ICAEW
REPRESENTATION 110/21

DATA - A NEW DIRECTION

Issued 19 November 2021

ICAEW welcomes the opportunity to comment on the: *Data: a new direction* consultation published by Department for Digital, Culture, Media & Sport on 10 September 2021, a copy of which is available from this link.

We agree that data is increasingly important for economic growth and wider benefits to society. A good regulatory regime is essential if the full benefits are to be reaped, including through innovative use of data such as AI.

The existing regime rightly seeks to promote public trust and is largely sound. In general, we believe that practical difficulties arising can best be addressed through regulatory interventions (eg clear guidance and education) or, where appropriate, the courts rather than change in legislation, and that Parliament should extend the powers and responsibilities of ICO if necessary for that purpose.

As noted in our response (Rep 94/21) to the recent consultation on *Reforming the Framework for Better Regulation*, it is important that powerful regulators are subject to ongoing and meaningful Parliamentary oversight and this applies to ICO, particularly if its powers are increased.

ICAEW is a world-leading professional body established under a Royal Charter to serve the public interest. In pursuit of its vision of a world of strong economies, ICAEW works with governments, regulators and businesses and it leads, connects, supports and regulates more than 157,800 chartered accountant members in over 147 countries. ICAEW members work in all types of private and public organisations, including public practice firms, and are trained to provide clarity and rigour and apply the highest professional, technical and ethical standards.

ICAEW
Chartered Accountants' Hall Moorgate Place London EC2R 6EA UK
T +44 (0)20 7920 8100 F +44 (0)20 7920 0547 icaew.com

The Institute of Chartered Accountants in England and Wales (ICAEW) incorporated by Royal Charter (RC000246)
Registered office: Chartered Accountants' Hall Moorgate Place London EC2R 6EA UK

KEY POINTS

ICAEW'S EXPERIENCE OF THE REGIME

1. Our response draws on our own experience of the data protection regime and on feedback from our member firms, including large global firms. Some of our firms are heavy users of data and provide advisory services involving personal data to a variety of UK and multinational businesses.

THE IMPORTANCE OF TRUST

2. The Ministerial Forward states that protection of people's data must be at the heart of the UK's regime and that without public trust the other objectives cannot be met.
3. We agree. In a free society, public trust is crucial. Without it, individuals may be reluctant voluntarily to disclose the personal data which is often the essential raw material from which products and services are developed.
4. This means that individuals should be able to understand what their data is being used for, or at least trust that it will only be used in ways that would reasonably be expected.
5. The existing regime seeks to promote trust and we believe it is largely sound.
6. Trust can be dented by personal experience (eg exposure to fraud from data breaches) or eroded through seemingly ineffective yet intrusive mechanisms (eg cookie consents). We therefore fully support initiatives such as this which seek to identify and address any shortcomings in the regime.

NEED FOR CHANGE IN THE REGULATIONS?

Balance between prescription and principles or guidance

7. The data protection legislation and regulations are lengthy and, in some respects, prescriptive, but the regime is built around key principles (fairness, transparency etc), which is appropriate given its broad application to nearly all businesses and personal data of the public at large.
8. We note that it is for business and other users of data such as government to win and maintain the trust of the public through behaving in a trustworthy way. A principles-based approach is helpful in that respect as the principles can serve to educate both business and the public.
9. In our view, the current regime already strikes a reasonable balance between prescription and principles and the most productive way to improve it will, with a couple of exceptions, be through reform of the regulatory approach rather than through legislative change. Specifically, we believe that the current regime is not always well understood and that the ICO could provide more definitive guidance in certain areas. Even if prescriptive, ICO's regulatory guidance can be made in a flexible way to address concerns that arise in specified circumstances and promptly changed if necessary. If ICO's powers or objectives need to be changed to allow this, we would support that.

Stability in regulation

10. Business and wider society has, for the most part, become used to the current regime. An enormous amount of work was required to comply with the regulations when they were new, including the design and introduction of compliance processes. But that work has largely been done, precedents have been and continue to be established and, while there is room for improvement, there is better understanding of the principles behind the regulations and how to adhere to them.

