The General Data Protection Regulation: Protection or Problem?

Former Enyo Law Legal Assistant Sam Parsons discusses some of the positive features of the new EU General Data Protection Regulation ('GDPR') as well as the challenges it may pose in the future.

What is the GDPR?

The GDPR makes some significant changes to the Directive that has governed EU data protection since its implementation in 1998.[1] The key changes are as follows. First, the use of a Regulation minimises the scope for Member States to tailor data protection laws, and is a real step towards creating a harmonised single digital market. Second, subtle changes have been made to the requirements for consent, which are designed to raise the bar for the protection of EU citizens' data. Third, data processors will need to take additional steps to fulfil their compliance requirements, including making data privacy impact assessments, appointing a data protection officer in many cases, and notifying national supervisory authorities if and when breaches occur. Fourth, the size of fines that data processors are subject to is significantly increased. Fifth, the GDPR grants data subjects the right to demand access to their data in an easily portable format, and enshrines their 'right to erasure' (previously known as the 'right to be forgotten') first seen in the *Google Spain* ruling of the Court of Justice of the European Union ('CJEU').

Like the Directive that came before it, the GDPR sets a new international standard for data protection. Even outside of the EU, any data processing that has effects on EU citizens will need to comply with the GDPR (Article 3).

EU Data Protection after Brexit

Preparing for a Regulation that is due to apply from 25 May 2018 might be viewed as an unnecessary concern for British businesses in light of the result of the Referendum on European Union membership.[2] But whatever results from the outcome of Brexit, European trade will still form a core part of British business. It would be folly for companies in the UK to ignore this key piece of European legislation, particularly as it is premised on Fundamental Rights.[3] The lengthy negotiations over the EU-US Privacy Shield are demonstrative of the care the UK must take in whatever data protection regime it chooses to follow after Brexit.[4] It would therefore be reasonable to assume that data protection in Britain will continue to resemble the European model, at least in the short-term.

Overview of Challenges

The Internet is unlike any other resource or marketplace, not least in the way that it transcends national borders. Harmonisation of data protection standards across the EU is therefore a welcome step towards overcoming geographical borders to create a single digital market. Potential problems focused on in this article relate to consent, the introduction of larger fines, and the position of companies that fall victim to hacking.

Consent

The first 'principle' of the GDPR as given in Article 5(1)(a) requires that personal data shall be "processed lawfully, fairly and in a transparent manner." In this context, "lawfully" means in accordance with Article 6 - processing will be lawful only if one or more of the criteria in Article 6 are met. The first of these is that "the data subject has given consent to the processing of his or her personal data for one or more specific purposes."

[1] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[2] See: Reform of EU data protection rules

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Recitals 1, 2, 4.

[4] See: European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows

Article 7 sets out the conditions for consent:[6]

1. *Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*

2. *If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*

3. *The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*

4. *When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*

A provision on consent seems both necessary and sensible; Internet users should be made specifically aware of what they are signing up to and be able to withdraw their consent just as easily as they give it. Furthermore, services should be offered in a way that is clearly distinct from the processing of personal data.

However, three issues arise from this paragraph. The first is that although consent must be given freely and separately from other matters, actual consideration of data protection independently from the rest of the contract is unlikely to take place. It is submitted that in practice all this means is that the user will need to check two boxes instead of one when accepting an online form. Once she has been through the process of downloading and - in a minority of cases - reading the contractual text before accepting a contract online, she is unlikely to be deterred by a second checkbox. This begs the question whether consent has really been freely given.

Second is the idea that consent cannot be given on a 'take it or leave it' basis - can consent really be given separately from the remainder of an agreement? The most obvious example is to be found in social media platforms.[7] Access to user data is part and parcel of the deal struck between the platform and the data subject. Presumably in such cases, consent will continue to be given so that the contract can be continued, and will only be revocable on an 'all or nothing' basis. But this is by no means obvious from the drafting of the Regulation, whose aims appear to point in the opposite direction.

The third and largest question is to what kind of data processing users must consent. The determination of whether or not consent has been given may depend upon how narrowly or broadly the terms of use are defined. Article 6's "one or more specific purposes" definition is - it is submitted - too vague to be of assistance to companies. As with the above point, a widely-draft consent clause is unlikely to deter many social media users. There is nothing to indicate that a statement such as "data will be used for any purpose whatsoever" will not be sufficient to fulfil the consent provisions.[8]

In sum, despite the attempts of the EU institutions to protect EU citizens and their data, this work may all very easily be undone by the citizens themselves. It is submitted that a CJEU ruling is required for the exact boundaries of expressions such as "one or more specific purposes" to become clear. In the meantime, it would be prudent for companies not to draft such clauses too widely, or in such a way that goes against the grain of the Regulation.

