



Department
for Business
Innovation & Skills

Better
Regulation
Delivery Office

**Data Sharing for Non-Economic
Regulators
Government Response**

March 2015

Executive summary

Government is committed to facilitating effective regulation that protects the public whilst encouraging compliant businesses to grow. In order to regulate effectively, it makes sense that regulators should be able to share data about the businesses they regulate, in a proportionate manner.

BRDO has conducted a project to examine data sharing amongst non-economic regulators and explore the potential benefits of data sharing, from the perspectives of regulators and business. This document sets out the results of the project, including the results of public consultation, a research project and pilot, and explains Government's intended next steps.

The Regulators' Code ('the Code') sets out a framework for how non-economic regulators should interact with the businesses they regulate. The Code provides that regulators should target their activities according to risk, and should share information about risk, where legally possible. Government is keen to ensure that regulators are able to comply with these provisions to the fullest extent possible in order to maximise benefits for both regulators and business.

The consultation opened on 28 April 2014 and closed on 7 July 2014. Over 50 responses were received from business, trade associations, professional bodies and national and local regulators (see Annex A). Five workshops were held in Birmingham, London and Cardiff for regulators and businesses. In addition to the workshops, BRDO held a number of individual discussions with businesses, trade associations and regulators. Stakeholder input from these events has contributed to the Government's response to the consultation.

The findings of the project indicate that significant benefits can result from regulatory data sharing, both in terms of enabling regulators to fulfil their statutory functions more efficiently and effectively, and in reducing burden and delivering earned recognition for compliant businesses.

Some non-economic regulators are already sharing data. However, the results of the project indicate that the full benefits of data sharing are not yet being completely realised. Some regulators would like to be doing more in terms of sharing data but feel unable to do so, for a variety of reasons. These include a lack of knowledge and/or resources to begin sharing data and confusion as to the circumstances in which it is legal to share data. A small number of regulators cited specific statutory barriers preventing them from sharing data. A significant portion of respondents cited confusion about the Data Protection Act 1998 ('the DPA') as a barrier to data sharing, with some noting there is genuine misunderstanding as to what can be shared under the DPA and others noting that the DPA is often cited as a reason not to share data, when this may in fact not be the case.

The consultation posed three options: a measure in primary legislation, embedding data sharing as best practice, and a single point of registration. Respondents' views as to options to encourage further data sharing were diverse. Views on a measure in primary legislation were equally split between those for and those against, and of those in favour of such a measure, opinions differed as to what such a measure should look like. Views on the potential for a single point of registration were equally mixed, with some respondents against the idea on the basis that it may create more burden for business and regulators. Others noted that whilst a single point of registration may be desirable, its implementation could prove impractical. Embedding data sharing as best practice was the option favoured by both business and regulator respondents.

Data Sharing for Non-Economic Regulators

This document sets out Government's intended course of action to better equip non-economic regulators to share data with a view to targeting activity more effectively and reducing burden for business. Government intends to assist regulators to better understand the DPA, and to this end BRDO will work with the Information Commissioner's Office to produce guidance and other tools specifically for regulators. BRDO will also consider developing practical tools to assist regulators to begin (or expand) data sharing activity with minimal resources. Further consideration is to be given to the evaluation of the IRIS pilot in the context of informing the development of systems that will assist regulators in sharing data and information.

Contents

Executive summary	2
1. Introduction	5
2. Exploring data types and barriers to sharing data	6
3. Scoping the options	24
4. The Intelligent Regulatory Information System pilot, research project and Better Business Compliance partnerships	30
5. Next steps	33
Annex A: Respondents to the consultation	34
Annex B: Regulators in scope of the Regulators' Code	36

1. Introduction

- 1.1 Regulators need to collect information from and about the businesses they regulate in order to fulfil their statutory obligations. It makes sense that regulators should be able to share this information. Using information effectively, and sharing it appropriately, can assist regulators to focus their activities according to risk, and in turn to regulate more effectively and efficiently. In turn, regulatory burden on business can be minimised and compliant businesses can be rewarded for their efforts, for example, by way of fewer and/or short inspections and fewer requests for information. The Regulators' Code ('the Code') reflects this by providing that regulators should base their activities on risk (Part 3) and should share information about compliance and risk, where legally possible (Part 4). This document uses the term 'data' to refer to the information used by regulators to fulfil their statutory obligations.
- 1.2 BRDO has examined data sharing amongst non-economic regulators during 2014, via a public consultation, research project and a pilot of the Intelligent Regulatory Information System (IRIS). Each of these elements has produced results to inform policy development. This response document encompasses the results of all three elements and proposes a course of action to assist non-economic regulators to share data in order to realise benefits for regulators and business, as well as to meet the provisions of the Code.
- 1.3 The IRIS pilot involved local authority regulators and the Fire and Rescue Service in Leicestershire testing the concept of data sharing under controlled conditions, using an extended version of the 'Find It' software tool developed by the Health and Safety Laboratory (HSL). This tool was originally developed for use by the Health and Safety Executive (HSE) and was adapted for use by four Leicestershire regulators. The pilot ran for six months and its purpose was twofold: to test the extended version of the software tool and to test the concept of data sharing, including an evaluation of benefits, under controlled conditions. An evaluation exercise has been carried out following the conclusion of the pilot. The pilot and its evaluation are discussed further on page 29.
- 1.4 BRDO commissioned the University of Cambridge to carry out research to examine the practical implementation of data sharing under the Code. The researchers conducted interviews with regulators and key stakeholders as well as a review of current literature. The research project is discussed further on page 29.
- 1.5 Government is committed to assisting non-economic regulators to function efficiently and in a way which minimises burdens upon compliant business. This document sets out Government's intentions to make it easier for non-economic regulators to share data, legally and proportionately, in order to realise benefits for regulators and business, as well as helping regulators to meet their obligations under the Code.

2. Exploring data types and barriers to sharing data

- 2.1 The consultation explored the different types of data collected by regulators about the businesses they regulate, whether these data types should be shared and any barriers which prevent sharing. A list of data types was posed by the consultation as a suggested starting point, and a series of questions posed for each data type. The consultation also sought input as to data types not identified in the list.

Data types

1. Personal data
 2. Fact based standard data
 3. Fact based specialist data
 4. Licence data
 5. Compliance data supplied by business
 6. Data voluntarily supplied by business
 7. Inspection results and analysis
 8. Ongoing investigations
 9. Complaints data
 10. Enforcement action
- 2.2 Government is keen to identify the barriers which may prevent or discourage regulators from sharing data. The consultation posed several questions in this regard to identify barriers and how these impact upon regulators' ability to share data. The consultation posed three potential solutions, and sought input as to any other potential solutions.

Consultation responses

Question 1:

Should personal data¹ be shared? If so, for what purpose?

- 2.3 There were 45 responses to this question, including national and local regulators and business groups. The majority (42) agreed that personal data should be shared. Responses indicated that sharing personal data provides benefits in terms of improving efficiency by ensuring data integrity, helping to allocate resources and assisting investigations. The remaining three responses did not disagree with the notion of sharing personal data entirely, but indicated that careful consideration needs to be made when deciding whether personal data should be shared and that it should be within the limits set out by guidance of The Information Commissioner's Office (ICO) and the Ministry of Justice. The Health and Safety Executive (HSE) expressed a view that sharing *"might be viewed controversially by the general public and may have an impact on duty holders, members of the public or whistleblowers having the confidence to contact HSE with information."*

¹ Personal data is data that relates to a living individual who can be identified from that data, or other data that is in the data controller's possession (or is likely to come into their possession). For example, name, address and date of birth.

Question 2:

Do you have the necessary legal power (vires) to enable you to share this data? If so, does it specify a purpose for which this data is allowed to be shared?

- 2.4 There were 27 responses to this question, of which all but one indicated that they have the necessary legal powers to share personal data. Respondents mentioned the Enterprise Act 2002, the Crime and Disorder Act 1998 and the Fire and Rescue Services Act 2004 as examples of legislation that enable personal data sharing. Some respondents also quoted the benefits of memoranda of understanding (MoU) in establishing a framework of sharing data, for example, the financial MoUs between the Prudential Regulation Authority and the Financial Conduct Authority (FCA), Financial Services Compensation Scheme (FSCS), and Financial Ombudsman Service (FOS).
- 2.5 The National Trading Standards Board and Association of Chief Trading Standards Officers felt that the legal powers were in place to enable data sharing although *“we do have concerns that different government departments seem to have different approaches in how they are willing to share data with us and the level of MoUs, agreements etc. they require and the advice they give local authorities in order to facilitate this. It would be helpful if this would be applied more consistently.”*

Question 3:

Are there any circumstances in which personal data should not be shared? Do you feel that the Data Protection Act 1998 prevents the sharing of personal data? Please provide detail for your answer.

