Link to Article

The GDPR enforcement deadline is looming – are you ready?

Is this relevant to the Wealth Management community is Asia?

It is relevant to your business if you have "an establishment" in the EU and you process EU citizens personal data outside of the EU or your business offers "goods or services" to or "monitors the behaviour" of EU citizens within the EU.

The General Data Protection Regulation (GDPR)

"The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established."

If there were any doubt about how seriously the European Union ("EU") takes the issue of data privacy, the opening words from the EU GDPR website provides several clues.

First, the type of legislation by the EU used has been uprated from a "Directive" to a "Regulation". This means that the law has direct effect and requires no Member State implementing measures to have this law applied in every state within the Union. It is also important because it removes risks that might arise in how Member States interpret the law when implementing it, as is commonly the case with Directives.

Second, is the extension of the protections afforded to citizens; specifically referring to data breaches as well as issues of privacy. This is a significant step forward and signals a change in approach; moving from a reactive to a more interactive style.

Third is the recognition that the "data" world has changed beyond all recognition since 1995 and that international boundaries have little or no relevance to the ease of

HOW IS THIS RELEVANT TO ME?

The language of the Regulation is clear:

*"**Article 3***
Territorial scope

1. *This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*
2. *This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
   - *(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
   - *(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.*

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

This means that you will have to comply with the Regulation if:

- *you are a Controller or Processor who has an EU based establishment, but you process relevant data outside of the EU; or*
- *you have no EU based establishment, but you process personal data of EU citizens because you are offering goods or services..." to them or your business is engaged in "monitoring of their behaviour..."*

To determine whether you are "offering goods or services" to EU citizens, the mere accessibility of a website operated by a Controller, Processor or Intermediary by EU data subjects and use of an EU language are not enough. There must be other evidence to show that there is an intention to offer such goods or services to persons in the EU. The inclusion of prices in EU currencies is regarded as a strong indicator of such an intention.

As regards monitoring the behaviour of data subjects, this involves tracking individuals on the internet including profiling an individual, particularly in order to take decisions concerning them or for analysing or predicting their personal preferences, behaviours and attitudes.

If your business targets EU citizens, you should already be a long way towards making the necessary changes to your business systems to meet the requirements of GDPR. For those businesses that do not regard EU citizens as a significant target market but will work with them if approached, this may not be high on your agenda. If the latter is true for you, then you need to develop a plan to assess your vulnerability to this legislation as a matter of urgency.

General Data Protection Regulation - Regulation 2016/679
GDPR Key Changes

movement of data and, accordingly, laws affecting this vital area also need to be transnational and applied consistently.

It is in this context that the greater extra-territorial applicability makes it important that Wealth Managers who typically operate outside the EU consider whether this applies to them.

A step change in the protection of an individual's data?

The first thing to remember is that the GDPR is aimed at protecting EU citizens, so to that extent the focus remains the same and so does the overall framework, including the data protection principles which underpin the EU's approach to this area.

What is changing is the ambit of those protections and the way those protections are applied and enforced. It also has consequences for how businesses organise themselves to meet these challenges.

There are two fundamental shifts contained within the Regulation. The first relates to the operational framework within which data processing occurs and the need for greater emphasis on the correct management of data to protect what is now increasingly seen as an individual's primary asset, their personal data.

The second focuses on extending the rights of individuals to allow them greater power to control how their data is used.

OBLIGATIONS IMPOSED ON BUSINESSES

Privacy by Design

By no means a new concept, but now made into a legal requirement by the GDPR. Indeed, the language of the regulation goes further. Under the heading "Data Protection by Design and by Default", the intention of EU legislators is clear, making data protection a core component of system design, rather than a later addition. The consequence being that data protection must be an integral feature of the way the system operates and reduces the risks of data breaches by making data protection the "default" position of each system.

