RESPONSE TO DCMS CONSULTATION DATA REFORM UK GBPR

Response by Rosemary Jay individual responder.

DATA REFORM

I INTRODUCTION

1. The consultation is clearly the product of detailed work and consideration. It represents a major effort to re-imagine and modernize the UK position. As such its aims are admirable. Clearly the central policy aim, to foster and encourage innovation, while balanced with the protection of personal data, is one to which most would subscribe. The consultation includes a number of helpful and practical proposals. However the wide scope means that it can be difficult to tease out the useful and/or significant elements. In some cases the impact of the proposals is not clear and in some places it is difficult to work out how different aspects of the proposals fit together. In addition there are some regrettable omissions.

2. The most striking omission is the absence of any assessment of the proposals on the UK's adequacy finding from the EU. This is very significant for the UK, also bearing in mind that countries other than the EU have adequacy rules and any EU finding would potentially be persuasive in other jurisdictions. While it is assumed this was a deliberate decision by the authors, presumably on the basis that such impact would fall to be assessed at a later stage, it may mean that many who read the consultation paper will assume that none of these proposals will have a potential impact on adequacy. This is far from the reality. The proposals to remove the DPO role, DPIAs and central records of processing; the proposed changes to the position and independence of the ICO; the potential changes to the compatibility regime; the potential removal of the Article 22 rights; the proposal to diminish the test of fairness in relation to AI, and the cookie proposals all raise potentially serious problems with the adequacy assessment. As a result the failure to evaluate and discuss the adequacy risks attached to different parts of the proposed changes means an essential element of the relevant policy consideration is missing in every aspect of the proposal.

3. Secondly there is little clarity over which parts of the proposals would impact on the law enforcement and security provisions in the Data Protection Act 2018 (DPA 2018). Although the Introduction states that the changes would improve the functionality of these aspects of the law the only changes which appear to impact are related to the role and powers of the Information Commissioner (ICO) and it is not clear how these changes would be of any benefit to the law enforcement or security functions.

4. In addition the consultation strays into some specialist and difficult areas where there are multiple other considerations involved and which would be better served by specific, targeted discussions addressing the complexities of those areas. This is particularly the case in respect of the sections on AI and on the regulation of cookies.

Overall it would have been helpful for the consultation to more positively highlight the value of data protection, particularly as enabling individual choice and supporting the rights of individuals to respect for their autonomy and the privacy of personal data.

It is to be hoped that at the next stage the proposals can be winnowed down to a number of clearly expressed practical changes which will improve the data protection regime in ways which meet the policy aims to encourage and support innovation without risking the importance of the UK's adequacy finding.

II REMOVING BARRIERS TO RESPONSIBLE INNOVATION

OVERVIEW

While I have made every effort to comment on the proposals individually, the proposals in this section are in broad, general terms so I have found it difficult to comment at the level of specificity and detail that these potentially radical changes would merit. Inevitably I have had to speculate as to how the proposals could take shape or work in practice.

Overall I am inclined to the view that some of these points are misconceived. It is not apparent why the issue of compatibility has been given prominence. In the 1981 Treaty (now modernized Convention 108 – Convention 108+) and the OECD Guidelines the concept of compatibility matters because it is the primary basis on which the acceptability of new processing is assessed. Since Directive 95/46 introduced the concept of specific grounds for processing, the concept of compatibility has become less relevant. The restrictions on new uses of data derive primarily from the grounds for processing and, as such, the relationship with the data subject. Controllers who seek to use data for new purposes now focus on their notices and contracts rather than the issue of compatibility.

GENERAL INTRODUCTION

5. As far as it appears from the Introduction the Government has pinpointed only limited problems with the current regime. These appear to be:

   (a) Some definitions are unclear.

   (b) Some rules, such as research, are difficult to navigate leading to a risk adverse approach

   (c) There is some report that uncertainty about the legal grounds to use has led to an over-reliance on consent

   These are not ground-breaking challenges. For example, many of the definitions are derived from previous law and the lack of clarity is often around the way they apply to new technologies, which is hardly a fault of the definitions. Amending them may be equivalent to removing the last carriage of the train because that is the one where there are always most fatalities in the event of a crash.