11. There is a real risk that substantial change will result in another wave of compliance costs which is not merited by the potential gains. The burden of 'regulatory churn' should not be underestimated, a point we highlighted in our response to the Reforming the Framework for Better Regulation consultation noted above.
12. Further, various elements of the regime are interlinked and the relationship between them can be complex. There is a substantial risk that changing the balance in one area will have unintended consequences in others.

International considerations

13. The Ministerial forward refers to the 'UK's status as a global hub for the free and responsible flow of personal data' and we support this ambition.
14. However, to achieve it, government should consider further the issues highlighted by the ICO in its response to the consultation. The UK cannot operate in isolation in a global business environment, regardless of Brexit.
15. In practice, the UK's regime will need to conform to international norms or additional burdens to business may result (eg complying with more than one regime on similar matters or being unable to access markets). We also believe that it is important for the UK to retain 'adequacy' for the purposes of data transfers with the EU.
16. As the current legislation meets international (including EU) norms, this is a reason to keep legislative change to a minimum and to consider whether there are other ways to address practical difficulties that arise.

Risk-based approach

17. The regime impacts such a range of activity in society that it cannot meet its general objectives by prescribing rules covering every possible circumstance. In many respects the current regime is a risk-based one (eg impact assessments and breach reporting) and we support this approach.
18. However, business often welcomes the clarity and certainty that comes from a prescriptive approach. A consistent approach on similar issues can help public understanding and trust. Assessing risks (with related work on policies, monitoring etc) can be burdensome for business and sometimes a regulator may be in a better position to assess whether risks of general application are acceptable than individual businesses.
19. It would be helpful if the ICO could provide guidance that is sufficiently definitive in relevant circumstances. Regulators may be reluctant to take any risks themselves (eg by defining what are 'low risk' activities and in what ways a low risk business might avoid compliance work necessary for higher risk businesses), so it is also important that Parliament retains good oversight so that the advantages of a risk-based approach materialise in practice.

Role of the regulator

20. In many respects we agree with ICO's response to the consultation. It has produced some excellent guidance and thought leadership. The papers on AI produced with the Turing Institute, for instance, strike us as being very helpful in promoting understanding of the difficult issues involved – understanding that will prove essential for public trust as use of AI increases.
21. We believe, however, that there is scope for ICO to provide more definitive guidance and consultation advice to reduce any ambiguities or uncertainties that arise in specialist areas or, more simply, to help 'low risk' businesses minimise resource on compliance activity. It

could also help increase understanding of how the rules apply in specific contexts. For instance, it might provide guidance on research (see further below).

Artificial intelligence and innovation

22. We agree that use of data, including through AI, is helping businesses to innovate and we are pleased to see the Government's focus on this. This is a developing area where it is essential to retain public trust.
23. The note on *Explaining Decisions made with AI* of ICO and Alan Turing Institute is helpful in explaining the current regime and the balances that need to be struck by relevant businesses. For the time being, we believe that the regulatory regime strikes the right balance and it would be premature to reduce safeguards on how decisions about individuals are taken through AI.
24. We do see potential for de-regulating in some areas, but only alongside growth in maturity of this technology and public trust in it. In the meantime, Parliament should retain decision making powers on changes involving important matters of principle and the regulator should continue to consult and engage stakeholders to ensure that the regulators and legislators remain informed of relevant developments.
25. Government and ICO should also monitor practice elsewhere and seek to assess levels of public trust in case there is a need for strengthening rather than relaxing the regime on AI.

Costs versus benefits analysis

26. We understand that the 'Data: a new direction, Analysis of expected impact' is a starting point and will be developed further. However, as it stands, we do not consider that the data and assumptions on which the analysis is based are of sufficient quality to form any reliable conclusions. Of particular concern, is the expectation in paragraph 69 of a switch to SCCs if EC adequacy status is lost. This will not necessarily be the case; if the EC specifically determines that changes to UK GDPR have reduced the UK data protection regime to a position where there is no longer an adequate level of protection, it could become very difficult for EEA exporters to identify any appropriate safeguards to deploy alongside SCCs to rectify the situation, thereby invalidating the use of SCCs as a transfer mechanism. This would create a significant deterrent against EEA data exports to the UK, resulting in a loss of adequacy impact far higher than the analysis estimates.