- 2.6 Thirty-eight respondents answered this question. Of these, 22 indicated that personal data should not be shared in some circumstances. These circumstances include where the data subject does not consent to the sharing of their personal data, where there is unnecessary disclosure or where the sharing has no specific objective.
- 2.7 Fifteen responses cited the Data Protection Act 1998 (“DPA”) as a barrier to data sharing. Some respondents cited confusion as to the circumstances under which sharing personal data was permissible under the DPA and felt that guidance on the DPA was limited and/or unclear. Similarly some respondents indicated that the DPA poses a cultural barrier in that some regulators are discouraged from sharing personal data because they are unnecessarily concerned about breaching the DPA.
- 2.8 Eight responses indicated that the DPA actively supports the sharing of personal information under appropriate safeguards. However, these respondents cited a lack of understanding about how the DPA operates in practice, which discourages regulators from sharing data, rather than the DPA itself.
- 2.9 Some respondents indicated that whilst the DPA provides a clear direction as to the sharing of personal data in relation to criminal matters, the situation in relation to non-criminal matters is somewhat unclear and guidance in this regard would be helpful.

Question 4:

Do regulators consider data regarding sole traders to be personal data?

- 2.10 Twenty-one respondents indicated that they consider data regarding sole traders to be personal data. Of these, 19 were regulators and two were businesses. A further three respondents indicated that they do not consider this data as personal, and some further respondents were unsure. The Homes and Communities Agency (HCA) commented that: *“When processing information about sole traders that relates not just to their business activity but also their private life, the ability to share data will need to be considered more carefully, and considered on a case by case basis.”* The ICO response made it clear that its view is that sole trader data is personal for the purposes of the DPA: *“We consider information about the business of a sole trader to be personal data as information about the business will necessarily be about the sole trader. We consider information about an individual in a partnership will be personal data if it relates to a specific partner, and this will be more likely in a small partnership.”*

Question 5a:

Should fact based standard data² be shared? If so, for what purpose?

- 2.11 Thirty-two respondents indicated that fact based standard information should be shared, and that doing so can assist to better inform risk assessments and enhance transparency and consistency. Many noted that much data was already available in the public domain such as company accounts, business names and addresses, annual reports and business plans. These responses also indicated that sharing this data type can reduce administrative burdens for both business and regulators. Business workshop participants also indicated that they were content for this type of data shared in order to reduce administrative burden.
- 2.12 The Office for Nuclear Regulation (ONR) felt that: *“We have no concerns with the sharing of this data, and agree that it would be useful to pool knowledge on when stakeholders have changed names, moved, dissolved etc. However, there would need to be an accepted verification process to ensure that this data remained valid and useful at any given moment.”*
- 2.13 Gloucestershire County Council commented that: *“Where this information relates to business identity and location this would appear to be mutually beneficial and honest businesses should have nothing to fear. This would appear to fit with the requirements of the Regulators’ Code to reduce the burden on business.”*
- 2.14 A further three respondents indicated that this data type should not be shared, as doing so could increase administrative burden for regulators. Another two respondents indicated that this data type should only be shared in certain circumstances. Trading Standards South East felt that data sharing be proportionate: *“It should only be shared for purposes directly attributable to the functions of the Regulator concerned. It may be justifiable and proportionate for a local Trading Standards Service and Environment Health Departments to share data with each other and the Food Standards Agency in respects of food enforcement. It is unlikely that it would be justifiable and proportionate for either local authority agency to share the same data with the Financial Conduct Authority. Consequently, careful consideration would need to be given to the construction of the relevant legislative framework to ensure that fact based standard data is not routinely shared where it is not justifiable and proportionate to do so.”*

² Fact based standard data is basic, factual information about a business, such as business name and address.

Question 5b:

Do you have the necessary legal power (vires) to enable you to share this data? If so, does it specify a purpose for which this data is allowed to be shared?

- 2.15 The majority of the 30 respondents who answered this question indicated that they have the necessary legal powers to share this data. Some respondents indicated that they have specific legal powers in their enabling statutes, whereas others cited the DPA and Enterprise Act 2002 as the source of their powers to share.
- 2.16 Respondents noted how the purpose of sharing data determined whether and under what circumstances it could be shared. For example, investigation of alleged criminal offences or breaches of civil legislation is enabled under the DPA and consumer legislation. Gloucestershire County Council commented that sharing fact based data to focus inspections could be more complex: *“The statutory powers available to Trading Standards Services could not be used as, in the main, the powers allowing us to require production of evidence are only available on suspicion or belief that provisions of the legislation have been breached and an offence may have been committed. This restriction would also apply to sharing fact based data with non-enforcement regulators. Where we hold information gathered through exercising functions specified in the Enterprise Act 2002, we are prohibited from sharing that information unless a permissive gateway exists. These gateways allow for information sharing to other enforcers under certain conditions but they are permissive not automatic, therefore data can still be withheld where it is not necessary and proportionate to share it.”*

Question 5c:

Are there any circumstances in which fact based standard data should not be shared?

- 2.17 Thirty-eight respondents answered this question and the majority indicated that sharing should only occur when it is legal and proportionate to do so. The ICO felt that: *“There is unlikely to be a problem in sharing for genuine regulatory purposes.”* Some respondents indicated that sharing of data could occur if the provisions of the DPA, the Human Rights Act 1998 and the Duty of Confidentiality were met. Many agreed that sharing should not occur where the data concerned may be personally or commercially sensitive or is related to sites that have specific security issues.
- 2.18 The Homes and Community Agency (HCA) noted that data *“should also not be shared where there is an agreement or contract either written or implied that the data will not be shared unless it meet the exceptions to do so as laid down by legislation. Data should also not be shared when doing so would hinder the HCA from meeting its statutory objectives and undertaking effective regulation.”*

Question 6a:

Should fact based specialist data³ be shared? If so, for what purpose?

- 2.19 Thirty-two respondents answered this question, of which 28 indicated that fact based specialist data should be shared. Generally respondents felt that whilst sharing this type of data could be beneficial, such data may not always be relevant to all regulators. The utility of sharing may therefore be situation-specific.

³ Fact based specialist data is detailed, specialised information about a business (for example, the processes or equipment used by the business which are subject to regulatory requirements).

- 2.20 The Wales Head of Environmental Health Group commented on the existing exchange of data between regulators: *“Data is currently shared if there is value in sharing it. Local authority regulators do share it and also use it with external partners (including police, UK Border Force, HMRC, Department for Work and Pensions, NAFN⁴, Food Standards Agency, Health and Safety Executive, Local Health Boards, Welsh Government Data Unit, Department for Environment Food and Rural Affairs and Welsh Government etc).”*
- 2.21 Some business respondents cited Primary Authority as an example of businesses willingly providing this type of data to regulators with the expectation that it will be shared, and in turn burden upon business will be reduced.

Question 6b:

Do you have the necessary legal power (vires) to enable you to share this data? If so, does it specify a purpose for which this data is allowed to be shared?

- 2.22 Seventeen respondents indicated that they have the necessary legal powers to share this type of data. Of these, 10 respondents indicated that they have a specific legal power to share fact based specialist data, and in some cases there is a statutory requirement to publish and/or share the data. For example, the legislation that established the ONR, The Energy Act 2013, contains an information sharing Schedule 9. This allows the sharing of information, including fact-based specialist data, with consent from the person supplying the information, or where necessary for the purposes of a government department or a select number of ‘relevant authorities’ ONR can also disclose information for its own purposes. However, ONR note that *“this does not allow for the wholesale sharing of fact-based specialist data without consent, unless this is governed by FOIA⁵ or DPA.”*
- 2.23 The Royal Borough of Kensington & Chelsea said that: *“If it is to carry out a statutory function of ours then we do have the necessary legal power to enable us to share personal data as long as it is fair and necessary.”*
- 2.24 Some told us that they are creating specific mechanisms to make the application of data sharing provisions clearer. Wales Heads of Environmental Health commented that: *“The Data Protection Act is not always straightforward to understand, therefore a Wales Accord on the Sharing of Personal Information framework is being developed as a practical initiative that seeks to make compliance with the law much easier for organisations when sharing personal information.”*

Question 6c:

Are there any circumstances in which fact based specialist data should not be shared?

- 2.25 Sixteen respondents indicated that this data should not be shared where sharing could compromise the security of the data, particularly where the data is sensitive in nature. Six respondents indicated that there should be a legitimate need for regulators to share the data for the purposes of carrying out their regulatory functions. Some of the responses commented on the need for strict controls if such information was to be shared. For example, the HSE commented that commercially sensitive data *“could only be shared if it was relevant and security data security provisions were in place.”*

⁴ National Anti-Fraud Network

⁵ The Freedom of Information Act 2000

Question 7a:

Should licence data be shared? If so, for what purpose?

- 2.26 Twenty-nine respondents answered this question, and all but one recognised that licence data is in the public domain and therefore sharing such data should not be regarded as a contentious issue. Respondents felt that sharing licence data could reduce burden for both businesses and regulators, as well as assisting regulators to carry out regulatory functions more effectively. One respondent indicated that licence data may be personal, if it concerns the licensee's home address.
- 2.27 The National Federation of Meat and Food Traders commented that sharing of licence data would be beneficial and result in *"consistency, transparency and reduce repetitiveness."*

Question 7b:

Do you have the necessary legal power (vires) to enable you to share this data? If so, does it specify a purpose for which this data is allowed to be shared?

