DEPARTMENT FOR BUSINESS INNOVATION & SKILLS' CONSULTATION ON DATA SHARING FOR NON-ECONOMIC REGULATORS

A RESPONSE BY

THE CHARTERED INSTITUTE OF LEGAL EXECUTIVES

AND

ILEX PROFESSIONAL STANDARDS LIMITED

DATE: JULY 2014

Introduction

1. This response represents the joint views of The Chartered Institute of Legal Executives (CILEx), a professional body representing 22,000 qualified and trainee Fellows and ILEX Professional Standards Limited (IPS), the regulatory body for members of CILEx. CILEx is an Approved Regulator under the Legal Services Act 2007 (LSA) and Fellows are authorised persons under the LSA.

2. The consultation was separately considered by CILEx and IPS. The outcomes of those respective considerations were exchanged and with no significant difference of opinion between the two organisations, a joint response is tendered. For the purposes of this response, 'we' is used to mean both CILEx and IPS unless the context indicates otherwise.

3. Although CILEx and IPS recognise the benefits of sharing data with other regulatory organisations we remain cautious to the potential risks associated with data sharing which would have to be carefully managed, in order to remain within ethical and legal boundaries.

Personal data

Question 1: Should personal data be shared? If so, for what purpose?

4. The consultation paper proposes the sharing of information through a large scale data sharing arrangement with other regulators. All the regulators need to consider the legal implications for the sharing of data on a large scale basis. The capacity to share information is subject to a number of legal constraints which go beyond the requirements of the Data Protection Act (DPA). For example, there may well be other considerations such as specific statutory prohibitions on sharing, copyright restrictions or a duty of confidence that may affect the ability to share personal data. A duty of confidence may be stated, or it may be implied by the content of the information or because it was collected

in circumstances where confidentiality is expected – medical or disciplinary information.

5. The DPA distinguishes personal data from sensitive data. The latter being defined as:

(a) the racial or ethnic origin of the data subject,

(b) his/her political opinions,

(c) his/her religious beliefs or other beliefs of a similar nature,

(d) whether s/he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his/her physical or mental health or condition,

(f) his/her sexual life,

(g) the commission or alleged commission by him or her of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

6. The processing of sensitive data must only be carried out in accordance with Schedule 3 of the DPA. This is the most sensitive type of data an organisation can hold about an individual. At present IPS only regulates individual members of CILEx, therefore all information held about members is considered to be personal data which is highly sensitive. Such sharing of sensitive data may be seen to contravene the Data Protection Act 1998 (DPA). We believe that sensitive data should only be shared with the express permission of the person it concerns as per the DPA.

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?

7. As a regulator and a membership body we have the ability to share personal data of members only in certain circumstances. Moreover, we would only share this data in accordance with the principles of the DPA.

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.

8. We do not believe that any personal data should be freely shared between regulators without any specific objectives for that data. This is especially relevant to highly sensitive personal data such as an individual's ethnic background, political opinions, religious beliefs, health, sexual health and criminal records.

9. The Consultation paper does not distinguish personal data from sensitive data. The sharing of sensitive data must comply with Schedule 3 of the DPA, and any proposed sharing of personal data must have regard to the Data Protection principles outlined in schedule 3 to the DPA.

Question 4: Do regulators consider data regarding sole traders to be personal data?

10. We consider data regarding sole traders to be personal data as it includes personal details such as a person's home address and contact details. Moreover, the DPA defines personal data as:

"personal data" means data which relate to a living individual who can be identified—

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual[1].

The above definition of personal data would include data held on sole traders if from the personal data (and other information held) a sole trader can be identified.

Question 5a: Should fact based standard data be shared? If so, for what purpose?

11. Fact based standard data is basic information about a business which is readily available on sites such as companies house website, business directories and the internet, therefore the sharing of this information poses no problem for IPS and CILEx.

12. If, however, information from the fact based data leads to the identifying of personal data defined above, the principles of the DPA would operate.

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?

13. As previously stated, we have the ability to share personal data of members only in certain circumstances. As the consultation paper suggests at paragraph 2.7 much of fact based data would fall outside the definition of personal data. It follows that we are not legally constrained to share fact based data. However, we do not actively share this data with others.

Question 5c: Are there any circumstances in which fact based standard data should not be shared?

14. See paragraph 13 of this consultation response.

[1] Section 1 of the data Protection Act 1998

Fact based specialist data

Question 6a: Should fact based specialist data be shared? If so, for what purpose?

