Platinum SQUARED

GDPR — Business as Usual?

How much of impact will GDPR have on businesses

Introduction
In the last few months, there has been a large amount of publicity surrounding the European Union General Data Protection Regulation (GDPR) and the UK's proposed implementation of GDPR via the Data Protection Bill (both referred to as 'the regulations' for the purposes of this article).

While there are obvious changes to existing Data Protection Law and increased penalties for failing to adhere to the regulations, this article argues that for those organisations who currently comply with existing Data Protection legislation, who have robust security controls in place and who take information management seriously, the new regulations should not be onerous to implement and in many instances are business as usual.

Although not intended as a comprehensive review of all of the requirements of the regulations, it hopefully highlights some of the key requirements and how organisations should already be compliant, with one or two exceptions or with only minor amendments to existing policies and processes.

Background
The GDPR will come into force on the 25th May 2018; the UK Government announced the Data Protection Bill in the Queen's Speech on 21st June 2017 which is currently being scrutinised by Parliament. This legislation is how the UK will implement a revised Data Protection Act to apply the GDPR's standards in preparation for the UK's exit from the European Union.

Useful documentation has already been produced by the Information Commissioner's Office (ICO) and independent consultancies have increased their service offerings to help organisations understand the requirements of the new regulations and to implement controls to move organisations into a state of compliance. However, are the changes required as onerous as some may fear?

The existing eight Data Protection Principles as enshrined in the 1998 Data Protection Act (DPA) are now documented as six data protection principles along with the additional rights of the data subject:

1. Processing must be lawful, fair and transparent;
2. The purposes of processing must be specified, explicit and legitimate;
3. Personal data must be adequate, relevant and not excessive;
4. Personal data must be accurate and kept up to date;
5. Personal data must be kept no longer than necessary;
6. Personal data must be processed in a secure manner.

The rights of the data subject have been enhanced and also include a new right of data portability and now cover:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;

- The right to object; and
- The right not to be subject to automated decision making including profiling.

The international transfer of personal data is still retained under the regulations and, similar to the DPA, requires that any data you transfer outside of the European Union is subject to adequate safeguards and data security in place, that it is documented in a written contract and that audits are conducted to measure the documented security arrangements. For those compliant with the existing DPA and who already actively manage security and the associated governance requirements this should be business as usual.

Understanding Data Flows
The regulations require organisations to understand and document what personal data they hold, where it came from, who it is shared with and what they do with it. These requirements were implicit under the DPA and should be familiar to those organisations who have in place robust security controls. After all, how can an organisation protect its data if it does not know where it is or where it goes?

Data Protection by Design
The regulations make data protection by design an express legal requirement. However, this has always been good practice and those organisations who take security seriously should already have this embedded as part of business as usual. Those organisations who meet the requirements of ISO 27001 will already have controls in place to meet the requirements documented under the requirements for 'Security in development and support processes'. It should also be noted that the controls implemented must be based on an understanding of the risks that the organisation faces. Again, for those organisations who already comply with standards such as ISO 27001, this adoption of a risk managed approach to security will be business as usual.

Reporting Incidents
The regulations introduce a duty on all organisations to report certain types of data breach to the ICO. In cases where the data loss could result in a 'high risk to the rights and freedoms' of the individual, the loss has to be reported to the data subject as well. The regulations require that organisations report notifiable incidents to the ICO within 72 hours of the breach occurring. For those organisations who comply with ISO 27001, the requirements to have in place robust incident management and reporting processes will be nothing new as they are captured under the control requirements for information security incident management. There may be a requirement to review polices and processes to ensure that the 72 hour reporting requirement is enforceable, but the fundamental process of incident reporting and management should already be embedded.

Seeking consent
The requirements to seek consent to processing already exist in the current DPA and while there is more rigour around implicit consent, organisations already compliant with the DPA should not find compliance with this requirement onerous.

There are new requirements to be transparent about the processing you undertake and to implement privacy notices to keep the public informed as to the reasons you process personal information and how you comply with the regulation.