ANSWERS TO SPECIFIC QUESTIONS

27. The consultation is wide-ranging and we are responding selectively to the specific questions, by subject heading rather than individual questions, as noted below.

CHAPTER 1 – Reducing barriers to responsible innovation

Questions 1.2 - Research purposes

28. We suggest that most of the issues raised could be addressed through guidance rather than legislative change. For instance, guidance could help the relevant audience navigate the disparate and complex parts of the legislation related to research, without the legislation itself being redrafted for that audience.
29. If there are areas that are unclear in the particular context (eg the status of relevant recitals to UK GDPR) and ICO is not currently empowered to clarify through issuing definitive guidance, an alternative might be to extend its powers.

30. If, as proposed, the special status of research in UK GDPR is to be re-enforced through the legislation, it will be necessary to provide, and justify, a formal definition and we think this could be challenging.

31. Scientific research is not the preserve of any given predetermined group of people such as universities, other educational establishments or charities. It may be done in the public interest but also serve other objectives (eg university funding may be linked to research or universities may have commercial ventures with the private sector). Even defining what is in the 'public interest' is no easy task (eg see ICAEW's paper on 'acting in the public interest'). Neither are some of the risks of abuse of data lessened merely because the data was provided in the name of research. Risk of bias (eg when AI is involved) may arise in the research context too.

32. While UK GDPR contains specific provisions for research, it nevertheless requires researchers to respect the key principles protecting personal data of individuals. It is important that this continues to be the case so that room for substantial change on this issue may be limited.

33. As an alternative, guidance from the ICO might be targeted at particular circumstances (eg type of researcher and use of data envisaged, how individuals' rights are protected) in a way that would be difficult to achieve through legislation. Guidance provided to researchers on relevant matters, such as anonymisation, may also help other users of data (by analogy). Deciding whether data is 'personal data' is an important matter relevant to all.

34. The ICO has developed leading expertise on what constitutes (or therefore does not constitute) personal data. We believe that its experience should be leveraged by other UK regulators looking at related issues (eg FCA's consideration of 'big data') and that government and regulators should adopt a consistent approach on overlapping issues.

Questions 1.3 - Further processing

35. In general, we think it unobjectionable that data controllers should be required to 'take into account' the various factors identified in Article 6(4) of UK GDPR and we support the idea that data users (businesses and government) should think about the possible impact of their actions on those they supposedly serve (eg customers, the public).

36. Diluting these requirements simply tilts the balance away from protection of the rights of individuals and could reduce public trust and potentially make it more challenging to offer services in the EEA as the purpose limitation is an important part of the current EU regime.

37. It is unclear how relaxing the rules to make it easier for data to be re-used by a different data controller would protect the legitimate rights of individuals. For instance, use should always be in line with the reasonable expectations of those providing the data.

38. We find it difficult to envisage how rules would be crafted to address all potential concerns without becoming unwieldy.

39. One exception to the above is that further processing to anonymise personal data should always be permitted (subject to appropriate technical and organisational safeguards). At present it is not always possible to identify an Article 9 condition that permits further processing to anonymise special category personal data.

Questions 1.4 - Legitimate interests

40. We agree that some businesses mistakenly tend to think first of consent when identifying the lawful basis for processing personal data, despite alternative and often superior lawful bases being available.