Fine size and Disincentives

One of the most talked-about aspects of the GDPR are the dramatically increased fines that companies and other data processors may have to pay in the event of non-compliance. Supervisory authorities are to introduce "effective, proportionate and dissuasive" fines in cases of breach of various obligations set down by the GDPR (Article 83).

[6] Further defined in Article 4(11): 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

[7] Such platforms were probably at the forefront of the GDPR's drafters' intentions.

[8] Although companies may still fall foul of other rules in the Regulation, notably on data minimisation.

In cases where the fault was of the controller, processor, or the certification or monitoring bodies, fines may total "up to €10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year" (Article 83(4)). For breaches including the basic principles for data processing (such as consent), the data subjects' rights, or relating to transfer of data to third countries, the party may be "subject to administrative fines up to €20,000,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher" (Article 83(5)).

One of the aims of the GDPR is to create a culture of compliance. Coupled with the obligation to appoint a Data Protection Officer in settings where data collection is, broadly speaking, on a large scale or of a more sensitive nature (Article 37), these new fines represent a significant increase in pressure on companies to take proper care of data under their control. There are also obligations to report breaches in some instances, which could create even more severe reputational damage for companies.[9]

All of this should incentivise a culture of compliance, transparency, and openness. Such large fine - combined with the reputational damage associated with reporting - could threaten the existence of many companies. But although the GDPR makes specific provision that Data Protection Officers must be protected in carrying out their duties,[10] there still exists a large incentive not to report breaches simply *because* the potential fines are so large. In a circumstance where potentially hundreds of jobs, including one's own, will be weighed up against a list of strangers' names, there is a clear emotional incentive against reporting. For less scrupulous companies, the potential for such large fines may therefore end up being the opposite of "effective, proportionate and dissuasive," especially if the breach will not be discovered without reporting.

It is hoped that supervisory authorities such as the UK's Information Commissioner's Office ('ICO') continue to offer a supporting and preventive role to companies. The GDPR may grant them new powers to levy fines, but it would not be in their interests to be too heavy-handed.

Types of Breach

In a perfect world, taking reasonable precautions would be sufficient to prevent any security breach. However, the more commonly-acknowledged reality within cyber-security circles is an expectation along the lines of "everything has been hacked. We just don't know about it yet."[11]

The GDPR will continue the pattern of levying fines on victims of malicious cyber attacks if it is determined by the Data Protection Act ('DPA'), which will no doubt continue to be controversial. In 2013, for example, the ICO fined Sony Computer Entertainment £250,000 under the DPA after the company fell victim to a hack that resulted in the personal details of millions of gamers being leaked online. The ICO came to the conclusion that Sony's defences were not adequate in the circumstances.

The drafters of the GDPR acknowledge that breaches may occur despite measures taken by companies to reduce their likelihood. Article 83(2) lists a number of factors to be taken into account when deciding whether to impose an administrative fine and the amount of any such fine.[12] As such, the reputational damage that a company will suffer from falling prey to a malicious hack is unlikely to be compounded by a disproportionately large fine.

However, there is no guarantee of clemency from the supervisory authority, nor is there any specific guidance in the Regulation as to what will constitute adequate protection against being fined after being the targeted. With so much of the practical implementation of the GDPR dependent on Codes of Conduct and national supervisory authorities, this brings into question the likelihood of a truly harmonised standard across the EU being achieved.

It also makes economic sense for there to be a level of proportionality inherent in whatever steps a company takes to protect the data it collects. While fines as large as 4% of annual global turnover will encourage companies to err on the side of caution, this may also lead to the diversion of resources away from more productive investments. The improved efficiency that the EU institutions believe the GDPR will herald may in fact be stymied by the spectre of such massive fines, even in cases where - as happened to Sony - the company claimed it took sensible precautions.

[9] Articles 33 and 34.

[10] Artcile 38(3): "...He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks…"

[11] Pinned tweet on Sheera Frenkel's *Twitter* account.

[12] Article 83(2).

Conclusion

The GDPR marks a significant step towards the goal of creating a single digital market. The Regulation is to be lauded for its foresight and for taking data protection rights seriously. But in taking the steps it does, it will require equally large commitments from data processors to update their protocols, methods, and technologies. Whether the goals of the Regulation will be achieved in practice may be determined by matters that come before the CJEU. Just as key cases on the Free Movement of Goods such as *Dassonville* and *Cassis de Dijon* cemented the integration of the physical single market, so it may now fall again to the CJEU to demarcate the boundaries of the digital single market.