- 2.28 Eighteen respondents indicated that they have the necessary legal powers to share licence data. Many respondents noted that most licence data is already in the public domain. For example, The Licensing Act 2003 and Gambling Act 2005 require the information to be provided in a public register. This information enables consumers have access to transparent information for consumer protection purposes.
- 2.29 Devon and Somerset Trading Standards Service felt that: *"There are appropriate legal gateways which allow sharing for specific purposes."*

Question 7c:

Are there any circumstances in which licence data should not be shared?

- 2.30 Twenty-three respondents answered this question, 13 of which indicated that there are no circumstances in which licence data should not be shared as it is already in the public domain. The remainder indicated that caution should be exercised where the data may be personally or commercially sensitive.
- 2.31 Security issues were also cited as a reason not to share licence data. The HSE felt that: *"Some sites may have specific national security issues. In such cases, HSE would require suitable security measures to be in place before we could consider if such data should be shared."*

Question 8a:

Should compliance data supplied by business be shared? If so, for what purpose?

- 2.32 This data consists of information a business is required to supply to its regulator(s) in relation to its compliance with regulations or certain occurrences or activities. Thirty-four respondents answered this question, of which 29 indicated that this type of data should be shared. Business respondents felt that sharing this type of data could help to deliver earned recognition, and to assist regulators to prioritise inspections according to risk.
- 2.33 Responses from regulators indicated that such sharing could allow for more effective and 'joined up' regulation. Some regulators noted that they are statutorily obliged to share this type of data with certain bodies, such as the police and HMRC.

- 2.34 The ICO noted that some compliance data is already proactively published on its website: *“In our view, the sharing of other compliance data is beneficial to allow effective, joined-up regulatory action and avoid duplication. For example, in fulfilling our enforcement roles under the Privacy and Electronic Communication Regulations (PECR) it is beneficial for us to share compliance data with other relevant regulators and agencies such as Ofcom and the Ministry of Justice Claims Management Regulatory Unit.”*
- 2.35 Several responses noted that context is important in terms of whether sharing this type of data is useful. Compliance data might be relevant only to one regulator and not to another, for example. Compliance data shared without contextual information may limit the usefulness of the data.

Question 8b:

Do you have the necessary legal power (vires) to enable you to share this data? If so, does it specify a purpose for which this data is allowed to be shared?

- 2.36 Thirteen respondents indicated that they have the necessary legal powers to share this data. Some expressed a view that vires will depend on the exact nature of material to be shared and for what purpose. Of these, most cited the DPA and Enterprise Act as the source of their powers. Some respondents noted that there are some restrictions on their abilities to share data, such as disclosure only to specified bodies. Some respondents noted that it is easier to share in the context of criminal offences. A further eight respondents indicated that they were unsure, or their powers to share were limited.

Question 8c:

Are there any circumstances in which compliance data should not be shared?

- 2.37 Sixteen respondents indicated that this type of data should not be shared in some circumstances, for example where the data is commercially or personally sensitive. Many respondents stressed the importance of safeguards in the context of sharing compliance data, particularly where the data could damage the reputation of a business. Some respondents were concerned that sharing compliance data prematurely could present an incomplete or unclear picture of a business' compliance record.
- 2.38 The Association of Accounting Technicians considers the process of sharing data *“would be assisted on an ongoing basis by having an independent party (e.g. an appointed ombudsman or Information Commissioner) decide on case by case basis.”*

Question 9a:

Should data voluntarily supplied by business⁶ be shared? If so, for what purpose?

- 2.39 Thirty-five respondents answered this question, of which 29 indicated that data voluntarily supplied by the business should be shared.

⁶ This question pertains to information a business might voluntarily supply to its regulator(s), for example in relation to its compliance procedures, which is beyond the requirements of regulation.

- 2.40 Respondents cited benefits of sharing this data including delivering earned recognition for compliant businesses, and encouraging open, collaborative relationships between regulators and businesses. The Home Retail Group felt that *“if the business consents to the data being used then it’s not a problem. Whether it is in the interests of good regulation for this data to be shared without the consent of the business – whether the creation of a statutory duty or ability to share will have an effect on businesses willingness to share information voluntarily is the key issue here. It is highly likely that information that has been voluntarily shared has been done so by the business in its interest so further sharing would normally be intended to promote its approach to compliance.”*
- 2.41 Several responses noted however that, given this data is supplied voluntarily, the consent of the business should be obtained before sharing. One respondent indicated that the business should retain the discretion to share. Some respondents were concerned that sharing this data may discourage businesses from voluntarily supplying it.

Question 9b:

Do you have the necessary legal power (vires) to enable you to share this data? If so, does it specify a purpose for which this data is allowed to be shared?

- 2.42 Twenty-four respondents indicated that they have the necessary legal power to share this data, although responses noted that because the data is voluntarily supplied, legal powers to share are not necessarily clearly defined. The DPA and Crime and Disorder Act 1998 gateways were cited as the source of powers to share.
- 2.43 Primary Authority was cited as a good example of where information sharing works well between partners, being used to inform assured advice and the inspection plan. The Home Retail Group felt that: *“Some of this data will be shared on the Primary Authority Register in support of the assured advice – the business is happy for it to be shared and the regulator sees the benefit of making it available to other regulators, whether it’s in full or in a summarised form.”*

Question 9c:

Are there any circumstances in which data voluntarily supplied by businesses should not be shared?

- 2.44 Fifteen respondents indicated that this type of data should not be routinely shared. Many respondents were concerned that sharing could undermine business’ trust in regulators and discourage the provision of data on a voluntary basis. One respondent suggested that in circumstances making the benefits of sharing evident to business will encourage the voluntary provision of data. Primary Authority was cited as an example of this.
- 2.45 The ICO stressed that *“it is important to bear in mind that regulators must be open and honest with businesses about data sharing. In the case of data voluntarily supplied the consequence of sharing may be that the business declines to supply the data in the first place, thus undermining effective regulation.”*

Question 10a:

Should inspection results and analysis be shared? If so, for what purpose, and what benefits might result?

- 2.46 Twenty-seven respondents indicated that inspection results and analysis should be shared. Respondents indicated that such sharing could deliver benefits including ensuring efficient allocation of resources and providing a more detail for risk assessments.
- 2.47 Leicestershire County Council, Trading Standards noted that *“sharing inspection results would make effective use of resources and avoid unnecessary inspections.”* Many responses cautioned that this type of data should only be shared where there is a legitimate and proportionate need, and stressed the importance of context. Business and regulator respondents agreed on the importance of clear guidelines on the boundaries of historical data. This was echoed in both the business and regulator workshops.
- 2.48 Five respondents indicated that this data should not be shared, some of which questioned the relevancy of one regulator's inspection results and analysis to other regulators. Business workshop attendees expressed some reservations that the sharing of inspection results and analysis could result in a business receiving undue attention from regulators.

Question 10b:

Do you have the necessary legal power (vires) to enable you to share this data? If so, does it specify a purpose for which this data is allowed to be shared?

- 2.49 Twenty-three respondents indicated that they have the necessary legal powers to share this data. The DPA and Enterprise Act were cited as the sources of these powers.
- 2.50 The HCA expressed uncertainty about the extent to which the underpinning data can be shared: *“The Housing and Regeneration Act 2008 states that the inspection report that is produced can be published and as such we would be able to share this report; however the Act is silent on the full range of data and analysis that sits behind the report and the purpose for publishing/sharing the data.”*

Question 10c:

Are there any circumstances in which inspection results and analysis should not be shared?

- 2.51 Twelve respondents indicated that under some circumstances this data should not be shared, whereas 10 respondents indicated to the contrary. Some respondents questioned the relevance of one regulator's inspection results and analysis to other regulators.
- 2.52 The National Federation of Meat and Food Traders commented that the information should not be shared *“in cases with subjective criteria and inadequate appeal processes.”*
- 2.53 The HSE commented that in cases with technically complex issues that may take significant time to resolve *“the sharing of such data would have to [be] very carefully handled to avoid misinterpretation.”*

Question 11a:

Should the existence of ongoing investigations be shared? If so, for what purpose?

- 2.54 Thirty-five respondents answered this question, of which 26 indicated that the existence of ongoing investigations should be shared. Several regulators saw advantages in sharing this data, including encouraging joined up regulation and assisting regulators to identify risks. For example, the HCA currently publishes details of 'grading's under review' which are a form of investigation and *"sees no reason why the existence of on-going investigations in the form of 'grading's under review' should not be shared."*
- 2.55 Some respondents noted that early knowledge of the existence of investigations could prove invaluable, particularly in the context of public health and welfare issues. The nine respondents who indicated that such information should not be shared were concerned that sharing this data could create an unclear or imperfect picture of a business, and impact negatively upon its regulation.
- 2.56 The FCA told us that *"although the fact of an investigation is not confidential information"* there are circumstances under which they will not generally publically confirm or deny that an investigation exists *"unless failing to make the position clear is likely to cause public uncertainty, speculation or rumour in relation to takeover bids."*

Question 11b:

Should details of ongoing investigations be shared? If so, for what purpose?

