SR Consulting
Insight - Solutions - Support

decisive:it
supporting your success

GDPR
FOR
SME BUSINESSES

A White Paper

FEBRUARY 1, 2018

SR CONSULTING
Sivatech Building, Gatehouse Close, Aylesbury, Buckinghamshire HP19 8DJ

SR Consulting
Insight - Solutions - Support

1.0 Introduction

1.1 On 25th May this year the new General Data Protection Regulation (GDPR) will come into force. GDPR will affect businesses and organisations across the country. It will update the 1998 Data Protection Act, which was developed before the advent of social media, algorithms, cloud based IT systems etc., and puts the rights of data subjects – that's you and me as individuals – at the very heart of the Regulation.

1.2 The purpose of this paper is to set out the key features of GDPR so that you can start (or continue) thinking about how to implement the GDPR requirements in the context of your business. Every business and organisation are different not least in how they rely on data processing to be successful and how their existing policies and procedures are meeting the refreshed requirements. There is no one size fits all or downloadable formulaic answer to GDPR. All businesses and organisations will need their own tailored approach.

1.3 My name is Jonathan Lane and I am a Director with SR Consulting, a business that specialises in helping SMEs and similar sized organisations come up with solutions to meet operational and strategic issues they face. GDPR is one such issue. Our clients have asked us to help them become GDPR compliant on time. We have been working on such projects for the last two years. There is within the business a wealth of experience in successfully running organisations that processed significant amounts of sensitive personal data on a routine and regular basis.

2.0 GDPR and your business

2.1 Our supervisory organisation the Information Commissioner's Office (ICO) has the unenviable task of providing guidance on the application of GDPR to all the businesses and organisations it affects. While the vast majority of its guidance is helpful it does suffer from a lack of precision not least because it must be equally applicable to multinationals and micro-businesses at the same time.

2.2 The ICO guidance must, therefore, be applied by you in the context of your business or organisation. But how can you do that in an effective way? Well we think that there is a simple starting point that involves the following three "P's":

2.2.1 The **Six Principles**, which underpin GDPR. They are set out in Article 5(1) of the Regulation, and they are summarised as follows.:

a) Lawfulness, fairness and transparency;
b) Purpose limitation;
c) Data minimisation;
d) Accuracy;
e) Storage minimisation; and
f) Integrity and confidentiality.

Any policies and procedures that you develop for your business in response to GDPR will need to be mappable on to these six Principles and all will need to be covered in some suitable way. But in doing so:

2.2.2 You will want to recognise the scale and extent of the risks that your business faces so your response will need to be **Proportionate**. GDPR compliance, in our view, does not mean the introduction of a myriad of policies and procedures but rather a suitable and measured approach; and

2.2.3 You will need to do this in a way that is appropriate to the way your business or organisation is run, that is in a **Pragmatic** manner.

2.3 Article 5(2) requires you to be able to demonstrate compliance by your business with all six Principles, so 2.2.1 is a useful starting point in checking your response to GDPR.

2.4 Principle (a) above requires you to undertake the processing of personal data only when you have a lawful reason to do so, and these are set out in Article 6. In summary, they are:

2.4.1 Consent by the data subject;
2.4.2 Necessary for the development or delivery of a contract with the data subject;
2.4.3 Necessary for compliance by your business or organisation with a legal obligation;
2.4.4 Necessary to protect the vital interests of the data subject;
2.4.5 Necessary for a task carried out in the public interest; and
2.4.6 Necessary for the legitimate interests of the business unless that interest is overridden by any risks facing the data subject especially is that data subject is a child.

What is important to appreciate here is that the legal basis under which your business processes personal data can vary throughout the time it holds that data; for example, you might start processing using consent, but you might retain personal data in the longer term, possibly in a reduced form, if you need to comply with a legal obligation.