Notwithstanding the penalties for processing an individual's information who has not provided consent, for most organisations it makes clear business sense to make sure consent has been obtained. If you have a mailing list of potential clients what is the point of contacting people who have expressed no interest in your services? At best, you are wasting your time and resources in marketing to someone who is not interested.

One fundamental change is the additional requirements for dealing with children. Under the DP Bill the age for which parental consent is not required to process data online will be 13, and 16 for those that must comply with the GDPR.

The guidance from the ICO is that organisations should 'start thinking about whether you need to put systems in place to verify individual's ages and to obtain parental or guardian consent for any data processing activity.' This requirement is primarily focused on those organisations offering social networking services and if taking forward the risk-based approach to security, a large number of organisations could argue that it is highly unlikely that a child would want to engage with them. How many people under the age of 13 are likely to register with you as a supplier? The controls in place to verify an individual's age for these organisations could be as basic as a check box to confirm that the data subject is over 13 (or 16).

Data Portability
The right to data portability is new, however it only applies:

- To personal data an individual has provided to a controller;
- Where the processing is based on the individual's consent or for the performance of a contract;
- When the processing is carried out by automated means.

While this is a new requirement, it is obvious that a lot of organisations such as banks and utility companies have already addressed this issue. Although this requirement now applies to all organisations, in reality how many organisations who are not providing banking or utilities will be called upon to transfer client data to a new supplier on a regular basis?

Right to be Forgotten
Much has been written about the requirement of the 'right to be forgotten' but the regulations are really just clarifying and enhancing what already existed under the DPA as the data subject's rights in relation to the 'rectification, blocking, erasure and destruction of personal data'.

While the new regulations expand upon the requirement for erasure and destruction, they should not be onerous to implement and it would make good business sense to remove data of someone who is not a client or who does not want to receive details of your organisation's services. Why would you want to take responsibility and face costs relating to holding data relating to someone who is no longer a client or who is no longer relevant to you unless there are legal or regulatory reasons that apply?

Definition of Responsibilities
The regulations and guidance from the ICO states that 'you should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. For some organisations such as Public Authorities or those organisation that process large volumes of personal data, there is an explicit requirement to formally designate a Data Protection Officer.

There are also clear requirements to define and document the responsibilities for both Data Controllers and Data Processors with a requirement that controllers and processors have in place written contracts that ensure that the processing carried out by the processor meets all of the requirements of the regulations (not just those related to keeping personal data secure). For those organisations that align to ISO 27001 these requirements should already be in force. ISO 27001 already requires you to have clear governance structures in place and specific control requirements for management direction of information security.

Conclusion
The penalties for non-compliance under the regulations can be frighteningly high, the Data Protection Bill is proposing a maximum fine of £18 million (up from £500,000). There will be requirements to update policies and processes to meet some of the requirements of the regulations. However, most of the changes required should not be onerous if an organisation is already compliant with existing DP legislation and has already adopted a robust security stance aligned to a standard such as ISO 27001 with the controls implemented applicable to the risks the organisation faces. It should also be noted that the changes required by the regulations make sound business sense.

If your organisation does have a sound information security management system in place, GDPR offers an excellent opportunity to convince senior management of the benefits of investing in improving their security stance to meet data protection requirements and other information security requirements within the business.

About the Author

Michael Stimson has worked in the Information Assurance industry for over 20 years. He is a highly motivated and enthusiastic manager and consultant with excellent communication and problem-solving skills, a proactive team leader and member with ability to work using own initiative. Michael has demonstrated his dedication to learning new skills through the completion of a number of external and internal training courses including ISO 27001 Lead Auditor which has provided him with the breadth of knowledge required to successfully tackle new challenges.

He is HMG security vetted and was a member of the CESG Listed Advisor Scheme (CLAS) when that scheme operated. He has strong skills in Risk Analysis, IA Policy & Procedure, Data Privacy, GDPR compliance, Legal & Regulatory Compliance, project management and business development. Further specialisms include ISO 27001 (Certification & Compliance), Risk Management and Accreditation Document Sets (RMADS) and IA Governance.