41. There is scope for improving understanding and reliance on the 'legitimate interest' basis, but we are not convinced that an 'exhaustive list' is the best approach. The list of public tasks under the 2018 Act would need further consideration in this context as some are potentially broad in scope. It is important that the basis is not too broad, because trust in the regime may be damaged if legitimate interest strays beyond use that an individual would reasonably expect.
42. Rather than having a list where there is no balancing test, we suggest that ICO could substantially change its current guidance to provide detailed examples (which would include a balancing test) that organisations can adopt for their own legitimate interest assessments.
43. This would retain the principle that legitimate interests must be balanced against the impact on individuals, but potentially reduce uncertainty and also help businesses to understand how rights of individuals may be balanced with business objectives.
44. ICO should have much of the know-how to do this because data controllers are already required to state what are their legitimate interests for processing in their privacy statements. If, as seems likely, there is a good degree of commonality, then either businesses currently are getting it wrong (a problem in itself), or there is scope for a more standard approach. Rather than repeating the relevant legitimate interest assessments, businesses could then refer to the guidance, so reducing work all round (except for ICO).
45. The regulator would need to seek feedback from individuals, business and other interested bodies to ensure that it continues to strike the right balance and addresses concerns promptly when they arise. Parliament should retain good oversight and be ready to step in if it seems this approach is having undesired consequences. Addressing the issue through guidance rather than legislation means that it will be easier to evolve over time and take account of fast-paced technological change.

Questions 1.5 - AI and Machine learning

46. The consultation paper alludes to the fact that AI is impacted by various regulations, not just data protection. It is important that government looks at this holistically so that any resultant regulatory regime is a coherent whole. If reform of the data protection regime is intended to simplify or reduce burdens, then it is difficult to see why government would choose to use this regulation as tool for wider objectives that might be achieved by other means. However, where other regulators consider matters pertaining to personal data (including when data ceases to be personal data, eg through anonymisation) and bias in AI, we believe that ICO should have a leading role to play given its expertise on the issues.
47. We believe that government should organise feedback groups to enable further consideration and discussion and include other regulators tasked with relevant duties in (eg on bias and equality).
48. So far as UK GDPR is concerned, we are not currently convinced that it is impeding the responsible development and application of AI in a disproportionate way. While the concept of 'fair' processing may not be defined, Article 22 specifically addresses what appears to be the key consideration in this context.
49. In response to Q1.5.17, we note that Article 22 does not prevent automated decision making but gives individuals the right to human intervention and challenge when automated decisions have been made. We do not think this an unreasonable approach at this stage of the development of AI and it is anyway restricted to 'solely' automated processing having a 'legal or similarly significant effect'. The importance of Article 22 was recently illustrated by the public outcry at the inappropriateness of sole reliance on algorithms when determining children's examination results.

50. The benefits of regulation should not be overlooked. Absent provision for transparency, some businesses are likely to seek to exploit AI to their own advantage without due concern for the legitimate interests of their customers (ie the public).
51. ICO has provided some useful guidance on the subject and we believe that issues arising could continue to be addressed through guidance for the time being.

Questions 1.6 - Data Minimisation and Anonymisation

52. We agree that more robust guidance from ICO on what constitutes anonymised data would be helpful (both for research purposes and more generally). If the principles apparent from the preamble to UK GDPR, international guidance on the issue and EU court cases are generally accepted, it is difficult to see why changes in regulation should be required.

Questions 1.7 - Innovative Data Sharing Solutions

53. We agree that there is potential for independent third parties to provide forms of assurance to individuals about how their data is used. This may make individuals more comfortable about agreeing to share their data.
54. However, we are unclear whether government proposes that protections afforded to individuals should be relaxed for such third parties. As the paper observes, data intermediaries are subject to the same data regulation requirements as others. We think that they should be. They potentially present at least as great a risk to data security and rights to privacy as any other business in possession of our data.
55. Even where one business has a 'legitimate interest' to process personal data provided to it, its legitimate interest should not include sharing that data with others except in accordance with the regulations (including consent).
56. Government should also consider carefully the risks involved in concentrating personal data in a few bodies, or widening access to data held by any given body, both of which can increase opportunities or incentives for fraud, including identity theft.