6. It further states that the recitals cause problems, as follows.

"[recitals] offer information about the intended scope, purpose or effects of the law, which are valuable for understanding how it should operate in practice. The recitals do not however, form part of the operative text in legal terms and their contents are not fully mirrored in the main body of the UK GDPR. Consequently organisations may be reluctant to adopt an interpretation of the legislation that relies on a reading of the recitals that is not supported by a an appropriately literal reading of the operative text, even if such an interpretation is likely to be in keeping with the intent of the law."

7. Recitals are potentially problematic. They are meant to give assistance to interpretation. They cannot have normative effect i.e. if the legislative text does not reflect the recital, the recital is of no effect[1]. They should use "non-mandatory language" but not "desires, intentions or declaration". The recitals in the GDPR do not universally meet these standards. In places they remain the sad embodiment of the hopes and (failed) dreams of lobbyists.

8. The paper appears to contemplate that elements of Recital 50 should be imported into the UK GDPR (it seems to be suggested that the statement that a new legal ground for processing is not required for compatible processing might be added to UK law). There must be stringent assessment of this proposal as it is clear that elements of that recital do not meet the test of being of assistance to interpretation but instead seek to insinuate a normative provision directly contrary to the terms of the legislative text. Any prudent organization would be well advised to steer clear of relying on such a provision. In view of the potential importance of this I have looked at Recital 50 in some more detail. The analysis is included in this response in Annex 1.

   The analysis concludes that the proposal that this odd sentence in Recital 50, cited above, be imported into UK law is fatally flawed. It would undermine the UK regime by importing an unjustified liberty to carry out new processing without proper assessment and ensuring the application of adequate grounds for processing in the particular case. As the grounds for processing are a fundamental concept in the GDPR this would amount to a significant undermining of the UK regime.

III RESEARCH

9. The research provisions are complex and scattered in the GDPR and bringing them together would be useful. The inclusion of Recital 159 seems unnecessary but may be useful to some people. However see below on the proposal to single out specific recitals for inclusion.

10. It is not clear from the paper whether there is any evidence that controllers are struggling to find grounds for processing for research. It states the Government is seeking further evidence which suggests it has a paucity so far.

---

[1] *Casa Fleischhandel* Case C-215/88. See also the Guide to the drafting of Union legislation 2014. For a fuller discussion of the issues around recitals see *Data Protection Law and Practice* 5the Edition published Sweet and Maxwell. Author Rosemary Jay

11. The decision to single out and incorporate specific recitals is potentially problematic. It creates an ambiguity in that those recitals which are not specifically included may be regarded as irrelevant. It creates an uncertainty in the UK approach overall to the interpretation of the GDPR which might impact on views on adequacy. This is exacerbated if only those recitals which support a "UK preferred" reading of the GDPR are singled out and even more so if those recitals would not be regarded as reliable guides applying the considerations canvassed in Annex 1 in relation to Recital 50.

IV RE-USE

12. This section addresses two separate issues:

    (a) Research issues and

    (b) Compatibility and further use issues generally

    My reading of the issues and questions being posed is set out below. It is noted however that the questions set out at the end of the section in the paper do not cover quite the same ground and include a question which does not appear to have been addressed in the discussion section. This is added in italics below with a note to that effect.

V RESEARCH PROPOSALS

13. In summary these are:

- Clarifying that consent to research may be provided in broad terms
- Making explicit that the further processing of personal data for research purposes is always compatible with the original purpose of collection
- Making explicit that the further processing of personal data for research purposes is always lawful under Article 6(1) UK GDPR
- Providing a disproportionate effort exemption for controllers who wish to reuse personal data for research purpose from the obligation to notify individuals of that purpose

VI COMPATIBILITY AND FURTHER USE ISSUES GENERALLY – PROPOSALS

14. In summary these are:

- Irrespective of the purpose of the processing or the purpose of collection, to permit the re-use of personal data for a new, incompatible purpose where the processing safeguards an important public interest. Irrationally (and arguably giving a misleading impression) this also covers where the data subject has "reconsented" to the new purpose which is a wholly different fact

set and should be clearly differentiated. In such a case the controller can rely on the consent and the issue of compatibility does not arise.[2]

- "Clarify"[3] when a different data controller than the controller which originally obtained the personal data is permitted to process personal data for a new and incompatible purposes. Irrationally (and arguably giving a misleading impression) this includes a reference to historical, scientific or statistical research purposes which should be covered in a separate point as there is a presumption that such processing will be compatible. As with the point above this is irrespective of the purpose of the processing or the purpose of collection.