Sadly, the EU does not follow its strictures on clear and plain language but including the full text of Article 25(1) and (2) gives a clear indication of the extent of the obligation placed on data Controllers:

1. *"(1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the Controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection*

principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. *(2) The Controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."*

What is clear is that the expectations on Controllers (and by default Processors) have been greatly enhanced. Requirements to continually assess the purpose or processing and consequently the data that needs to be used to achieve that purpose are significant. What is also clear is that the range of factors to be considered by Controllers in making these decisions are also significant and that consideration will need to be documented to be able show that "appropriate" measures had been put in place in the event of a data breach.

Consent

The conditions imposed on companies for demonstrating they have consent for data processing have been made more stringent. In short, to be able to demonstrate that consent has truly been given, Controllers must show that requests for consent:

- use plain and simple language; and
- are provided in an easily accessible form, clearly explaining the purpose and the processing that consent is sought for; and
- are limited in scope both as to use and time.

There are two other points here, the giving of consent must be clear and distinguishable from any other matters that the individual may be asked about in the process being followed and it must be as easy to withdraw consent as it is to give it.

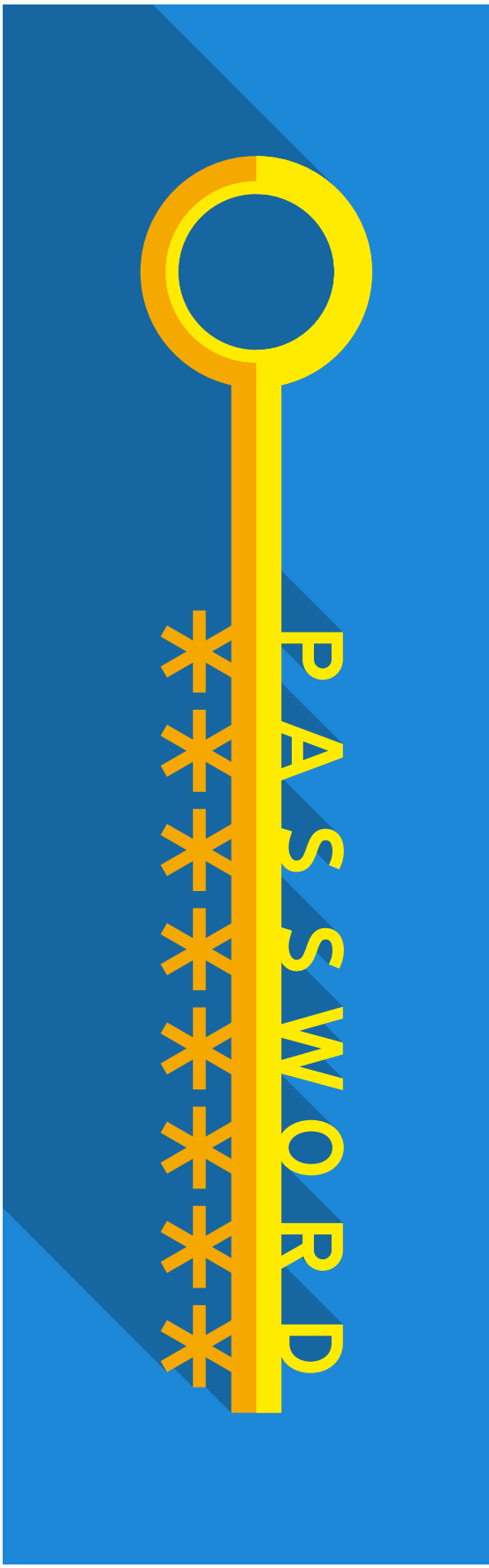
Pseudonymisation

This is a concept introduced into the Regulation and is regarded as an important measure to be adopted by Controllers to protect personal data, it is defined in Article 4(5) as

"the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".

Penalties

Perhaps not surprising with the range and extent of recent data breaches but the consequences for breaching the GDPR can be



Access to European Union law

significant. Interestingly, and very sensibly, the approach to punishment is tiered depending upon the severity of the breach. Primarily to help enforcement across Member States (and to ensure consistency) specific upper limits have set to frame the enforcement process.

For the most egregious infringements of the GDPR (for example, breaches of Articles 5, 6, 7 and 9, Articles 12 to 22, Articles 44 to 49, or Article 58(1) & (2)), fines could be up to the higher of either 4% of turnover globally or EUR20 million.