CHAPTER 2 – Reducing burdens on business and delivering better outcomes

57. The regime is sometimes perceived to tend towards a 'box-ticking' and one size fits all approach that can have a disproportionate impact. This is contrary to the 'principles' based approach underlying the regime that encourages data controllers to think about the implications of proposed data processing.
58. We therefore support a focus on outcomes and pursuit of a proportionate approach to reduce costs while maintaining protections for individuals and current processes that already operate effectively.
59. We are not in a position to comment on all the various alternatives raised in the paper (eg depending on whether or not the privacy management programmes are taken forward) or on all relevant matters arising but hope that our general observations will be useful.
60. Our overall conclusion is that we would encourage government to make changes through a more nuanced approach to enforcement and guidance from ICO rather than by wholesale changes to the regulations, where possible.

Questions 2.2 - Reform of the Accountability Framework

Accountability based on privacy management programmes

61. It is unclear why government believes that introducing a new privacy management programme requirement would reduce burdens on business. It appears to impose additional requirements on how businesses should comply and increases scope for differing practices (and uncertainty that goes with that).
62. Many of the suggested processes are in effect carried out by some businesses currently as a matter of good practice and to assist with compliance, but others are not compelled to do so.
63. The bulk of data protection requirements would remain and the suggested deregulation that might be made as a result seems modest by comparison.
64. The distinction between the proposed privacy management programme and the current requirements for organisations to have appropriate data protection policies to ensure compliance with the legislation strikes us as a fine one, albeit we have not considered the Australian, Singaporean etc examples cited. Any international comparison would need to look at the laws and regulation of the jurisdiction concerned as a whole, not just one element of them. If the result would be to substantially weaken protections for individuals, then the potential impact on international transfers noted in our introduction arise.
65. Replacing a list of something you currently have to do under the regulations with something you should think about doing does not necessarily reduce work (as noted in para 182 of the consultation paper) or result in better outcomes. Smaller businesses may benefit most from having a list of requirements for the certainty it provides. Otherwise a business might do work that others might consider was unnecessary or not do something that others would expect to be done, with risk of subsequent criticism or sanctions. It would often be good practice to document the basis on which judgement has been exercised (eg in case of regulatory intervention) which in itself requires work (even in relation to matters judged low risk).
66. If the intention is to tighten up regulation (eg improve consistency as noted in para 183 of the paper), we would like better to understand exactly what outcomes (as opposed to outputs) government seeks to achieve by this.
67. If data management programmes are to be required, government should consider the potential impact on small business. This is already a concern under the current regime, but aspects of it are proportionate eg by size (250 employee threshold for elements of the risk assessment regime) or risk (eg data protection officers). Imposing new requirements that would apply to all businesses does not appear to be serving the interests of small businesses.

Data protection officers

68. Feedback suggests that some organisations, particularly at the smaller end of the scale, do not find it easy to appoint data protection officers and we would support targeted reforms to alleviate this concern.
69. The regime has advantages, including meaning that a consistent approach is adopted by relevant businesses. This can enhance the sharing of data and increase levels of trust and understanding. It can be helpful for the public as well as in business-to-business interactions for there to be an identified individual designated for the purpose of receiving data protection complaints or queries etc. at relevant organisations. The requirements are targeted towards large organisations or those carrying out specified activities, but even small businesses can benefit from having a person identified within the business as being responsible for various data protection matters, eg handling potential data breaches (which need to be carefully

managed from the wider business risk perspective). We do not, therefore, believe the requirements should be removed entirely.

70. However, the current requirements are more prescriptive than might be desirable regarding the qualifications and experience required by a DPO and we would support modification of the regime in that respect. For instance, the regime assumes that an individual will have a high level of data protection training and advise an organisation when, in fact, there may be better ways for an organisation to achieve these outcomes. This having been said, the experience of our members is that privacy related issues can be more readily resolved when businesses have a knowledgeable DPO.

Data protection impact assessments

71. We believe that impact assessments serve a useful purpose and are an effective tool. Even if there were to be no formal requirement to complete a DPIA, it would be beneficial for businesses to carry out similar assessments of their high risk processing activities to reduce risk of inappropriate use of data (and breach of the regulations).