- "Clarify" that processing for a new purpose, always has a lawful basis for processing when it is "based on law that safeguards an important public interest". Note that this is not the same test proposed above which refer to cases where the processing "safeguards an important public interest" with no reference to the law or to safeguards. Again, irrationally (and arguably giving a misleading impression) this includes reference to when the data subject has consented initially or has re-consented. These should be clearly differentiated. In such cases the controller can rely on the consent of the data subject and the issue of compatibility does not arise.

- *Should the Government "clarify" when further processing may occur when the original lawful ground was consent?*

15. These proposals are extremely confusing. It is difficult to have any real sense of what is being proposed. The conflation of research with non-research further processing is misleading. The proposals need to be clearly re-drafted and set out concisely what is being proposed in each case. In particular the cases where there is a statutory presumption of compatibility need to be distinguished from those where there is no such presumption, therefore re-use for research purposes should be clearly distinguished and it made clear the second section does not cover re-use for research. Further, the use of the broad, generic term "public interest" needs to be addressed – there is no generic test of public interest and it needs to be considered and applied in specific contexts; re-consent or consent situations should be distinguished from those where there is no consent or no other ground.

VII RESEARCH PROPOSALS

16. Research may cover a wide range of activities, from clinical research on the one hand, which may be invasive or have significant health implications, right through to epidemiological research carried out remotely on historic datasets, taking in applied research, commercial research etc.. along the way. The problem of how to deal with data processing for research and balance competing interests has

[2] Note that this appears to have been derived from the wording of Recital 50. This is not helpful and it would be far clearer if the different situations were clearly differentiated

[3] The use of the term "clarify" suggests that it is an accurate statement of the law that new and incompatible purposes can be adopted without the standard compliance safeguards in certain cases outside the exemptions and the research area. However the GDPR only appears to permit that where the new processing is subject to a legal obligation, which would qualify for an exemption in any case.

exercised data protection legislators since the 1970s. As with any data processing activity, the starting point is that the law applies to the activity unless: a) the application of the law causes problems for the pursuit of the activity, which cannot be addressed by normal compliance activity and b) there is a countervailing public interest in the activity being able to continue which means that the rigour of the law should give way to the extent necessary and appropriate to meet the defined public interest.

17. It cannot be asserted that there is always a public interest in all research, or that, to the extent there is a public interest, it is always of the same nature or importance. Research into the hair colour of women who buy stiletto heels in not on a par with research into the causes of diabetes.

18. Accordingly there is no justification for removing the rigour of the law from *all* research and a more appropriate and balanced option needs to be considered.

Further, given the importance of the application of the safeguard conditions and potential for claiming exemptions for research, it is critically important that the boundaries of what is or is not research remain clear. This is an important part of the obligation of accountability of data controllers. Research is a separate purpose from the fulfilment of a service or contract. It may be that there is a need to refine the boundaries between activities such as analytics from research to clarify those boundaries but the distinction should remain.

19. Proposed - clarifying that consent to research may be provided in broad terms

As is noted in this paper, DP consents and grounds for processing intersect with other research provisions, for example there are strict rules about consent for clinical research and such research must meet rigorous tests of consent. Such consent cannot be given in broad terms. The GDPR contemplates the possibility of broad consent but under the GDPR Recital 33 links the possibility of broad consents for scientific research in keeping with ethical standards. This is a sensible and balanced approach which has much to recommend it. **It there is to be provision for consents for research to be given in general terms it should be clearly limited to cases of this nature or others which have a clear public interest justification. The provisions must also take account of other legal and ethical constraints applicable to the research.**

20. In practical terms consents are often given on the basis of implied undertakings, in other words the controller sets out specific assurances such as confidentiality etc. The level of consent is also intimately linked to the nature and potential intrusiveness of the data.