- 2.57 Thirty-two respondents answered this question, of which 21 indicated that details of ongoing investigations should be shared. These respondents agreed that there are benefits to sharing this data, but cautioned that such data should be shared on a case-by-case, or 'if requested' basis, recognising that some cases may be particularly sensitive or legally privileged. Seven respondents indicated that this data should definitely not be shared, and a further four indicated that it might be appropriate to share, depending on the circumstances involved.
- 2.58 The Home Retail Group felt that caution was needed around sharing information during an investigation: *"The details of the investigation, the evidence gathered is likely to be the subject of confidentiality – gathered using statutory powers and only in the public domain if the matter goes to court, so it feels inappropriate to share that information during the investigation. The mere fact an investigation is under way should not receive the same weight as a matter that has concluded its passage through due legal process."*

Question 11c:

Do you have the necessary legal power (vires) to enable you to share this data? If so, does it specify a purpose for which this data is allowed to be shared?

- 2.59 Twenty-eight respondents answered this question, of which 24 indicated that they have the necessary legal power to share this data. The DPA and Enterprise Act were cited as the gateways used to share this data. Two respondents indicated that they do not have the necessary legal power to share this data, and another two were unsure.

- 2.60 Some respondents outlined mechanisms to share data including specific gateways such as those under the Financial Services and Markets Act 2000 (Disclosure of Confidential Information) Regulations 2001. The FCA has a 'self-help gateway' to disclose confidential information to another person, if it will enable or assist them in the discharge of their public functions, i.e. to obtain information to assist in their investigation.

Question 11d:

Are there any circumstances in which the existence and/or details of ongoing investigations should not be shared?

- 2.61 Twenty-three respondents answered this question, of which 15 respondents identified circumstances in which this data should not be shared. These include the duty of the regulator to protect sensitive commercial data where the release of this data could have a negative effect on the business and where onward disclosure would risk prejudicing ongoing investigations. The ONR, for example, commented that: *"We have no concerns with sharing the existence of investigations, where appropriate. We would also take into consideration whether disclosure at the time might affect the outcome of that investigation and act appropriately."*

Question 12a:

Should complaints data be shared? If so, for what purpose?

- 2.62 Thirty-five respondents answered this question, of which 21 indicated that complaints data should be shared. Seven respondents indicated that complaints data should not be shared, and a further seven indicated that it might be acceptable to share complaints data, depending on the circumstances. The ICO said that: *"In terms of complaints data collected by the ICO as part of our regulatory functions, then we consider it would be helpful to share the most common causes of concern. We also consider it would be crucial to share the associated action taken to help avoid those complaints or issues arising in the same frequency."*
- 2.63 Many respondents indicated that 'complaint' can have different meanings depending on the surrounding circumstances, and pointed to a need for a common definition. This was echoed in the regulator workshops. Some respondents indicated that complaints data is of little use or relevance unless it is placed into context; therefore sharing basic information such as complaints figures may be of limited use.
- 2.64 Some respondents indicated that complainants may not wish to have details of their complaints shared, and that this may discourage complainants from coming forward. Some business respondents indicated that it would be unfair to share complaints data, particularly if the complaints were later proved unsubstantiated. Conversely, some regulators indicated that sharing complaints data is very useful, in terms of identifying trends and compliance issues.
- 2.65 The Chartered Institute of Legal Executives and ILEX Professional Standards Limited said that: *"We have no issues with sharing anonymous complaints data as the statistics are published on the IPS website annually. However caution must be exercised in relation to sharing complaints data about individuals or entities which remain unproven."*

Question 12b:

Do you have the necessary legal power (vires) to enable you to share this data? If so, does it specify a purpose for which this data is allowed to be shared?

- 2.66 Twenty-seven respondents answered this question, of which 23 indicated that they have the necessary legal powers to share complaints data. Several respondents indicated that they were only able to share complaints data when there was a belief that an offence had been committed. Some respondents, such as The Marine Management Organisation, indicated that they share complaints data under the DPA, where such data has been appropriately anonymised: *“Sharing of complaints data will contravene the Data Protection Act 1998, as is typically not shared unless it is sufficiently anonymised prior to sharing.”*
- 2.67 The FCA said it is *“able to share complaints data with a public body, either to help the FCA carry out its own statutory functions, or to help another public body carry out its functions, provided that that public body is identified in the regulations made under the section 349 of the Financial Services and Market Act 2000 and sharing is consistent with European law (where it applies).”*

Question 12c:

Are there any circumstances in which complaints data should not be shared?

- 2.68 Thirty respondents answered this question, of which 21 indicated that complaints data should not be shared in certain circumstances. The majority of respondents indicated that complaints data can be shared where it is legal and proportionate to do so, but this data should not be shared where for example there is an ongoing investigation or where impartiality and fairness could be compromised as a result. Respondents also expressed concern as to the impact of sharing complaints data upon the reputation of business, for example where a business’ reputation may be adversely affected without justification.
- 2.69 One fire and rescue service commented that: *“The complaint but not the complainant’s details (should be shared); these may be vexatious and as such shared to identify potential patterns.”*

Question 13a:

Should enforcement action data be shared? If so, for what purpose, and how much detail should be shared?

- 2.70 Enforcement action is used in this context to refer to any action taken by regulators to secure compliance with legislation. Thirty-four respondents answered this question, of which 27 indicated that enforcement action data should be shared. The majority of these felt that sharing this data encourages greater transparency amongst regulators and in turn results in better informed risk assessment, often leading to lower levels of enforcement action being taken against businesses. Some responses highlighted the public interest element to regulators sharing enforcement action data, particularly in terms of regulators working collaboratively.

- 2.71 It was generally felt that sharing such data can assist regulators to target regulatory action appropriately, such as offering advice and assistance rather than taking punitive measures, where appropriate. The Claims Management Regulation Unit, Ministry of Justice, commented that *“a large amount of enforcement action against any businesses may flag up the need for intervention of some type, which may not be enforcement action, and could lead to the business receiving appropriate regulatory assistance and/or advice.”*
- 2.72 Some of these responses indicated that the Rehabilitation of Offenders Act 1974 limits the period for which information about criminal cases can be retained to five years.
- 2.73 Three responses indicated that enforcement action data should not be shared, on the basis that such data is not always relevant and can add burden to regulators. The HCA, for example, commented that *“much of our existing enforcement action is on public record, but usually only after the end of a process.”* Some business respondents cautioned that appropriate safeguards need to be in place in order for this type of data to be shared. This was echoed by some regulators such as the HCA who advocated *“a case by case approach to the sharing of enforcement data. The best way to achieve this would be through establishing data sharing protocols between relevant non-economic regulators to ensure that only relevant and legitimate data is shared. We feel that the Regulators’ Code section 4.2 gives us the mandate to use this approach (when the law permits) and no further direction is needed.”*

Question 13b:

Do you have the necessary legal power (vires) to enable you to share this data? If so, does it specify a purpose for which this data is allowed to be shared?

- 2.74 Twenty-six respondents answered this question, of which 21 indicated that they have the necessary legal power to share enforcement action data. Some of these indicated that they are able to share this data publicly, whereas others are able to share it with other regulators. The HSE commented that *“there are specific restrictions on HSE collecting and releasing information and these are set out in the Health and Safety at Work Etc. Act 1974 Sections 27 to 28. However, enforcement data relating to an individual is removed from HSE’s website after 5 years in order to comply with the Rehabilitation of Offenders Act 1974, and a mechanism would have to be put in place that would allow this data to be removed from a shared database.”*

Question 13c:

Are there any circumstances in which enforcement action data should not be shared?

- 2.75 Twenty-eight respondents answered this question, of which 20 indicated that this type of data should not be shared in some circumstances, including instances where the enforcement action has been appealed against or where enforcement action is ongoing. Business respondents indicated that robust safeguards need to be in place before this type of data is shared.
- 2.76 The ONR felt that information should not be shared where the information is not relevant to other regulators or where it is likely to be merely prejudicial than probative *“with the sharing of this data, beyond any resource burdens imposed, although we would not expect to share details of ongoing enforcement action unless this was already in the public domain. Information requiring certain levels of security clearance should not be shared with organisations that do not have an equivalent standard level – and where security information was included as part of safety requirements.”*

Question 14a:

Other than those listed above, are there any other types of data which regulators could share? If so, for what purpose?

Question 14b:

Do you have the necessary legal power (vires) to enable you to share this data? If so, does it specify a purpose for which this data is allowed to be shared?

Question 14c:

Are there any circumstances in which this information should not be shared?

2.77 Thirteen respondents answered the above three questions in one answer. Several suggestions were made as to other types of data regulators could share, including:

- product test results to enable regulators to better test compliance with standards;
- turnover and/or profit information to enable regulators to better understand motives for non-compliance;
- advice provided to businesses;
- performance data relevant to the Governments priority regulatory outcomes; and
- data pertaining to the economic standing of geographical areas in order to give context and identify compliance patterns.

2.78 Response to questions 14 b and c reflected and the responses given to questions 5-13. For example, the HSE commented that issues related to *“collecting and releasing information are set out in the Health and Safety at Work Etc. Act 1974 Sections 27 to 28.”*

Question 15:

Which regulators currently share data, and how is it shared? What is the purpose of sharing the data, and what benefits does it bring?

Please name the regulators involved, or indicate the type of regulator (for example, national regulator, local authority) and give details as to how the data is shared (for example, by use of a database, on request, etc).