72. Again, if the requirements are considered overly prescriptive, we suggest that this might best be addressed through revised guidance. The current guidance is lengthy and could perhaps be simplified, but we think further detail of government intentions is required before moving entirely away from this regime. For instance, which, if any of the areas currently identified as being of high risk (eg biometrics) does government think are not high risk?

Prior consultation requirements

73. We speculate that the prior consultation requirements may be little used because data controllers find ways to mitigate risks, so obviating the need for consultation or abandon plans if risks cannot be mitigated. In cases of doubt, there may be a concern that the regulator will err on the side of caution and businesses might prefer to take the risk, even if the risk is exacerbated by possible sanctions for failing to consult.

74. We believe that regulators should welcome interaction with those that they regulate and offer assistance and guidance regarding compliance. We are not convinced that threatening business with additional sanctions for failing to consult is the best way to promote this.

75. On balance, we agree that the requirement should be replaced with a right to consult, so that businesses can easily approach ICO for advice/views etc. ICO should nevertheless be alert to data processing developments that it considers to be ‘high risk’ and be prepared to use its powers to investigate where appropriate. Government should also consider whether ICO could take a more proactive role providing education to business, eg on emerging risks or new developments in the markets. It will need to be appropriately resourced to perform these functions effectively.

Record keeping

76. We agree that the record of processing activities can be onerous to implement and maintain. However, they are now embedded in many organisations and businesses may have contractual arrangements requiring them to maintain such records.

77. The consultation proposes that the current arrangements be replaced with a more flexible approach as part of a risk management programme. We suggest that government consider, as an alternative, introducing a degree of flexibility to the current arrangements eg through guidance. For instance, the amount of work involved depends in part on the granularity with which processing activities are defined and the approach on this already varies considerably between different businesses.

78. The consultation notes that the requirements in effect call for replication of information contained in other records. If the requirements could be made more consistent there might be scope for one record to serve more than one purpose. For instance, in straightforward cases, there might be scope for a privacy statement also to serve (or largely serve) as the relevant record.

79. Article 30 of UK GDPR requires organisations to maintain a Record of Processing Activities, including categorisation of the data and the purpose of processing. Paragraph 39 of Part 4 of Schedule 1 to the 2018 Act sets out the requirements for an 'Appropriate Policy Document' concerning use of Special Category and criminal conviction data. This appears to be duplicative, and government might consider removing this requirement from the Act or ICO might provide guidance to make clear that the record of processing activities may be a suitable policy document for the purposes of the Act.

Breach reporting requirements

80. The regulations require reporting unless 'unlikely to result in a risk…', but the ICO guidance makes clear that an assessment of materiality is required (and the self-assessment tool refers to 'high risk to individuals' rights and freedoms').

81. It is possible that overreporting occurs because people are following the letter of the regulations rather than ICO guidance, in which case there would be something to be said for better alignment between law or regulation.

82. Other explanations are possible, including that people are likely to err on the side of caution when failure to report is itself punishable with very substantial fines and that there are too many areas of uncertainty (in which case further guidance should be considered).

83. In any event, we believe that further guidance to help organisations assess whether or not to report would be helpful.

Voluntary undertakings process

84. We are not in a position to comment on the Singapore regime. If the regime is to favour organisations that 'engage with ICO' it will be necessary for ICO to be resourced to engage with all potential users similarly to ensure that the process is fair, and transparency will be required. Government should also consider other ways to encourage the 'regulated' to work constructively with their regulator (and vice versa).

Questions 2.3 - Subject access requests

85. We agree that requests can be time consuming and take up significant levels of resource and would welcome targeted reform of this aspect of the regime.

86. As noted in the paper, before 2018 there was a £10 fee for data access requests; we believe that this did deter many frivolous requests. On balance we would support the reintroduction of the right (but not obligation) for data controllers to charge a nominal fee to deter such requests. Some safeguards might be required for those who could not afford even a nominal fee.

87. Such a fee would not cover the costs of work typically involved in handling many requests or address certain other concerns, so it is not a complete answer to the problem.