21. Given these constraints it is recommended that any clarification that consent may be given in broad terms includes considerations of proportionality, vulnerability of the data subjects and contextual considerations. Further the burden of proving consent must remain on the data controller.

22. Proposed - Making explicit that the further processing of personal data for research purposes is always compatible with the original purpose of collection

As is noted in the paper, the UK GDPR imposes safeguarding provisions in relation to research. Art.5 provides specifically that the further processing of personal data for research purposes in accord with the safeguarding conditions is not to be considered incompatible with the original purpose. While this introduces what might be regarded as a deeming provision, it does not do away with the obligations of fairness and transparency in relation to the further processing. It is not therefore clear what the proposed clarification would achieve, unless it is proposed to remove the application of the safeguard provisions or the fairness or transparency provisions as well? This would be a serious and detrimental change and needs to be clarified.

23. Proposed - Making explicit that the further processing of personal data for research purposes is always lawful under Article 6(1) UK GDPR

The paper states "the operative text [of the GDPR] does not state explicitly that further use of data for research purposes passes the lawfulness test under Article 6 of the UK GDPR". This is not a terribly helpful statement as the text does not state anything about Article 6, either explicitly or implicitly. Article 5(1)(b) states that further processing for research is compatible with the original purpose but nothing about the grounds for processing. This is because the processing for the research purpose will be a processing for a new purpose and will therefore have to be evaluated by the controller for its compliance de novo. The fact it is deemed to be not incompatible is simply a threshold test. It does not mean that any other compliance requirements are met. Nor should it. It may be that this odd formulation of the question is derived from a reading of Recital 50 and the outlier sentence (the effect of which is analysed in Annex 1) about grounds for new purposes. As such it would be misconceived.

24. The proposal is flawed in that any new processing must meet one or more grounds in Article 6(1). There is no such thing as meeting 6(1) in abstract; an actual ground must be applicable. In the absence of consent or a legal mandate (assuming it cannot meet the contractual or vital interest tests as a matter of fact) the available potential grounds would likely be 6(1) e or 6(1)(f) depending on whether it was research by the public or private sector. However there are elements of balance/public interest tests in both and the research would have to pass those tests.

25. Proposed - Providing a disproportionate effort exemption for controllers who wish to reuse personal data for research purpose from the obligation to notify individuals of that purpose

The paper proposes this for cases which would otherwise fall into Article 13(3) where the controller intends to process for a new purpose which was not notified at the point of collection. This may well be too broadly framed. Given the growth of Big Data uses almost any data collected by anyone might be used in research at a later date and most privacy policies include some form of generic reference to research. Again we come back to the issue that research is not one category but covers a huge range of activity. If there is to be an exemption it should mirror that in Art.14(5)(b) so it imposes the same safeguards etc..

VIII COMPATIBILITY AND FURTHER USE ISSUES GENERALLY – PROPOSALS

26. The first proposal is :

- Irrespective of the purpose of the processing or the purpose of collection, it recommends permitting the re-use of personal data for a new purpose, including an incompatible purpose, where the processing safeguards an important public interest. Irrationally (and arguably giving a misleading impression) this also covers where the data subject has "reconsented" to the new purpose which is a wholly different fact set and should be clearly differentiated. In such a case the controller can rely on the consent and the issue of compatibility does not arise.

27. In responding to this point I have ignored the "consent /re-consent" issue as irrelevant. The core of the proposal is that, in all cases of new uses of data, any new purpose, compatible processing is "permitted". The words used in the Question Box refer to the processing "may be lawful". In the context of the UK GDPR this appears to have to mean that it is deemed to meet one or more of the grounds in Article 6(1). However, as noted earlier, it is not possible to have a deeming provision for Article 6(1) generally. Article 6(1) cannot be met in the abstract. These are questions of fact as discussed in Annex 1.

28. 28.First there is the question of principle in relation to compatible processing under the UK GDPR. As discussed earlier, if processing is compatible it passes the threshold test, so to speak, and the controller must then consider the other principles including the ground for processing. Assuming one applies, the controller must decide how to handle transparency and fairness. It is not apparent that this proposed reference to Article 6(1) adds anything of use.

