



balanceofcompetences@justice.gsi.gov.uk

1 July 2014

Dear Sir/Madam

**FSB response to:
Public Consultation on Information Rights**

Please find below the response of the Federation of Small Businesses (FSB) to the Balance of Competences Review: Information Rights.

The 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. The FSB is non-party-political and, with around 200,000 members, it is also the largest organisation representing small and medium-sized businesses in the UK.

Small businesses make up 99 per cent of all businesses in the UK, and make a huge contribution to the UK economy. They contribute up to 50 per cent of GDP and employ over 59 per cent of the private-sector workforce.

The FSB has a diverse membership across a range of sectors, and there are a range of views about the pros and cons of our relationship with the EU. However, the European market remains the main destination for our exporting members. Our research shows that they are also starting to look to countries outside the EU. The EU trade agreements with third countries to open up markets further afield are therefore of major importance to them. However, for most members Europe is close to home and easier to access than emerging economies. Furthermore, inward investment enables businesses in the supply chain to benefit from companies from outside the EU that base themselves in the UK to deliver to the European market.

There are more than four million people in the UK that are either self-employed or run their own business. Although the single European market gives them access to more than 500 million customers and 20 million businesses, the burden of EU regulation falls too heavily on the smallest firms. The Government and the EU must do everything they can to further free up barriers to trade, ensuring small businesses have the best support and environment in which they can create growth and jobs. This requires strict adherence to smart regulation principles to create legislation that is proportionate, evidence-based and suitable for all sizes of businesses.

Data protection rules affect all small firms and the FSB has been making the case to make the new rules small-business friendly and has called on politicians to 'Think Small First' when discussing updates to the data protection framework.

We trust that you will find our comments helpful and that they will be taken into consideration.

Yours faithfully

Clive Davenport
Chairman for Trade, Enterprise and Innovation
Federation of Small Businesses



Federation of Small Businesses
The UK's Leading Business Organisation



FSB response to the Government Balance of Competences Review: consultation on Information Rights

July 2014



Introduction

Small businesses are the lifeblood of the European economy, providing around two-thirds of private sector employment. SMEs make up 99 per cent of all businesses in the EU, of which 92 per cent are micro enterprises. The average headcount of an FSB member's business is eleven members of staff.¹ Around one fifth of FSB members export and the European market is their main destination (85 per cent trade within the EEA).² Just over half of our exporting members export goods, mostly to the EEA, while over one third export services.³

The internal market offers easy access for first-time exporters with a market of over 500 million customers and over 20 million businesses on their doorstep. The internal market creates legal certainty and attempts to level the playing field through competition rules and harmonised rules. This means that businesses can save considerable cost when selling to EU countries. In theory, 28 sets of domestic regulation are merged into one.

The FSB supports the continuous development of the internal market and the liberalisation of trade, including digital entrepreneurship. However, the FSB insists its rules are developed and screened according to the highest standard of smart regulation principles. Small and micro-businesses have more difficulty complying with regulation than big businesses and suffer from the cumulative effect of legislation. Almost a third (27 per cent) of FSB members find more regulation and enforcement (EU and UK legislation) a barrier to success.⁴ One particular law may not appear so burdensome, but it is the accumulation of burdens that discourages a business from taking on staff or venturing into new markets. Therefore, we believe quality legislation, implemented to the same standard by all the member states, is essential for the common market to thrive and grow.

This response focuses on questions relating to the new data protection framework (q1-4). Data protection rules affect all small firms and we will discuss this shared competence by taking together questions 1 and 3. Furthermore, the FSB considers that an adequate data protection policy is part of good business practice for small firms. However, a balance needs to be struck between the burdens on businesses and individuals' rights. We will elaborate on this point taking together questions 2 and 4.

¹ FSB 'Voice of Small Business' Member Survey, March 2014.

² Id.

³ Id.

⁴ Id.



Questions

1. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) has been advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

3. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) is meeting the challenges posed by the increasing international flow of data, technological developments, and the growth of online commerce and social networks?

For a small business, whether data protection is an issue that needs to be dealt with at EU level or not depends on its activities and trading partners. For example, for a cross-border cloud computing provider, ecommerce business, businesses in the services or data-driven industries, it would make sense to have one common set of data protection rules. However, if the newly proposed harmonisation of rules gets through, there would no longer be any discretion or flexibility possible on the part of the UK Government. This in turn may disadvantage some businesses. For example, in the new rules it is proposed that the Subject Access Request fee may no longer be applied in the UK. If that really happens, it will increase costs for small firms to comply with the data protection rules (see answer to questions 2 and 4). Also, there will be no room for discretion within the new rules when it comes to imposing a fine on small businesses for data breaches, as opposed to imposing a fine on bigger businesses.

The FSB represents many different businesses in all sectors. It believes common rules are helping small firms to trade in the EU. However, lack of local flexibility of the rules would disadvantage many businesses within its membership. Local circumstances should not be forgotten. We therefore support common rules for the Single Market that, where possible, would allow for local variation. The FSB acknowledges that this is very difficult, but calls on the Government to find areas where local interpretation of the rules is not hampering free trade across borders. At the same time, the Government should advocate common rules where it would help businesses find new markets. In particular in the Digital Single Market, where data should freely flow across borders.



2. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) strikes the right balance between individuals' data protection rights and the pursuit of economic growth?

4. What evidence is there that proposals for a new EU Data Protection Regulation will be advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

As explained above, the new rules can bring advantages to small firms. This is mainly because it will create more harmonisation of the data protection regimes in the EU member states. Cloud computing providers, data driven businesses and ecommerce businesses can benefit from more harmonised laws. See answer to question 1 and 3 for a discussion about harmonisation versus the need for local flexibility.

However, the regulation as proposed will introduce additional, and in some cases, unnecessary costs and burdens on small businesses. The FSB accepts that updating of existing legislation is necessary to allow for technological advances, although we question whether the EU proposals achieve this. We are concerned that small businesses will find the new rules overly prescriptive and bureaucratic.

The following issues that are under negotiation in the new EU data protection rules could be costly and disproportionately burdensome for small firms:

- **Abolishing the Subject Access Request Fee**

Under the new rules, employees or clients have the right to be given their personal information free of charge. In countries that have an access fee, token payments have deterred malicious, excessive or frivolous requests. A small fee for every request is a sensible and moderate way of ensuring requests are genuine. It saves businesses hours of work, in particular small firms. The costs for a business of responding to an Access Request are estimated to be in between £50-100.⁵ Research has shown that abolishing the fee increases the number of access requests, and thus the burden on small businesses.⁶ A fee of £10 currently acts as a deterrent against malicious or frivolous requests.

- **Extended rights of access**

Currently, a business has to inform a client or an employee about the purpose, the different categories and the recipients of their processed data. In the new rules a business also has to indicate the *period* for which the personal data will be stored, and in case it is used for profiling, the *significance* and *consequences* of the use of personal data.

- **Extended 'Right to be forgotten'**

If the client/employee withdraws their consent, or when the storage period expires, a business has to destroy their personal data. It also has to inform third parties that were allowed publication of the clients' personal data. However, under the new rules the business remains responsible for that publication by third parties.

- **Wider definition of personal data**

Any information relating to a client or employee, for example their IP address, counts as personal data. In case of an access request a business would have to search all its databases and all its digital communication, and separate out those pieces of information on one individual.

- **Employing/training/appointing a Data Protection Officer**

⁵ UK Government Impact Assessment on the Proposal for an EU Data Protection Regulation, MoJ, 22 November 2012.

⁶ Id.



As the new rules now stand in the negotiation, it is unclear which businesses would need to employ a Data Protection Officer. We fear that more businesses would be covered by this obligation than necessary. The Commission has proposed an exemption for non-data driven small businesses; the Parliament deleted this and introduced a certain number of data subjects as a threshold. The FSB is not in favour of any threshold as this would be arbitrary. Instead, it would like to see a risk-based approach. Employing a Data Protection Officer on a voluntary basis could be advocated as part of good business practice, for example for businesses that use data as their core business. However, most small businesses hold email addresses for information purposes. These data are kept in house and not used for any other purposes. A Data Protection officer would be entirely unnecessary, not to mention disproportionately burdensome. The cost of employing a Data Protection Officer is estimated to be around £60,000.⁷ This is quite high as DPOs are fully trained legal professionals. The turn-over of the average start-up simply does not allow for this kind of expenditure. This is a typical example of where the compliance burden outweighs regulatory necessity.

- **Carrying out a Data Protection Impact Assessment**

The reasoning above also applies to the obligation to carry out a Data Protection Impact Assessment. We would like to see a risk-based approach and a voluntary arrangement. Where a business is clearly not data-driven/only uses data for emailing purposes, a costly impact assessment should be avoided.

The cost of carrying out a Data Protection Impact Assessment is estimated by the Commission to be around £12,000.⁸

- **New documentation requirements**

A business has to keep track of how they handle personal data. It is currently unclear which businesses would be covered by the new rules. Again, we would like to see a risk-based approach and voluntary arrangements that are part of good business practice.

- **Fines**

Instead of fixed amounts of up to £500,000, breaches of the legislation will attract a fine from 0.5% of turn-over to 2%, with one single occasion of non-intentional non-compliance before a business is fined. The FSB agrees with fines for serious breaches of the data protection rules. However, the rules under negotiation are rather prescriptive and non-intentional non-compliance happens easily. Therefore, the FSB would like to see *two* occasions of non-intentional non-compliance for small firms before fines kick in (the 'three strikes' approach).

- **Giving Consent** needs to be 'explicit'

Under the current rules, the client needs to give their consent to process personal data in an 'unambiguous' way. However, the new rules ask for an active statement or clear affirmative action. This means small firms could face costs for changing their websites and IT systems to reflect this. Instead of asking once, they would need to ask for consent in every step of the process. Under the current rules, consent is implicitly understood once it is given at the beginning.

For further information

sietske.degroot@fsb.org.uk

Federation of Small Businesses, 2 Catherine Place, London SW1E 6HF

⁷ Commission Impact Assessment accompanying the proposals for a Regulation and for a Directive. SEC (2012) 72, p. 110.
http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.

⁸ Commission Impact Assessment accompanying the proposals for a Regulation and for a Directive. SEC (2012) 72, p. 70.
http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.