88. One concern is where requests involve confidential business information or personal information of other individuals. It can be very time consuming to weigh up potentially competing interests and information may need to be manually redacted or individuals contacted to give consent, all of which is time consuming and can lead to disputes. Another concern (noted in the consultation) is that requests may lead to disclosure of (or expectation

of disclosure of) opinions about the data subject for purposes of litigation and which ought more properly be obtained through court disclosure procedures.

89. We are not convinced that a 'cost ceiling' approach would address these sorts of concern or otherwise be the best solution. The context is different from Freedom of Information Requests. That approach could reward the disorganised (who cannot economically find data) or inflated costs might be assigned. In either case, it could lead to a weakening of data subjects' ability to exercise their rights. Also, what might be appropriate for one kind of business might not be appropriate for another.

90. An alternative might be to build upon the existing provisions regarding vexatious requests. This recognises that requests may be refused if likely to cause a disproportionate or unjustifiable level of disruption. We believe that ICO should be empowered (if it is not already) and required to apply this in a way that would address legitimate concerns of data controllers on these matters. For instance, it might require the data subject to identify why the data subject seeks information containing personal data (eg opinions) of other individuals to ascertain whether the work required to provide it would be proportionate for the purpose.

91. See also our comments (Rep 01/20) on the 4 December draft Rights of Access Guidance consultation.

92. Providing additional legislative exemptions could also assist. The "Confidential references" exemption could be extended to cover other confidential opinions. In addition, personal data processed in the context of a statutory audit or other professional services provided under a duty of confidentiality to a client should be provided a similar degree of exemption as legal professional privilege. Practice in other EU countries such as Germany and Ireland might be informative in this context.

Questions 2.4 - Privacy and electronic communications

93. It is important that the concerns raised by the consultation on these issues are addressed because, apart from anything else, multiple cookie requests etc undermine confidence and trust in the wider data protection regime.

94. The prevalence of requests for consents is damaging. In practice it means users have little choice but to accept. They may then be accepting use that, if they considered carefully, they would not have accepted.

95. We agree that the definition of 'essential purposes' should be broadened if necessary to cover use for site analytics and, potentially, technical faults, ie the sort of thing that would reasonably expected by users. This would help reduce the number of, essentially, pointless cookie requests.

96. There would be a logic in conforming this regime to some degree with 'legitimate interests', but some aspects of cookies and electronic communications give rise to specific concerns so we do not believe that is a complete answer. There will be times when users should always be asked for consent even if a data controller considers that use falls within the legitimate interest basis.

97. Even where users may accept (by consent or otherwise) that their data may be used for marketing purposes, there may still be balances to be drawn. For example, those who consent to use of location data by a retailer might expect that to result in the retailer knowing where they live (or work) and making inferences on what they might like to buy from that. But they might not expect the data to be combined with the location data of others they have come into contact with (eg to enable the retailer to build up a social profile and make recommendations based on preferences of acquaintances).

98. Users also need to be aware when automated decision making is involved (with attendant risks, biases, and other shortcomings) and empowered to overrule it if needed.

99. These are complex issues that depend upon understanding what sort of use is made of personal data at any given time and the degree to which the public are concerned about that use (or would be concerned if they thought about it). ICO might conduct further (and continuous) research to identify areas of concern to the public at any given time to help government and other understand what usage is of most (or least) concern and work with the private sector to help promote good practice.

Questions 2.5 - Use of personal data for purposes of democratic government

100. Those directly involved in making this response do not believe that the rules around political parties, elected representatives etc should be relaxed at all.

CHAPTER 3 – Boosting trade and reducing barriers to trade flows

101. Please see our introductory comments on international aspects and costs v benefits.

CHAPTER 4 – Delivering better public services

102. We recognise the enormous potential benefits from data for government and the wider economy. It is fundamental to the future of the economy to get the right building blocks in place to enable the realisation of these benefits. The role of data in underpinning current AI technologies emphasises the importance of the topic.