29. Where the new processing is incompatible it "may be lawful" if it is "based on a law that safeguards an important public interest". This has two tests:

    (a) Based on a law – this seems to assume specific legislation and

    (b) The relevant law safeguards an important public interest.

30. It is not clear what "based on a law" means. It may mean mandated by a legal provision e.g. a mandatory duty to record disease occurrence or disclose information to the tax authorities etc… It may also include processing based on a discretionary power of a public body. In both cases the processing will have a basis in law. However, in relation to private sector bodies they are generally allowed to do anything which is not forbidden by the law so the words "based on law" have no clear meaning, save for the limited example of legally mandated processing. But where processing is mandated by law e.g. disclosures required by statute, there is almost certainly an exemption which will permit the processing /disclosure in any event. Accordingly it is difficult to give any clear meaning to the concept of "lawful processing " or processing being based on law. The question is also left hanging as to who decides what amounts to an "important public interest" and how is this weighted against the position of the individual data subject. All of these points need to be addressed before any useful commentary can be made.

31. Proposal - “Clarify” when a different data controller than the controller which originally obtained the personal data is permitted to process personal data for a new and incompatible purposes. Irrationally (and arguably giving a misleading impression) this includes a reference to historical, scientific or statistical research purposes which should be covered in a separate point as there is a presumption that such processing will be compatible. As with the point above this is irrespective of the purpose of the processing or the purpose of collection.

32. As above I have ignored the “consent/re-consent” issue. As far as it appears there is no ambiguity of the wording to clarify. If the aim is to change the UK GDPR so that a different controller can process for a new and incompatible purpose without going through the existing compliance requirements the effect would be to remove the purpose limitation principle from the UK GDPR. This would be an extraordinary and radical change. It would bring severely into issue the UK adequacy finding and also the UK’s position in respect of Convention 108+.

33. The factual situation described is that a new controller wishes to process an existing data set controlled by another controller, for a new purpose which is not compatible with the original purpose for which the data were collected and processed. Under the current regime the new controller has an obligation to comply with the principles and must assess the ground for processing, the quality of the data etc..the fairness of the proposed processing, how they are going to meet the transparency obligations and so on. They may need to carry out a DPIA (assuming these have not been abolished). The existing data controller must assess whether they can lawfully and fairly disclose the personal data to the new controller, and, if so, how they are going to do it. The purposes are incompatible so it is likely that, not only notice, but an opt-out or even a positive consent may be required. The parties may agree between themselves how it is to be done or the disclosing party may seek a warranty from the new party that all DP requirements are met, or the new party may negotiate for the disclosing party to fulfill the basic compliance requirements before disclosure. There is no explanation of how this in any way different from any other case where one controller wishes to disclose to another for a different and incompatible purpose. As noted above this proposal is perhaps the most radical in the paper. It effectively removes the purpose limitation and would create a significant gap between the UK regime and the EU regime.

34. Proposal - “Clarify” that processing for a new purpose, always has a lawful basis for processing when it is “based on law that safeguards an important public interest”. Note that this is the same test proposed above. Again, irrationally (and arguably giving a misleading impression) this includes reference to when the data subject has consented initially or has re-consented. These should be clearly differentiated. In such cases the controller can rely on the consent of the data subject and the issue of compatibility does not arise.

35. Article 6.4 provides that processing for a purpose other than the purpose of collection can be based on law which constitutes a necessary and proportionate measure in a democratic society to safeguards the objectives listed in Article 23(1). These are the list of public interests which can be protected by exemptions. The objective of the proposal could be achieved by referring to the exemptions in Schedule 1 Parts 1-4 DPA 2018 and permitting the processing for those purposes

subject to meeting the terms of the relevant exemption. It is difficult to see any other mechanism to meet the tests of necessity, proportionality and Article 23.

36. Question - Should the Government "clarify" when further processing may occur when the original lawful ground was consent.

