Challenges old and new: An analysis of the impacts of the General Data Protection Regulation

Neil Fraser

Technical Report

RHUL–ISG–2018–4

3 April 2018

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

EXECUTIVE SUMMARY

The *General Data Protection Regulation* (GDPR) will come into force on 25 May 2018. Its intent is to harmonise data protection laws and provide individuals with increased control over how their personal data is collected and used. By obligating companies to protect and use responsibly the personal data in their care, GDPR seeks to reinforce trust in organisations, support the development of new technologies and boost the digital economy. GDPR brings benefits to business in the form of improved consistency, relaxed notification requirements and clearer guidance on certain aspects of data protection. It also brings certain challenges, however, and the potential for significantly increased monetary penalties in cases of non-compliance.

Certain aspects of GDPR - including, unsurprisingly, the scale of potential penalties - have been subject to much discussion in the academic literature and general media. Others have been overlooked or at least partially misunderstood. Examples of the latter include questions relating to the Regulation's applicability to smaller organisations and how it will affect UK business after the country's withdrawal from the European Union. It is also fair to say that there has been a certain amount of 'scare-mongering' and, in some cases, the Regulation has been presented as being more onerous than it may prove to be. GDPR does bring new challenges to organisations, however, and some are not fully aware or prepared for its introduction. Even for those that are aware, questions remain: exactly what has changed, what does it mean for business, and how can organisations prepare?

Providing answers to these questions is the purpose of this report. It sets out to examine how GDPR differs from previous and current data protection laws and provides a synthesis of the key practical challenges for organisations handling personal data. In critically comparing GDPR with its predecessors, we discover that the underlying principles have remained largely intact since at least the 1970s. While these have been updated to consider new technologies and working practices, the measures to be taken are broadly consistent with the current regime. Only in certain areas does GDPR present markedly new challenges. These include changes to the rules surrounding consent, security of processing, accountability and data subject rights. Even where new challenges do exist, we identify that they are evolutionary and organisations already compliant with existing laws are well placed to deal with and, indeed, benefit from them. In a world where stories concerning cyber-attacks and personal data breaches are becoming common features in the mainstream media, providing good data protection could act as a powerful market differentiator in attracting consumers increasingly aware of the risks.

At its heart, GDPR is about good information governance: knowing what data is held, from whom and for what purpose it was obtained, where it is located and how it is protected. This report argues that, in this regard, GDPR-compliance and, indeed, data protection more generally, shares a great deal in common with the information security function. The two have complementary requirements and measures taken to meet obligations under GDPR have the potential to improve efficiency and the security of business data more generally. The Regulation thus provides an opportunity to drive convergence between data protection and security to benefit organisations while at the same time protecting individual rights.