103. We believe that greater emphasis should be placed on the benefits to citizens and the public interest, and the need to develop a citizen-centric approach to data to build trust. Trust is highly context specific, and citizens' acceptance of data uses will vary depending on what the government is trying to do. Therefore, further consideration should be given to how best to incorporate the priorities and views of citizens into the data protection regime and ensuring sufficient transparency and confidence in the purpose and objectives of government use of data.

104. In terms of the wider economy, the government is the biggest owner or user of data in the country and therefore can play a leadership role, being an exemplar in good practice, sharing its experience, and being at the forefront of thinking about how to enable safe, secure and trusted data sharing. There are also some specific types of support that it can give, such as funding innovations in data access across sectors.

105. However, to have the best chance of success, the data protection regime needs to link to many other elements as data does not exist in isolation. Data fundamentals, for example, will be improved by wider digitalisation of processes. Trust will benefit from strong cyber security. Transformation requires a range of cultural, organisational and people change.

106. We want individuals and business to have the ability to only give information once to government, but also for the data protection regime to operate smoothly to protect the use of such data from misuse (accidental or otherwise) by government departments who might not ordinarily/legally have access to that data.

107. For instance, in the context of company data, we support the recent initiatives aimed at allowing companies to file once with government, digital filing (with tagging) and greater checks of information filed. We believe that these are positive steps that will increase the value of the data held on the Company register and assist in preventing economic crime. However, the data protection regime needs to ensure that the information made publicly available on the register is used effectively, data submitted under a file once approach must

be appropriately safeguarded; and the data targeted to best combat economic crime. It is also important that wider implications are considered, for instance whether such data might be used for unfair competitive advantage by overseas companies or expose individuals to risk.

CHAPTER 5 – Reform of the Information Commissioner's Office

108. We agree with many of the objectives outlined in the consultation, including the central objective to uphold data rights of individuals (which is why we have the legislation in the first place). We also agree that recourse should be focused on addressing the most serious threats to public trust.

109. Some of the questions overlap with questions raised in the consultation on The Framework for Better Regulation referred to at the beginning of this response. These include the degree to which ICO should be set express objectives eg to have regard to economic growth, competition and innovation and the proposed promotion of sandboxes as a regulatory device.

110. We would like to see these questions addressed in a consolidated way so that lessons learned in one area are applied in another. We do not comment further here therefore but refer to our response to the earlier consultation, much of which is relevant in this context too. In particular, we believe that ICO should comply with the principles of good regulation and other aspects of the Regulator's Code.

111. We agree with ICO that its independence from Government must be preserved. There are elements of the proposals (eg direction from the Secretary of State) that are concerning in that respect. We suggested in our response to the earlier consultation that an independent body should be established to help Parliament hold regulators to account and we believe that such a body would be helpful in this context too.

Questions 5.5 - Codes of practice and guidance

112. We agree that provision of clear guidance is essential in this area of regulation and generally support the idea that ICO should be supported by expert panels etc.

113. We agree that there should be Parliamentary oversight of ICO which should include consideration of its guidance in novel areas resulting in changes to rights of individuals or obligations on business, but we are not able to comment on how this is best achieved at this stage, save to note that the independence of ICO should be maintained, which means that any extension of the powers of the Secretary of State need to be considered carefully.

Questions 5.6 - Complaints

114. We do not agree with the proposals on complaints. The ICO should be resourced to deal with complaints made to it. The proposal simply pushes the burden onto business, creating more bureaucracy and cost to business as a result (need to log, monitor, publish) and this does not belong in what is styled as a deregulatory initiative.

115. As an alternative, we suggest that ICO could include in its guidance on complaints a requirement that complainants seek to resolve the matter with the relevant business first and provide evidence that they have done so. It could then simply reject complaints that do not meet the minimum expected standards, and it can keep such logs of complaints as it sees fit.

116. If businesses are not responding appropriately to complaints, then the ICO should be investigating this, not leaving it to businesses to create logs.

117. Businesses will face many types of complaint and there comes a point when they need to improve or will go out of business, in theory at least. Government should consider to what extent it wishes to seek to replace (or duplicate) natural market forces with regulation.