2.79 Thirty respondents indicated that they currently share data with five or more regulators or other bodies. The most commonly cited of these include the Police, HMRC, Department for Work and Pensions (DWP) and the Food Standards Agency.

2.80 The responses outlined purposes for sharing data, including where it is a legislative requirement, for example the sharing of information with the Police and HMRC, and where it is believed to be of merit to share data in the prevention of crime and to aid investigations. The benefits of sharing data identified in the responses include improved data integrity and the allocation of resources to more proactive and targeted enforcement.

2.81 The majority of respondents indicated they share data on request which can include access to information requests, exchange of databases (including spreadsheets) and shared systems. Eight responses indicated they use shared databases, or compatible systems.

- 2.82 The responses note disparity between regulators as to the arrangements they need to have in place before sharing data and intelligence. Some regulators, such as the ICO and Fire and Rescue Services, set up data sharing agreements and/or memoranda of understanding, whereas others indicated less formal arrangements.
- 2.83 The workshops demonstrated that many regulators are already sharing data and realising benefits as a result. Several regulators indicated that they are using data sharing agreement and memoranda of understanding to facilitate data sharing.

Question 16:

Is there any type(s) of data which regulators need to share, but do not share at the present time? If so, please explain why this data is not shared.

- 2.84 Twenty-two respondents answered this question. Types of data cited included compliance and inspection data, personal data, national customer complaint data from the Citizens Advice Service and data from Ofcom, the DWP and HM Revenue and Customs. Reasons given for not sharing data include a lack of current gateways, legislative barriers and incompatible IT systems. Some of the legislative barriers cited as posing potential barriers to data sharing included the Enterprise Act 2002, the Groceries Code Adjudicator Act 2013 and the Pensions Act 2004.
- 2.85 The Charity Commission commented that two of the regulators that they liaise with, *“Ofcom and DWP, face practical obstacles in sharing data with us due to the legislation they work within although we have no difficulty in sharing data with them through our legal gateway. DWP, for example, use a section in the DPA that allows prosecuting authorities to share information. The [Charity] Commission is not a prosecuting authority so this is an obstacle.”*

Question 17:

What are the consequences of this inability to share data? Please give details (for example, wasted time, additional costs.

- 2.86 Twenty-nine respondents answered this question. A wide variety of consequences of regulators being unable to share data were cited, including:
- regulators being unable to target their activities appropriately, resulting in additional costs for regulators and business, as well as wasting public funds;
 - delays and inefficiencies;
 - businesses not receiving advice and/or protection from rogue traders;
 - compromised consumer protection;
 - duplication of regulatory effort;
 - unidentified crime;
 - regulators being unable to identify trends and missed opportunities for risk profiling; and
 - loss of potential to prevent cross-boundary activity, with flow on effects for public protections.

Question 18:

What prevents regulators from sharing data? Please be as specific as possible.

- 2.87 Thirty-five respondents answered this question. Twenty-three indicated that the DPA prevents regulators from sharing data, either directly, or indirectly (for example by creating confusion as to whether sharing is permissible, or being used as an 'excuse' as to why data cannot be shared). Some of these responses indicated that the DPA itself poses a barrier: one group of local authorities commented that: *"the provisions of the Data Protection Act are almost impenetrable."*
- 2.88 Others indicated that misunderstanding of the DPA is a barrier, by, for example, creating confusion as to whether sharing is permissible, or is being used as an 'excuse' as to why data cannot be shared. The ONR felt that: *"the DPA does not prevent the sharing of personal data, rather it is a failure to understand how the legislation works that is usually the problem."*
- 2.89 Fifteen responses indicated that the numerous gateways available to share information can create confusion as to which is the most appropriate gateway to use in order to share data. Some respondents cited this as a cause of administrative burden. A lack of understanding of legislative powers and gateways can contribute to confidence issues and fears over breaching data security, thereby discouraging regulators from sharing data. The London Borough of Richmond noted that *"the constantly growing and changing landscape of legal gateways makes this burdensome and confusing."*
- 2.90 Eight respondents indicated that cost and lack of time impact upon their ability to form and manage processes to share data. Monitor said: *'In some cases information can legally be shared but there is a high administrative burden in doing so. There is significant onus on the public body regarding accuracy...A high degree of care should also be taken in checking the data disclosed is not confidential and has addressed any legal risks, which also implies additional time and resource cost.'*
- 2.91 Some respondents cited cultural issues as preventing or discouraging the sharing of data – for example, failing to identify data sharing as an organisational priority, or a lack of trust amongst regulators to preserve the security of shared data. Leicestershire Fire and Rescue Service felt that *"the tendency may simply be to refuse to share data as a means of protecting organisational reputation and mitigate the potential risk if an issue arises."*
- 2.92 Ten respondents cited statutory prohibitions which prevent them from sharing specific types of data.
- 2.93 Other factors cited as preventing regulators from sharing data include technological barriers, concerns of the general public and concerns over protection for staff in the event of data being lost or mishandled by the receiving regulator. Gloucestershire County Council note the incompatibility of many ICT systems: *"Where disparate ICT systems are not compatible it is a lot of effort to share data manually and this takes time and is a drain on already stretched resources; regulators will not see unsolicited data sharing as a priority."*

- 2.94 A clear theme emerging from the regulator workshops is that regulators would like to share more data, but feel that they are unable to do so for a variety of reasons, including:
- A need (whether real or perceived) to have data sharing agreements or memoranda of understanding in place before data can be shared means that establishing data sharing practices can be time consuming and resource intensive.
 - Cleansing data received from other regulators can be resource intensive and can increase burden. There needs to be an appropriate balance between this burden and the benefits resulting from data sharing.
 - The DPA is commonly cited as reason why data cannot be shared. There is confusion as to the exemptions under the DPA and when these apply. This confusion is often perceived by regulators as either genuine misunderstanding or an excuse not to share data.
 - Some regulators are restricted by their enabling statutes, which limit the type of data they can share and who it can be shared with.
 - Cultural barriers can prevent or discourage data sharing. Some regulators do not consider data sharing to be useful in meeting their own priorities and therefore consider data sharing to be a low priority.
 - A reluctance to 'trust' that data will be safeguarded appropriately once it has been given to another regulator.

Exploring data types and barriers to sharing data: Government response

- 2.95 Responses from business clearly indicate that regulators sharing data brings benefits for business. It is recognised that data sharing can help regulators to deliver earned recognition and to use regulatory resources more efficiently, thus freeing resource to provide advice and guidance to help businesses comply, and to target non-compliance. Business is also clear that any sharing of data must be proportionate and for a specific purpose. Some data types are more sensitive than others and in some circumstances the sensitivity of some data types may outweigh the need to share. Government recognises that effective safeguards are important, to ensure that data is not misused and to maintain the confidence of businesses and the public.
- 2.96 Regulators are generally keen to share data and many are already doing so, albeit to varying degrees. Many regulators would prefer to share more data, and with more regulators, but are prevented from doing so for various reasons. From a regulatory perspective, data sharing brings tangible benefits by saving resources and equipping regulators with information necessary to regulate effectively. Regulators also recognise that sharing data enables a more cohesive, 'joined up' approach, which ultimately delivers improved public protections.

- 2.97 Regulators' responses suggest that considerable confusion and misunderstanding exists in relation to the DPA, and which is often cited as a reason why data cannot be shared, when often this is not the case. The DPA applies only to personal data, yet responses from regulators indicate that there is some confusion as to overlap between personal and business data (such as in the case of sole traders) and regulators sometimes find that making this distinction is too difficult and instead err on the side of caution by not sharing data. There is also a considerable amount of confusion, or lack of confidence, among regulators as to the framework established by the DPA for sharing personal data. As a result, regulators are discouraged from sharing data.
- 2.98 Some regulators have indicated that they find data sharing too burdensome and are hindered by a lack of resource or knowledge as to how best to go about sharing data, or how to get started. There is confusion as to when data sharing agreements or memoranda of understanding are warranted, and where these are necessary, regulators sometimes find developing them too resource intensive.

3. Scoping the options

Consultation responses

Question 19:

Is a measure in primary legislation the most appropriate means of encouraging regulators to share data? Please give reasons for your answer.

- 3.1 Thirty-four respondents answered this question. Opinion was evenly split, with 17 respondents indicated that primary legislation is the most appropriate means of encouraging regulators to share data, and 17 respondents indicating to the contrary.
- 3.2 Those in favour of primary legislation had diverse views as to what a primary legislative measure would look like and how it could work. Five respondents indicated that they would like primary legislation to provide an enabling power for regulators to share data. Three respondents indicated that data sharing should be a statutory requirement for regulators. A further three respondents indicated that primary legislation could be used to establish a clear framework as to data that can (or cannot) be shared. Four respondents indicated that they would prefer primary legislation to be used to remove specific statutory barriers to data sharing. Two respondents indicated that primary legislation should include an enforcement mechanism for misuse of data and/or inappropriate data sharing. The regulator workshops mirrored these differing opinions, with those regulators in favour of a primary legislative measure having differing views as to what such a measure could look like and how it could work. Several regulators were opposed to a primary legislative measure on the basis that it could increase burden or be overly prescriptive.
- 3.3 Those opposed to primary legislation had several concerns, in particular that a primary legislative measure could be too prescriptive, placing further legislative burdens on regulators. The Charity Commission noted that: *“Primary legislation may be the only way to remove legal obstacles to sharing that are identified (although it is also possible that active review of them might identify some as surmountable without legislative change)...A well designed programme of encouragement as good practice could bring faster, if less legally certain, results.”*
- 3.4 Some were concerned that regulators could be forced to comply with a restrictive regime, exacerbating complexity and confusion, and that extra resource might be needed in order to comply. One respondent was concerned that the introduction of a new legislative measure may inadvertently create conflict with individual regulators’ enabling statutes.
- 3.5 Business workshops attendees’ views were also mixed, with some indicating that a primary legislative measure could encourage greater data sharing and reduce burden for business. Others questioned the effectiveness of such a measure.