15. Fact based specialist data relates to detailed and specialised information about a business' activity. This may be seen as sensitive information from a business perspective, and having their data and process information widely shared amongst regulators may jeopardise their trade secrets and provide and advantage to their competitor(s). Therefore some businesses may feel uncomfortable for this data to be shared with other regulators and may object to it.

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?

16. We do not hold any fact based data about businesses as CILEx members are generally employed in entities regulated by other regulators.

Question 6c: Are there any circumstances in which fact based specialist data should not be shared?

17. We cannot comment on this as we do not hold any fact based specialist data about any businesses.

License Data

Question 7a: Should licence data be shared? If so, for what purpose?

18. We cannot comment on this as we do not hold any licence data about any businesses as we do not license businesses.

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?

19. We cannot comment on this as we do not hold any licence data about any businesses.

Question 7c: Are there any circumstances in which licence data should not be shared?

20. We cannot comment on this as we do not hold any licence data about any businesses.

Compliance data supplied by business

Question 8a: Should this type of compliance data be shared? If so, for what purpose?

21. We believe that there are benefits of sharing compliance data as this will reduce duplication of work for both the business and the regulator(s). However the risks associated with the data sharing have to be appropriately managed in order to ensure that the compliance data is not misused

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?

22. We cannot comment on this as we do not hold any compliance data from any businesses as we do not regulate entities.

Question 8c: Are there any circumstances in which this type of compliance data should not be shared?

23. We cannot comment on this as we do not hold any compliance data from any businesses as we do not regulate entities.

Data voluntarily supplied by business

Question 9a: Should this type of data be shared? If so, for what purpose?

22. A business may sometimes choose to supply data to its regulator(s) voluntarily. We believe that if a business voluntarily supplies data, this should only be shared if the business provides express permission for this to be done or if there are legitimate regulatory reasons for doing so.

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?

24. We cannot comment on this as we do not hold any voluntary data from any businesses as we do not regulate entities.

Question 9c: Are there any circumstances in this type of data should not be shared?

23. We cannot comment on this as we do not hold any voluntary data from any businesses as we do not regulate entities.

Inspections results and analysis

Question 10a: Should inspection results and analysis be shared? If so, for what purpose, and what benefits might result?

24. Regulators record the results of inspections and other activities they carry out on business premises and hold these as part of compliance records for the business. At present IPS does not regulate entities, however if inspection results and analysis were to be shared between regulators then this should be done carefully with the appropriate safeguards in place.

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?

25. We cannot comment on this as we do not hold any form of inspection results or analysis of businesses as we do not regulate entities.

Question 10c: Are there any circumstances in which inspection results or analysis should not be shared?

26. We cannot comment on this as we do not hold any form of inspection results or analysis of businesses as we do not regulate entities.

Ongoing investigations

Question 11a: Should the existence of ongoing investigations be shared? If so, for what purpose?

27. We believe that existence of ongoing investigations should only be shared if there is a connection between the individual being investigated and the organisation requesting the information. The test to provide the information would be whether there is a legitimate regulatory reason to do so?

Question 11b: Should details of ongoing investigations be shared? If so, for what purpose?

28. Sharing the details of ongoing investigations may affect the outcome of the inquiry and compromise IPS' position. Therefore prior to the conclusion of the investigation, IPS would not disclose details of the existing investigation unless there were legitimate regulatory reasons to do so.

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?

29. We would only share details of ongoing investigation data in certain circumstances.

Question 11d: Are there any circumstances in which the existence and/or details of ongoing investigations should not be shared?

30. Situations where the sharing of investigation data would jeopardise the investigation.

Complaints data

Question 12a: Should complaints data be shared? If so, for what purpose?

31. 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?

32. IPS has the rights to publish anonymous complaints data. If the data concerns individuals, again the question is the whether there's a legitimate regulatory reason.

Question 12c: Are there any circumstances in which complaints data should not be shared?

33. No, we cannot contemplate any circumstances where generalised complaints data should not be shared.

Enforcement action

Question 13a: Should enforcement action data be shared? If so, for what purpose, and how much detail should be shared?

34. We feel that there is no harm in sharing general enforcement action data which is published on the regulators website. However if in-depth information is required then the organisation asking for the information should write to the regulator to make the specific request and detail the reasons for the request.

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?

35. We have the right to publish the enforcement action data on our website.

Question 13c: Are there any circumstances in which enforcement action data should not be shared?