2.5 GDPR also identifies several categories of personal data that require particular attention: these include Article 8 regarding the provision of on line services to children; Article 9, which defines a number of special categories of personal data, such as racial and ethnic origin, political opinion, for example; and Article 10, which looks at issues around criminal convictions and offences. If your business regularly processes personal data of this nature then you will need to pay especial attention to this aspect of complying with GDPR.

2.6 Right at the start of this paper (section 1.1) the emphasis of GDPR on the rights of data subjects was highlighted. After May 2018 data subjects will be entitled to the following rights:

2.6.1 A right of access to the personal data your business may hold on them (Article 15);
2.6.2 A right to the rectification of any inaccurate personal data held on them by your business (Article 16);
2.6.3 A right to be forgotten by the erasure of any personal data that your business may hold on them, subject to some caveats (Article 17);
2.6.4 A right to have the processing of their personal data by your business restricted when certain conditions are satisfied (Article 18);
2.6.5 A right to have the personal data held by your business transferred to another data controller – an example of this already in place is switching banks (Article 20); and

2.6.6 A right to object to the processing of their personal data (Article 21) and to be the subject of automated decision making processes (Article 22). Both are subject to a number of conditions.

2.7 If your business collects and processes personal data then under GDPR you are a Data Controller: if your business processes personal data on behalf of another business – for example payroll – then you are a Data Processor: your business can have both roles. GDPR places a significant number of obligations on both entities; these obligations are set out throughout the Regulation, but some of the key ones are, for example:

2.7.1 Providing the data subject with information about the personal data you are collecting about them (Article 13);
2.7.2 Ensuring that your business can respond effectively should a data subject wish to exercise on of their rights as set out above;
2.7.3 Meeting your overarching obligation to be able to demonstrate that your business's processing of personal data are being carried out in accordance with the Regulation (Articles 24 and 28); and
2.7.4 Keeping a record of the processing activities carried out by your business subject to the caveated exemption for SMEs (Article 30).

2.8 It is not surprising that the security of personal data features large within the Regulation. The opening section of Article 32(1) states, for example:

"*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate*: ….."

As a business you will need to assess how you stack up against this balanced requirement in both your IT, people and premises policies, and what changes if any you will need to make. As someone who has run an organisation that processed a significant amount of personal data my experience is that getting the people side right is critical, not least so they can work effectively within any IT and premise policies you might need to implement before May 2018.

2.9 Articles 33 and 34 of the Regulation explain the revised approach to reporting and handling a personal data breach. The new reporting requirement is 72 hours of having become aware of the breach. If your business already has a contingency plan in place then it would be sensible to think how you might include within that plan the new breach requirements.

3.0 What you might want to do next

3.1 While remembering the three P's at section 2.2 above here are some steps that you might want to take when thinking about how your business might ready itself for GDPR compliance by May 2018:

3.1.1 Ensure that your senior management team, business owner or key leaders recognise the importance to your business of complying with the Regulation and that they are prepared to back any required changes, including finding any necessary resources;

3.1.2 Map out in some sensible way your current processing of personal data activities so that you are clear on the scale of the issues and risks for the business;

3.1.3 Determine just how far away from compliance with the Regulation your business might be – you may be surprised that you are closer than you think once you have done the analysis;

3.1.4 Decide how your business will best meet its obligations in terms of data subject rights – do you simply need to tweak your current approach or is something more substantive required;

3.1.5 Consider how your current approach to security in terms of IT, people and premises policies could meet the requirements of the Regulation; and

3.1.6 Put together and implement a costed plan of how your business will put in place the proportionate changes you have identified in a way that suits your business.

3.2 We hope that this paper has given you and your business a valuable insight into the new regulation and how you might respond to it. If it would be helpful, then we would be more than happy to discuss the issues it raises with you in more detail. As a business we have develop a range of tools to help our existing clients see how they can move to ensure compliance on time. We can be contacted at:

admin@sr-consult.co.uk
01296 340404

SR Consulting
1st February 2018