Question 20:

Is embedding data sharing as best practice the most appropriate means of encouraging regulators to share data? Please give reasons for your answer.

- 3.6 Thirty-three respondents answered this question, of which 19 agreed that embedding data sharing as best practice is the most appropriate means of encouraging regulators to share data. Of those in favour, several indicated that this option would be beneficial as a flexible, non-prescriptive means of encouraging regulators to share data according to their individual circumstances.

The Information Commissioner's Office (ICO) said that *"providing best practice guidance may help prioritise data sharing and build confidence around the ability to share data...Best practice is proportionate data sharing to further regulatory objectives, including simplification for businesses."*

- 3.7 Several respondents felt that this would be more responsive, and allow a more targeted approach, than a generic primary legislative measure. Some respondents preferred this option as it is likely to be cost effective in comparison to primary legislation or a single point of registration. The Marine Management Organisation said: *"There is a need for secure common tools and agreed quality assurance standards to facilitate productive and cost effective data sharing."*
- 3.8 Some respondents felt that embedding data sharing as a form of good practice would be ineffective because it would not address legal and practical barriers, which prevent data sharing. Neither would it encourage otherwise reluctant regulators to share data. Some respondents indicated that this option would only be feasible if implemented alongside a primary legislative measure.
- 3.9 In the regulator workshops, regulators were clear that this is the preferable option, and that in particular action is needed to improve regulators' understanding of the DPA. There was also support for practical tools such as template data sharing agreements to help regulators to share data without requiring significant resource. There was also general support for such measures from business workshop attendees.

Question 21:

Do you have any views as to whether a single point of registration would be desirable?

- 3.10 Responses to this question were very diverse. Thirty-eight respondents answered this question, of which 15 were in favour of a single point of registration. A further 15 respondents agreed with the concept of a single point of registration, but were cautious about how it could work in practice and were concerned about practical limitations. Eight respondents were not in favour of a single point of registration.
- 3.11 Those respondents in favour of a single point of registration indicated that it could result in resource savings for regulators by assisting them to access up to date information, as well as assisting start-up businesses to access relevant regulatory services in a cost effective way. Business views were generally positive, suggesting that a single point of registration could give businesses more control over the information held about them by regulators. There were some concerns however that businesses could potentially be burdened by requirements to answer generic questions which may not be relevant.

- 3.12 The consideration of a one-stop shop for childminders was noted, where they might be required to register with Ofsted, the Food Standards Agency and the ICO. However, the single point option was not pursued as not all childminders are required to register with all three regulators, the information requirements are very different and all are governed by legislation. As a result the ICO decided that to *“provide better information, signposting and links but to go further than this would be disproportionately complex and expensive.”*
- 3.13 Respondents with opposing views were concerned that a single point of registration would be too expensive to establish and maintain. Some questioned its usefulness and relevance to regulators and were concerned that a generic approach might increase burden for regulators and business alike. Concerns were also raised as to who would be responsible for maintaining a single point of registration and accountability for its use.
- 3.14 Fifteen respondents consider single point of registration to be desirable in theory, however in practice a system may fail to address the different information requirements of regulators and the legislation governing each area of regulation. The Homes and Communities Agency (HCA) saw this *“as a long-term option rather than a quick fix and would agree that this option will be many years down the line.”* There were some concerns that a single point of registration could result in a large quantity of data that could be unmanageable or irrelevant. Some respondents questioned whether regulators would adhere to using a single point of registration in the absence of a statutory requirement to do so. Some business workshop attendees questioned the value of such a tool, particularly for start-up businesses.

Question 22:

Other than the options outlined above, is there any other means by which data sharing could be encouraged?

- 3.15 Eighteen respondents made various suggestions as to other means by which data sharing could be encouraged. These included:
- helping regulators to establish data sharing protocols;
 - making more data publicly available, where such data is not personal or commercially sensitive;
 - making the benefits of data sharing evident to regulators;
 - helping business to promote data sharing, for example by requesting earned recognition;
 - establishing a data sharing code of conduct for regulators;
 - making common tools available to help regulators share data in a cost effective way; and
 - establishing quality assurance standards to facilitate data sharing.

Scoping the options: Government response

- 3.16 The consultation posed three potential options: a measure in primary legislation, embedding data sharing as best practice and a single point of registration. In the interests of open policy making, the consultation did not favour any particular option over the others.
- 3.17 It is evident that Government needs to act in order to support regulators to regulate effectively and to comply with the Code. Without this support, many regulators will be unable to regulate as efficiently as they otherwise might, and in turn, the full benefits of the Code will not be realised for regulators and ultimately, for business.

- 3.18 Stakeholder opinion was very mixed on the option of a measure in primary legislation. Many stakeholders indicated that a primary legislative measure was not warranted, or was not the most appropriate solution. Of those in favour of primary legislation, opinions were very mixed about how a measure would assist regulators to share data, with opinions ranging from the need for a compulsion to share data to a general enabling power, with some regulators wanting a measure more specific to their circumstances. Government is not convinced, on the basis of this consultation, that a measure in primary legislation is necessarily the most appropriate way forward at this time. Consultation responses generated some considerable evidence however and this issue may be revisited in future.
- 3.19 The consultation elicited strong opinions both for and against a single point of registration, amongst both regulator and business stakeholders. As noted in the consultation, establishing a single point of registration would involve significant resource and as such this option is not easily achievable. Government does not propose to take this option forward at this time.
- 3.20 Government's preferred option is to take steps to help regulators to embed data sharing as best practice. Evidence gathered from consultation workshops and responses indicates that clearer guidance on the DPA, particularly its application in the regulatory setting, is needed by regulators. Work also needs to be undertaken to dispel myths around data sharing and to give regulators the clarity and confidence they need to take data sharing practices forward. Government recognises that regulators are operating in conditions where resources are sometimes stretched. To this end, regulators need practical tools to help them embed data sharing as a routine activity and to fully realise the benefits of data sharing.

Question 23:

Are there any regulators listed in Annex B which should be excluded or others which should be included? Please give reasons for your answer.

- 3.21 Twenty-one respondents made suggestions as to regulators which should be included in, or excluded from, any measure to encourage further data sharing. One business respondent indicated that the Groceries Code Adjudicator should be excluded. One local authority noted that *"HMRC should have a duty to share with other regulators rather than distrusting them."* Several suggestions were made as to bodies that should be included, including:
- HMRC
 - Police
 - Ofcom
 - Office of Rail Regulation
 - Solicitors Regulation Authority
 - Competition and Markets Authority.

Question 24:

Is it desirable to allow further regulators to be included in future, if warranted?

- 3.22 Twenty-two respondents answered this question, of which 19 indicated that provision should be made to allow further regulators to be included in future. Some respondents suggested that any measure should be limited to those regulators in scope of the proposed statutory duty to have regard to economic growth.

- 3.23 The HSE agreed that the list should be expanded *“to ensure data sharing remained future proof. However, all such regulators would have to have the same high standards of data security.”*

Government response

- 3.24 Government's preferred option is to encourage regulators to embed data sharing as best practice. BRDO will take measures forward to help those regulators subject to the Code to comply with it. Other regulators can participate in these measures if they wish to.
- 3.25 Several regulators indicated that they would like to share data with HMRC, and/or that they provide data to HMRC but do not receive any data in return. HMRC's functions include the collection of tax and the payment of some benefits, and it has only a very limited role as a regulator (conferred by the Money Laundering Regulations 2007). HMRC has a legal duty of confidentiality which allows the department to share information the Department holds in connection with its functions only in the circumstances set out in legislation. This reflects the importance placed on 'taxpayer confidentiality' by Parliament when HMRC was created⁷.
- 3.26 When making a disclosure the HMRC official must also have regard to the Human Rights Act 1998 and the DPA – so the information shared must be limited to what is relevant, necessary and proportionate; that is, the minimum amount necessary to achieve the objective⁸.
- 3.27 HMRC, the Home Office, local authorities and other agencies are participating in the Better Business Compliance Partnerships (BBCP), a series of pilots operating across five local authority areas that are engaged in joint working operations and sharing information using existing legislation while developing and trialling new ways of joint working between local and national agencies. The partnerships are also exploring whether there are legislative or procedural changes that should be made to allow HMRC to share more data with other agencies.

Question 25:

Under what circumstances would data sharing warrant the inclusion of safeguards, and how could this be achieved?

