Experts in Business

Data Protection Team
Department for Culture, Media & Sport

10th May 2017

Dear Sir or Madam,

CALL FOR VIEWS ON THE GENERAL DATA PROTECTION REGULATION: DEROGATIONS

The Federation of Small Businesses (FSB) welcomes this opportunity to submit comments to the call for views on the implementation of the General Data Protection Regulation (GDPR). FSB is the UK's leading business organisation. It exists to protect and promote the interests of the self-employed and all those who run their own business. FSB is non-party political and is also the largest organisation representing small and medium sized businesses in the UK.

Small businesses make up 99.3 per cent of all businesses in the UK, and make a huge contribution to the UK economy. They contribute 51 per cent of the GDP and employ 58 per cent of the private sector workforce.

Small business and the GDPR

The GDPR is due to be implemented in the UK by the summer of 2018. Data protection ranks consistently high among the regulatory burdens impacting smaller businesses.[1] The GDPR is a significant step-up in the scope and complexity of data protection obligations. As such the result will be that data protection becomes a greater burden on smaller businesses than currently. The consequences will be the competitiveness of smaller firms will be negatively impacted with resources diverted away from business development activities and towards compliance.

FSB and BBA research suggested that those businesses subject to the full range of obligations under the GDPR e.g. those undertaking 'high risk' or large data processing activities, could face additional costs of up to £75,000 a year.[2] The 2012 Impact Assessment of the GDPR proposals conducted by the Ministry of Justice (MoJ) suggested that the yearly costs to business of the GDPR will not just be transitional but increase over time.[3] In 2018-

[1] RBD/ FSB. 'Voice of Small Business: Panel Survey'. (2013).
[2] FSB/ BBA. 'Data protection rules could cost small firms over £75,000 each year, says FSB and BBA'. (2013). Available at: https://www.fsb.org.uk/media-centre/press-releases/data-protection-rules-could-cost-small-firms-over-75-000-each-year-says-fsb-and-bba-pr-2013-60
[3] Calculations made using 2012 prices.

19 (first year of implementation) they are estimated to be £260 million. By 2025-26 the annual costs are estimated to be greater at £310 million. Some of the costs borne by smaller businesses will be a result of the fundamental design of the GDPR. The creation of new concepts such as 'pseudonymised data', 'large scale processing', 'risky' and 'high risk to individuals' create significant uncertainties, which will remain sources of considerable costs until these elements of the basic design of the GDPR are reduced. Other design related causes of the additional costs that will be incurred by smaller businesses as a result of the GDPR include: joint liability for data breaches between controllers and the processors, a reverse burden of proof, the new fining regime and the scope for follow-on actions, the new bar for lawful processing including the high 'consent' thresholds, the data breach notification rules, 'right to be forgotten', the appointment of Data Protection Officers (DPO), extensive data record keeping and Impact Assessment requirements and the greater number of types of data and thus the quantity of data to which the new rules will apply.

The scope of the GDPR, as outlined above, requires a collaborative approach from Government and the regulator to ensure concepts and definitions are clearly explained and all possible support is provided to small businesses to assist them to understand and adhere to the requirements of the GDPR.

In addition to the direct regulatory costs on smaller firms, the wider impacts of the GDPR on the digital economy also need to be considered. These include a long-term 'chilling' effect on the UK's dynamic digital and other new technology sectors as a result in the increase in the cost of the key factor of production in such industries: data. The specific wider impacts will include:

- Higher barriers to entry and growth for smaller data using firms who will find it more expensive to start-up and operate.
- Inhibitions on data based innovation by both incumbent businesses and new entrants which otherwise would have taken place or could have been done more easily and cheaply.

There is a further longer-term problem with the design of the GDPR. The tendency to be technology specific in parts of the regulation is a flaw. In the long-term, as technology evolves, parts of it will become out-of-date. The uncertainty that will result from the inapplicability of parts of the data protection framework will increase legal and other risks associated with smaller businesses using data.

Implementing the GDPR

As a result of the significant detriment likely to be incurred because of the GDPR, FSB considers that the GDPR has to be implemented as sensitively as possible, taking every

Source: MoJ. 'Proposal for an EU Data Protection Regulation'. (2012). Available at: https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf

fsb
Experts in Business

opportunity to minimise burdens and thus costs and the knock-on consequences for business growth. This requires:

- Utilising the scope for national derogations intelligently so as to apply the GDPR in as risk-based way as possible, when it commences.
- The Information Commissioners Office (ICO) taking a reasonable approach to monitoring and enforcement and crucially, complementing a proportionate enforcement role with an adequately funded strategic effort to support small businesses with compliance rather than punitive sanctioning. This will require a significant step-up in the quality and clarity of information and guidance offered to smaller businesses by regulators.

The derogations in the GDPR leave some room for Member States to adapt aspects of the law to domestic circumstances. In other areas the GDPR relies on there to be domestic law in order to operate properly. To this end, the exemptions for smaller businesses obtained by FSB, working with others, during the GDPR's progress through the EU legislative process need to be maintained by the UK Government. These include the exemptions from the requirements to appoint DPOs, maintaining processing data records and minor data breaches. In addition, FSB would like to see the Government make sure that:

- Advantage is taken of the freedom given in the GDPR for using personal where this is to help civil judicial proceedings.
- Reasonable co-operation and data-sharing between regulators is not impeded. The GDPR must not be allowed to prevent measures which improve the 'regulatory experience' of smaller businesses by preventing or making it more difficult for regulators to share data about businesses to reduce the burden of implementing regulations.

Further, the Government should avoid placing any additional restrictions on international transfers and add burdens onto smaller businesses handling employee data. Full advantage of the scope for ensuring data can be used flexibly for research should be taken. For example, high-growth life science businesses require a high degree of freedom in data use for the development of new medicines and other treatments. Finally, the Government needs to take a narrow interpretation of the circumstances in which the 'right to be forgotten' applies. This is a very burdensome principle and the scale of that burden needs to be minimised wherever possible.

It has been suggested in some quarters that a 'privacy seal' may be developed, utilising the provisions in Article 42. The development of such a 'seal' needs to take into account the needs of smaller businesses i.e. affordability, practicality and any administrative burden associated with it. A balance will need to be struck between ensuring consistent standards and application, reducing the risk of more 'blue tape' for smaller businesses while encouraging a range of providers to help minimise the price of obtaining a 'seal'.[4]

[4] 'Blue tape' is a term describing additional restrictions and requirements that burden smaller businesses which are not legal/ regulatory requirements. 'Blue tape' comes from a number of sources: non-statutory accreditation/ certification requirements e.g. in order to bid for supply contracts; insurance requirements that go beyond legal obligations and the implementation of

As has been illustrated briefly above, the consequences of the GDPR could be far reaching for smaller businesses and the wider digital economy. The timetable for implementation means that the new rules will commence before the UK leaves the EU. The latter offers opportunities for reform, which will be addressed in future FSB reports on small business regulation post-EU membership. In the short to medium-term FSB, as the leading representative body of smaller firms in the UK, intends to work constructively with Government and the ICO on the implementation of the GDPR. Getting it right is vital for smaller businesses in order to minimise the potentially significant amount of long-term disruption to business models, innovation (including the commercialisation of innovations) and growth that is likely to follow from the GDPR.

If you have any further questions regarding our views on this issue please do not hesitate to contact my colleague on the following number:

Yours sincerely

higher than required compliance standards and practices that small businesses implement as a result of external compliance advice.