36. No, we cannot contemplate any circumstances where complaints data should not be shared.

Question 14a: Other than those listed above, are there any other types of data which regulators could share? If so, for what purpose?

37. At present we have no further data types which can be shared.

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?

38. No comment.

Question 14c: Are there any circumstances in which this information should not be shared?

39. No comment

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?

40. At present IPS will only share sensitive data on a case by case basis with another organisation if they have an involvement with the matter. The data is usually shared in writing and the purpose of sharing the data is to ensure that consumers are appropriately protected.

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.

41. IPS/CILEx has MoUs with LeO, OISC and CPS for the purposes of data sharing. However generally legal regulators are not sharing data amongst themselves on a regular basis. A regulators forum has been set up to address this issue. The regulators and the Ombudsman are in the process of drawing up a MoU on the sharing of consumer and disciplinary information. It was recognised that the MoU must be broad enough to cover everything that needs sharing.

Question 17: What are the consequences of this inability to share data? Please give details (for example, wasted time, additional costs).

42. There is a risk that failure to share data can compromise consumer protection and result in some regulatory duplication, but it is not a significant concern for IPS/CILEx currently.

Question 18: What prevents regulators from sharing data? Please be as specific as possible.

43. IPS as the regulator is responsible for the register of authorised practitioners, even though the register is compiled by CILEx. If IPS needs to publish information and there are legitimate regulatory reasons for doing so, then it will. IPS has to be more cautious about the power to release data on non-authorised persons who are members.

44. Another issue which may prevent organisations from sharing data is the potential breach to the DPA

Primary legislation

Question 19: Is a measure in primary legislation the most appropriate means of encouraging regulators to share data? Please give reasons for your answer.

45. We believe that parliamentary scrutiny of legislation would be useful for a measure of this sort, particularly as it interacts with DPA and Freedom of Information Act 2000. Although we do understand that there will be significant difficulties in getting legislation that covers appropriately all the different organisations and powers which would be affected.

Data sharing as best practice

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.

46. The government has stated in the consultation paper that it may encourage regulators to share data by introducing the concept of best practice. This route is more favourable to IPS and CILEx, as it allows regulators flexibility to share data which they deem appropriate and in line with the DPA.

Single point of registration

Question 21: Do you have any views as to whether a single point of registration would be desirable?

47. Businesses which are regulated by multiple regulators may be required to provide the same information to each regulator, thereby causing duplication of information. The introduction of a single point of registration seems a desirable option but practically considering there would be the need to develop I.T. infrastructure to enable all the information to be inputted onto the system and then overcome legal and practical barriers to allow regulators to access data from a single point.

48. There are a number of risks that will arise from multiplicity of sensitive information being held in one place by a body with no ownership of the data and confused accountabilities. These risks would need to be assessed prior to the introduction of a single point of registration.

Question 22: Other than the options outlined above, is there any other means by which data sharing could be encouraged?

47. No comment.

Which regulators should be included?

Question 23: Are there any regulators listed in Annex A which should be excluded or others which should be included? Please give reasons for your answer.

48. No comment.

Safeguards

Question 25: Under what circumstances would data sharing warrant the inclusion of safeguards, and how could this be achieved?

49. There should be certain safeguards in place when sensitive personal information is shared with other regulators. Access to the data should be adequately protected and only a limited number of individuals should have the rights to access this information. The fewer individuals who have access to data means it will be less likely for the data to be compromised.

Question 26: Under what circumstances would the imposition of sanctions be appropriate?

50. Sanctions should only be imposed if data has been misused on purpose or if a regulator has been reckless with data on a number of occasions. An appropriate sanction would be to fine the organisation, as removing them from the list of organisations would mean information could not be shared by or with them, which would undermine the point of having the data sharing requirement. There are also private law alternatives where the persons or organisations affected by the breach can sue the regulator.

Monitoring

Question 27: Should the sharing of data be monitored? If so, to what extent?

51. It would be prudent for the sharing of data to be monitored as this would be an additional safeguard and ensure that all data is better protected. It would not be advisable to have sensitive data managed by an independent body with dubious accountability. This would inevitably increase regulatory complexity and cost and BIS should be looking at clarifying the powers and constraints affecting regulators who need to share information in the public interest, rather than inventing a new regulatory enforcement regime.

Question 28: Who should be responsible for monitoring the sharing of data?

52. The sharing of the data should be monitored by jointly by all regulators as they are the owners of the data.