely that such an onerous penalty will be imposed initially. Regulatory Authorities would have to assess fines along with a set of mitigating and aggravating factors; for example, an intentional violation is worse than a negligent one. Fines may be limited if data processors or controllers can mitigate the gravity, duration and/or damaging nature of the violation by reporting it as soon as possible and cooperating with the statutory authority. If an individual is hit with a fine, their income level and personal economic circumstances will influence the fine amount. Furthermore, there are two levels of maximum fines depending on whether the data controller or processor has committed any previous violations. The nature of the violation in question is also a consideration.

Implementation

When the EU Parliament and Council agreed on the terms of the GDPA in 2016 it gave organisations a "period of grace" to become compliant with its extensive requirements. The enforcement date in May 2018 is just two months away and various national Regulatory Authorities are beginning to get anxious as to whether the two year "grace period" should be extended for some short period after May 2018. In France the Regulatory Authority, La Commission Nationale de l'Informatique et des Libertés (CNIL) has indicated that it may postpone enforcement actions for a few months provided that organisations are making genuine efforts to become compliant and that they cooperate with the CNIL. Other national Regulatory Authorities are also considering extending the" grace period "after the 25th May 2018 deadline provided that organisations are making genuine efforts to be compliant.

The development of data protection legislation has always been treated thus, in the sense that legislation is enacted and then there is a "period of grace" during which entities and authorities try to come to terms with the new legislation. This is largely because the legislation itself is trying to cope with shifts in the technological landscape. Sweden was the first country in the world to enact national data protection legislation in 1973 in response to public concerns around the increasing use of computers to process and store personal data. It was more than 20 years after the enactment of the Swedish legislation that the EU Data Protection Directive was adopted in 1995. The Directive focused on the protection of individuals with regard to the processing of personal data and the free movement of such data. However, by the time the " grace period " had expired and active enforcement was being considered, computer technology and communication methods were being developed and used which could not be effectively controlled or come within the remit of the 1995 Directive. Now, more than 20 years later, in 2016 the GDPR was adopted and afforded a "grace period "of two years until the 25th May 2018. In all the legislative attempts to control data protection in the past 40 years there have been considerable" grace periods" which permit entities to become familiar with data protection legislation. The tendency has been that if businesses are taking their data protection preparations and obligations seriously and are making genuine efforts to comply with the rules they have less to fear than those opting to do little or taking a "wait and see" approach. It is likely that the Regulatory Authority will be more vigilant in relation to businesses which have, to date, been less compliant with data protection rules. However in GDPR there a new provision which makes it mandatory to report a data security breach and the terms of this provision may make it more difficult for the Regulatory Authority to be conciliatory or accommodating towards the offending data controller.

Mandatory Reporting

A data security breach has to be reported to the Regulatory Authority within 72 hours. Where there is a high risk to individuals those individuals must also be informed without undue delay. This provision also includes that the data subject should also be made aware of the data breach. In such circumstances it is likely that the data subject will react quickly; therefore the offending company could be subject to sanctions and legal action very quickly once the Regulation comes into force. This is particularly true because knowledge of the breach is triggered by the reporting to the Regulatory Authority by the data controller and the data subject is made aware of the breach. Therefore it is not simply a regulatory matter between the Regulatory Authority and the data controller because the injured party, the data subject, will also be seeking redress. The data controller should have a detailed procedure prepared in advance to deal with appropriate matters the day *after* a data breach has occurred in the organisation. A log should be kept of all the decisions that are taken and the data controller should be ready to explain and provide evidence of full compliance at any time. The GDPR is about managing risks and fostering an accountability culture. If GDPR is correctly implemented it will not only protect important information but it will also protect the organisation's reputation. Therefore it is recommended that all data controllers

develop an action response plan for data breaches rather than reflecting on what to do if a data breach occurs.

Finally, GDPR promotes the creation of codes of conduct and certification programmes. This will be the matter of considerable interest for the LIC organisation. In the next article on this subject I intend to deal exclusively with the effect of GDPR on the debt collection industry.

Liam M de Feu
President LIC

16 March 2018