- 3.28 Thirty-seven respondents answered this question. Respondents indicated that safeguards should be included where data is shared and stored, particularly where the data concerned relates to investigations and enforcement matters. Several respondents noted that safeguards play an important role in ensuring that data is shared legally and proportionally, as well as providing protection against misuse of data. The National Casino Forum said that its *“members would not support data sharing that could be misleading nor would it support data sharing of a commercial nature.”*

⁷ The circumstances where HMRC is allowed to share information outside the Department include:

- where there is another UK or EU law which permits or requires it;
- with the consent of the subject(s) of the information;
- where the Department has received a binding court order; and
- where, on a case by case basis, the disclosure is made for the purpose of HMRC's functions.

⁸ The duty of confidentiality applies to all information that is held by HMRC in connection with its functions, including where the information is publicly available. Unlawful disclosure of information that relates to an identifiable individual or legal entity is a criminal offence, and the official making such a disclosure is personally liable. If the disclosure relates to a living individual, the Information Commissioner can also fine HMRC if he concludes that the disclosure of information amounts to a 'serious contravention' of the DPA.

- 3.29 Respondents indicated that the nature of safeguards will depend in part on the type of measure involved, such as primary legislation or best practice. Respondents indicated that safeguards should be embedded within data sharing processes. For example, regulators should impose internal controls on the accessibility of data, such as restricting access to more sensitive data type to certain levels of seniority. Some respondents indicated that existing safeguards, such as those set out in the DPA and Enterprise Act, are adequate and no further safeguards are necessary.

Question 26:

Under what circumstances would the imposition of sanctions be appropriate?

- 3.30 Twenty-four respondents answered this question. Respondents noted that sanctions are appropriate and necessary to maintain confidence – both of the data subject and general public – that data is being handled appropriately and that any misuse will result in proportionate consequences. Eleven respondents indicated that existing sanctions (such as those imposed by the DPA and Enterprise Act) are adequate and the imposition of any further sanctions would be inappropriate.
- 3.31 The ICO said that the “*sanctions should address those who act maliciously or negligently but should not seek to punish those who make errors of judgement.*”

Question 27:

Should the sharing of data be monitored? If so, to what extent?

Question 28:

Who should be responsible for monitoring the sharing of data?

- 3.32 Twenty-nine respondents answered these questions. Twenty-three respondents indicated that some monitoring is necessary to support confidence in data sharing, although there is considerable diversity of views as to what monitoring should involve. Some respondents indicated that regulators implementing formal audit trails and self-monitoring systems would be adequate, whereas others believe external monitoring is necessary. The HCA, for example, said that “*monitoring of data sharing should be undertaken by regulators themselves as part of their data sharing agreements. This should also factor into the monitoring of the compliance against the Regulators’ Code.*” Nine respondents indicated that the ICO should be responsible for monitoring. Five respondents indicated that BRDO would be an appropriate monitor. Six respondents indicated that further monitoring measures, would be disproportionate, expensive and inefficient.

Monitoring of sharing of data: Government response

- 3.33 Government recognises the importance of safeguards and monitoring to ensure that data is handled safely and to give business and the public reassurance. The current legislative framework provides effective safeguards and monitoring provision. Given that Government does not intend to make legislative changes to regulators’ statutory ability to share data, there is no intention to alter the current framework for safeguarding data and monitoring its use.

4. The Intelligent Regulatory Information System pilot, research project and Better Business Compliance partnerships

IRIS pilot

- 4.1 BRDO led on a pilot of the Intelligent Regulatory Information System (IRIS) from March to September 2014. IRIS is a software tool adapted from the 'Find It' tool developed by the Health and Safety Executive's (HSE's) Health and Safety Laboratory (HSL). The 'Find It' tool helped HSE to transform the effectiveness of its inspection activities by helping to identify businesses and premises that are likely to be high risk in terms of their likelihood to be in breach of health and safety legislation. BRDO commissioned HSL to develop an extended version of the 'Find It' tool that could be used by several regulators to share data. In response, HSL developed IRIS.
- 4.2 The pilot involved four regulators (three local authorities and a fire and rescue service) in the Leicestershire area sharing data using IRIS. Data from the four regulators, plus data from other sources, was imported into IRIS so that all the regulators could access it. The pilot participants provided feedback to BRDO and HSL throughout the pilot and consequently IRIS was refined during the pilot to improve it. A key component of the pilot was use of a common scale of regulators' assessments to enable each pilot participant to understand the outcome of the other regulators' assessments of business compliance and risk management performance (often termed 'confidence in management').
- 4.3 HSL conducted an evaluation following the end of the pilot which involved analysing usage of IRIS and feedback provided by the pilot participants. Findings from the evaluation indicate that IRIS was useful to participants in several ways. IRIS assisted regulators to locate previously unknown premises which allowed a proactive approach to be taken to provide businesses with advice on compliance issues and enhance public protections. In addition to assisting pilot participants to identify high risk businesses and premises, IRIS also gave regulators the opportunity to consider how best to provide ongoing support to such businesses.
- 4.4 Being able to identify such businesses and premises also assisted in relation to the introduction of a particular set of new regulations applicable to types of premises that the relevant regulator had not previously had any dealings and thus did not know existed. The regulator was able to identify the relevant businesses and provide them with information about the new requirements. Participants also indicated that IRIS had potential to assist with planning inspection activity priorities for the year ahead, although the timing of the pilot meant that this benefit was not fully realised.
- 4.5 The full evaluation report is available on the BRDO website. BRDO has commissioned HSL to conduct a short scoping study to explore future options for IRIS, including the possibility of making IRIS available to more regulators on a voluntary basis.

Research project

- 4.6 The University of Cambridge was commissioned by BRDO to conduct a small research project to examine the practical implementation of data sharing under the Code. Researchers conducted interviews with 63 people from 30 organisations (mainly local and national regulators) to ascertain attitudes towards data sharing, barriers which prevent or discourage data sharing, and other issues which may influence regulatory appetite for data sharing.
- 4.7 The research findings indicate that several complex factors influence the ability and appetite of regulators to share data. The statutory remit to collect data, organisational culture, resources and networks all influence the extent to which regulators share data. In addition, there are legal considerations, such as statutory remit, and practical matters, including access to technology.
- 4.8 The findings were in line with the consultation and workshop responses, with most organisations engaged in some form of formal data sharing. There was generally some confusion as to the circumstances under which the DPA allows data to be shared. Awareness of the data that was held by other regulators and comparability of the data, whether due to technical or format issues, were common problems.
- 4.9 Whilst technology and legal issues may influence regulatory ability to share data, organisational culture was cited by interviewees as the major factor inhibiting data sharing. Those regulators considered to be 'data rich' – in possession of all the data needed to fulfil their functions – often have little incentive to share data. This in turn impacts upon regulators which are 'data poor' because it is harder for these regulators to obtain data.
- 4.10 For some policy issues, such as troubled families or children in care, it has required a critical incident to overcome cultural barriers to data sharing and prompt support from central government. As these incidents are rare in the business regulatory sector, overcoming these cultural barriers will be more difficult. The sanctions for breach of data protection laws were considered disproportionate.
- 4.11 The full research report is available on the BRDO website. Overall the recommendations from the research include:
- a duty to share data;
 - improved guidance on the need to share data and legal position;
 - review of the legal powers to share data; and
 - a national data sharing strategy including publication of regulatory data catalogues.

Better Business Compliance Partnerships

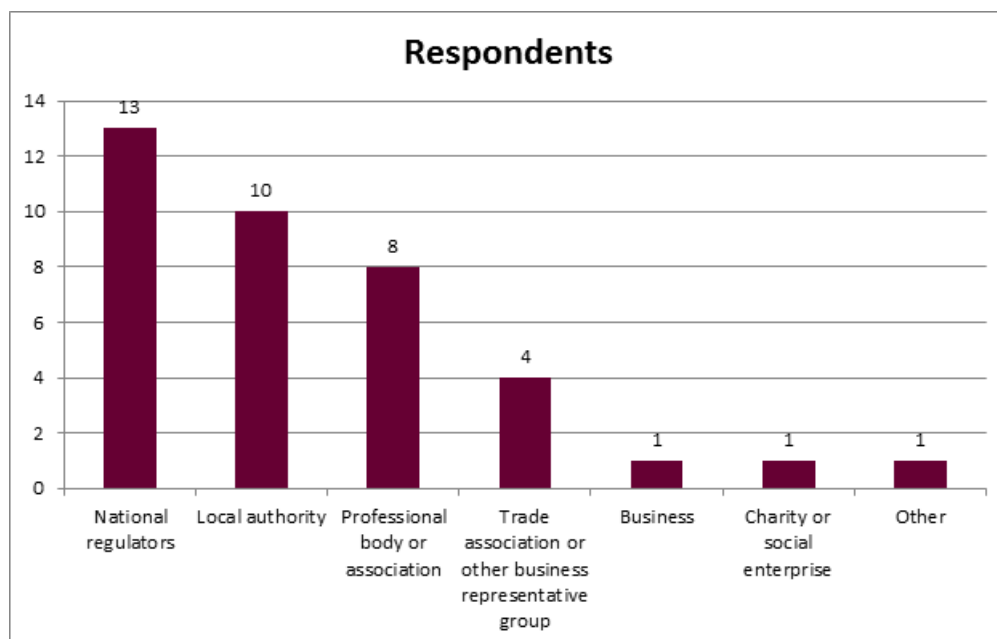
- 4.12 On 13 October 2014 the Government launched 'Better Business Compliance Partnerships' (BBCP), a series of pilots operating across five local authority areas, that are developing new ways of joint working within current constraints between local and national agencies in order to tackle illicit or hidden economic activity. The pilots are led by local authorities, with support from Cabinet Office, Home Office, HMRC, and BRDO.