For less egregious infringements of the GDPR (for example, breaches of Articles 8, 11, 25 to 39 and 42 and 43), fines could be up to the higher of either 2% of turnover globally or EUR10 million.

What is less clear is whether the difference in approach the Regulation is setting a bar. For example, does the tariff for a serious breach, say of Article 5, start at 2% or is a lower starting point an option?

It is worth noting that these apply to both Controllers and Processors of Data.

Data Controllers and Data Processors

Under the current Directive, Controllers are required to notify their data processing activities with local supervisory authorities, which, for multinationals, is a significant administrative burden with different notification requirements in most Member States.

This disappears under GDPR as it will not be necessary for companies to register its data processing activities with each supervisory authority. Equally the requirement to notify or obtain approval for transfers based on the Model Contract Clauses is removed. Instead, there are internal record keeping requirements.

However, for the first time Processors have obligations directly imposed upon them, partly in support of the obligations placed upon Controllers and partly to help deliver transparent services and protection for individuals.

Those obligations centre on record keeping and the need for having appropriate expertise within their organisations and appropriate procedures for meeting these obligations.

Data Protection Officers

The Act creates a process by which The appointment of a specially designated Data Protection Officer ("DPO") will only be mandatory for those Controllers and Processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data.

When they are required, a DPO:

- Must have expert knowledge on data protection law and practices
- Must report directly to the highest level of management
- Must be provided with appropriate resources to undertake duties and maintain expertise
- Must not have other responsibilities which could result in a conflict of interest
- May be a staff member or an external service provider

RIGHTS OF INDIVIDUALS

Right to Access

An area where the rights have been expanded amid the push towards transparency and giving data subjects the opportunity to exert greater control over their data.

Data subjects (individuals) will be able to demand confirmation as to whether their personal data is being processed, where and the purpose of that processing. Controllers will also be required to provide a copy of that data in electronic format free of charge to the data subject.

Right to erasure

Also known as the right to be forgotten, this is another significant step towards empowering individuals, Article 17 requires data Controllers to erase personal data held by them "without undue delay" if requested by the data subject. This includes stopping dissemination of personal data and halting processing by third party Processors acting for the Controller.

This right comes into effect in several situations, the most common being the personal data is no longer relevant to the initial purpose for processing the data or the data subject withdraws their consent to the processing. But it is not an absolute right, Controllers must consider a range of public interests in the data being retained.

Right to notification of a breach affecting their data

A new addition to the rights of individuals, who must be notified, where there is a "high risk to the rights and freedoms of natural persons", when their data has been subject to a data breach "without undue delay". When allied with the broader obligation to notify the appropriate supervisory authority within 72 hours of becoming aware of a data breach, this becomes an onerous obligation.

While the language seems reasonable "72 hours after becoming aware of…", when one looks at the requirement to enshrine data protection "by design and by default" into a business' systems, the scope for justification of not becoming aware of a data breach very quickly will be increasingly limited as time moves forward.

Summary

The GDPR is undoubtedly a significant piece of legislation. It will require affected businesses to review and assess all their systems which capture, store and process personal data of individuals who are EU citizens.

The regulation came into force in May 2016 but with a deferred enforcement date to 25 May 2018. The fact that the EU mandated a two-year implementation period is indicative of the EU's recognition and understanding of the impact this will have on businesses and the long lead times needed to embed "Data Protection by Design" within business systems.

The choice of words here is key - 25 May 2018 is the Enforcement Date, ie the date upon which the provisions will become enforceable. In this respect, it is different to MiFID II which has a similar lapse of time between the law being created and coming into force. MiFID II provisions enter into law on 3 January 2018, GDPR is already the law, it is just not yet enforceable.

While some may regard this as semantics it remains to be seen how Member State regulators will view this.

Certainly, it is open to regulators to take the view that business has had a long lead time and should already be compliant with the Regulation and those that are not should receive no leniency.

With the increasing frequency and scale of data breaches, either through targeted attacks by criminal organisations or poor internal systems and controls, it would be a brave business to assume that a further, post enforcement date, grace period will apply. ■