- 4.13 The partnerships aim to develop and trial new methods of working between agencies, including new ways of sharing resources, expertise, or responsibilities of their officers. The partnerships are beginning to identify the legal, cultural and operational barriers that prevent effective data sharing, and are exploring what legislative or procedural changes might be made.
- 4.14 An evaluation of the partnerships will be undertaken, which should identify barriers to information sharing. BRDO will continue to work with the partnerships, and following the evaluation, will assist to develop policy solutions.

5. Next steps

- 5.1 This consultation, and the wider project including the IRIS pilot and research project, indicate that regulators are keen to share data where it is appropriate to do so, and business sees benefits of such sharing in terms of reducing burden and delivering earned recognition. However, regulators are not as able to share data as often as they might like. This means that benefits are not being realised for regulators and for the businesses they regulate.
- 5.2 Government is keen to dispel myths around data sharing and establish clarity for regulators. Government also recognises that the DPA is sometimes misunderstood and that regulators need clarity on its operation. To this end, BRDO will work with the ICO to develop guidance on the DPA, specifically tailored to the needs of regulators. This will help regulators to better understand the framework established by the DPA and use it as a means of enabling data sharing rather than as a prohibition. BRDO and the Information Commissioner's Office will work together to consider any other initiatives, which may assist regulators in this regard.
- 5.3 Consideration will be given to the need for practical tools to assist regulators to share data in a cost-effective manner, such as developing template data sharing agreements to get regulators started with data sharing initiatives with minimal need for resources. This will help to incentivise regulators to share data by reducing the time and resource needed to establish data sharing arrangements.
- 5.4 BRDO will also consider how to maximise the potential benefits of IRIS on the basis of the scoping work commissioned from HSL.
- 5.5 The research by the University of Cambridge will assist Government to assess the practical implementation of the Code, and help to determine what initiatives can be taken to further assist regulators to meet their obligations under the Code.
- 5.6 BRDO will continue to work with Cabinet Office to identify and act upon common findings of the consultation and the partnerships. The partnerships will continue beyond March 2015 in order to develop the proposed solutions to barriers to information sharing.

Annex A: Respondents to the consultation (includes workshop participants)



*Graph includes written submissions only

Association of Accounting Technicians
 Belfast City Council, Building Control Service
 Birmingham City Council
 British Retail Consortium
 Central England Trading Standards Authorities
 Charity Commission
 Charnwood Borough Council
 Chartered Institute of Environmental Health
 Chartered Institute of Legal Executives (CILEX) and ILEX Professional Standards Limited
 Civil Aviation Authority
 Claims Management Regulation Unit
 Companies House
 Cornwall Council
 Coventry City Council
 Department for Environment, Food and Rural Affairs
 Department of Enterprise, Trade and Investment Northern Ireland
 Devon and Somerset Trading Standards Service
 Driving Standards Agency
 East Hertfordshire Council
 English Heritage
 Federation of Small Business
 Financial Conduct Authority
 Food and Drink Federation
 Food Standards Agency
 Forum of Private Business
 Gambling Commission
 Gloucestershire County Council
 Groceries Code Adjudicator

Hampshire Fire and Rescue Service
Health and Safety Executive
Home Retail Group
Homes and Communities Agency
Human Tissue Authority
Information Commissioner's Office
Insolvency Service
Intellectual Property Office
Legal Services Board
Leicestershire County Council
Leicestershire Fire and Rescue Service
Local Government Association
London Borough of Hammersmith and Fulham, Environmental Health Service Group
London Borough of Richmond upon Thames - Trading Standards
London Fire Brigade
Marine Management Organisation
Monitor
National Casino Forum
National Farmers Union
National Federation of Meat and Food Traders
National Measurement Office
National Trading Standards Board and the Association of Chief Trading Standards Officers
North West Leicestershire District Council
Office for Nuclear Regulation
Office for Standards in Education
Office of the Senior Traffic Commissioner
Oxfordshire County Council Fire and Rescue Service
Prudential Regulation Authority
Royal Borough of Kensington and Chelsea, Environmental Health Services Group
Security Industry Authority
Solicitors Regulation Authority
Staffordshire County Council
The Gibraltar Betting and Gaming Association
The Groceries Code Adjudicator
The Pensions Regulator
The UK Cards Association
Trading Standards Institute
Trading Standards South East
Wales Heads of Environmental Health Group
Wales Heads of Trading Standards
Welsh Government - Department of Natural Resources and Food
Welsh Government – Department for Economy, Science and Transport
West Midlands Fire and Rescue Service
West Midlands Regulatory Services Partnership

Annex B: Regulators within scope of the Regulators' Code

Local Authorities

Specific local authority functions relating to environmental health, licensing, trading standards and fire safety are within scope of the Regulators' Code. A full list will be available shortly on the BRDO website.

National Regulators

Animal Health and Veterinary Laboratories Agency
Animals in Science Regulation Unit
British Hallmarking Council
Care Council for Wales
Care Quality Commission
Centre for Environment, Fisheries and Aquaculture Science, Fish Health Inspectorate
Charity Commission for England and Wales
Civil Aviation Authority⁹
Claims Management Regulation Unit
Coal Authority
Commission for Equality and Human Rights
Companies House
Companies House (Scotland)
Companies House (Northern Ireland)
Disclosure and Barring Service
Drinking Water Inspectorate
Driver and Vehicle Licensing Authority
Driving Standards Agency
Employment Agency and Standards Directorate
English Heritage
Environment Agency
Financial Conduct Authority
Financial Reporting Council
Fire and rescue authorities in England
Food and Environment Research Agency
Food Standards Agency
Forestry Commission
Gambling Commission
Gangmasters Licensing Authority
Groceries Code Adjudicator
Health and Safety Executive
Her Majesty's Revenue and Customs (so far as they relate to functions conferred by the Money Laundering Regulations 2007)
Highways Agency
Homes and Communities Agency
Human Fertilisation and Embryology Authority

⁹ Other than any regulatory function under:

- Part 4 of the Airports Act 1986
- Part 1 of the Transport Act 2000
- Part 1 of the Civil Aviation Act 2012
- The Airports (Ground Handling) Regulations 1997
- The Single European Sky (National Supervisory Authority) Regulations 2004
- The Single European Sky (Functions of the National Supervisory Authority) Regulations 2006

Human Tissue Authority
Information Commissioner¹⁰
Insolvency Service including Insolvency Practitioner Unit
Intellectual Property Office
Legal Services Board
Marine Management Organisation
Maritime and Coastguard Agency
Medicines and Healthcare Products Regulatory Agency
Monitor
National Counter Terrorism Security Office
National Measurement Office
Natural England
Natural Resources Body for Wales
Office for Fair Access
Office for Standards in Education, Children's Services and Skills
Office for Nuclear Regulation¹¹
Office of the Regulator of Community Interest Companies
Pensions Regulator
Prudential Regulation Authority
Regulator of Social Housing
Rural Payments Agency
Security Industry Authority
Sports Ground Safety Authority
Traffic Commissioners
The Birmingham Assay Office
The Edinburgh Assay Office
The London Assay Office
The Sheffield Assay Office
Trinity House Lighthouse Services
Vehicle and Operator Services Agency
Vehicle Certification Agency
Veterinary Medicines Directorate

Others

A professional body listed in Schedule 3 to the Money Laundering Regulations 2007

A person authorised by the Homes and Communities Agency to carry out functions pursuant to sections 201, 202 and 203 of the Housing and Regeneration Act 2008

A person authorised by the Secretary of State under section 457 of the Companies Act 2006 for the purposes of section 456 of that Act

A body designated by the Secretary of State for the purposes of section 1252 of the Companies Act 2006

¹⁰ Other than any regulatory function under the Freedom of Information Act 2000.

¹¹ Other than any regulatory function exercised under or by virtue of:

- Section 2 of or Schedule 1 to the Nuclear Installations Act 1965
- The Import of Goods (Control) Order 1954
- The Nuclear Industries Security Regulations 2003
- Regulations 4 and 5 of the Uranium Enrichment Technology (Prohibition on Disclosure) Regulations 2004

© Crown copyright 2015

You may re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence. Visit www.nationalarchives.gov.uk/doc/open-government-licence, write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email psi@nationalarchives.gsi.gov.uk.

This publication is also available on our website at:
<https://www.gov.uk/government/organisations/better-regulation-delivery-office>

Any enquiries regarding this publication should be sent to:

Better Regulation Delivery Office
Department for Business, Innovation and Skills
Lower Ground Floor
Victoria Square House
Victoria Square
Birmingham
B2 4AJ

Tel: 0121 345 1200

If you require this publication in an alternative format, email consultation@brdo.bis.gsi.gov.uk, or call 0121 345 1200.

URN: BIS/15/211