37. It is not clear why the specific ground of consent is being raised here. Consent is one ground for processing; no better, no worse and no more powerful than any other. There is no legal barrier in the UK GDPR against further processing on another ground when consent was the original ground, albeit that, outside vital interest or legal compulsion, it may be difficult to satisfy the requirements of fairness etc. Consent may be part and parcel of an implicit or explicit agreement that the processing will be limited to the terms of the consent. But the same can be true of contractual terms. In such cases the move to process for another purpose on another ground (aside from vital interest or a mandatory legal ground) will be limited by the terms of the relationship and notices etc.. The question of whether there may be further processing which meets the DP standards may be fact-dependent, varying with the new purpose, the level of compatibility, the terms of the consent, the data involved etc… Without some detail on the nature of the proposal (as with so many other parts of this proposal) it is difficult to do other than query the justification for the proposal.

IX LEGITIMATE INTERESTS

38. The proposal is to add a list of processing activities which are deemed to be within the legitimate interest of the controller as an avoidance of doubt matter, excluding any processing relating to children. It is noted that two of the activities which are included in Recital 47 as being in the scope of legitimate interest, that is fraud prevention and direct marketing, are omitted, and it is recommended these be included in any list. Network security is included in Recital 49 and is generally accepted as a legitimate interest.

39. It seems that an assumption of legitimate interests is reasonable (a bit like the old registration or notification exemptions – processing widely accepted as low risk) however the categories proposed need to be re-examined. Overall the better approach may be to add a presumption of legitimacy which could be rebutted in specific cases, particularly in the case of internal business purposes. In relation to cookies this proposal seems nugatory and adds nothing to the impact of PECR and should be removed for the reasons set out below.

40. **Internal research and development** – Recital 48 recognises that the transfer of personal data within groups for admin purposes can be a legitimate interest however it gives no detail of what this covers other than the examples of processing employee or client data. In the proposal the admin purposes are different and appear to cover:

- Internal research and development;
- Business innovation aimed at improving services for customers.

41. These are two quite different purposes and the wording of both of the bullet points is broad. Internal research and development could cover anything, including potentially research and/or developments which are detrimental to data subjects' interests. This needs to be balanced by some level of safeguard. Equally the wording "business innovation aimed at improving services" is broad. I suspect I am not the only consumer who has found that "business innovation aimed at improving services" has been used as a basis for closing local bank branches and may look on the use of the terms with some suspicion. Given the breadth of the terms proposed I would suggest safeguards be attached for these purposes. In any event for all the proposed uses making it a rebuttable presumption of legitimate interest would be sensible.

42. **Cookies.** It is regrettable that cookies have been included in this section on legitimate interests without reference to the section of the paper covering PECR related issues, including the placing of cookies (see below). The two parts of the proposal in fact hang together: on the one hand that consent for some non-essntial cookies (analytic cookies) be no longer required; married with the proposal here that there should be a presumption that legitimate interest can be a legal basis for placing non-essential cookies.

43. The issue of the use and setting of cookies of various types raises complex issues (as noted later). It also has a serious impact on individual users. The road to make websites take responsibility for cookies and offer genuine choices has been long and wearisome. The indications are now that results are being delivered. More and more sites offer, if not an immediate option of "refuse all [non-essential] cookies" on the face of the site, at least a second stage "manage my preferences" which allows refusal of all. The cookies proposed to be allowed on the basis of legitimate interest are *not essential to the service* which means that they serve the interests of the setter only. If this enabled sites to set cookies with notice only this would be a major shift in the balance of rights between individuals and business with no benefit to individual data subjects.

44. However it is not at all clear how this would work in practice, given that the setter would have to give notice of the setting of the cookie according to Articles 13 and 14 and the user would have the right to opt-out under Article 21. Article 21(4) requires that the right to opt-out be brought to the attention of the data subject. So the UK GDPR would require notice and opt-out for these cookies in any event. It would no longer be possible for a website to state that by using the site consent was assumed or refer only to browser settings (which is actually unacceptable under the current law but persists nevertheless.) The practical effect might therefore be to strengthen the position of users who would have to be given an active opt out on the face of the site. Clearly this is not what is intended but is possibly a consequence of raising the cookie issue in this siloed manner.

45. It is recommended that all the PECR /cookies issues be addressed in one place. That any decision to change the current position take account of the ICO work on AdTech and ideally be deferred until the EU position on the ePrivacy legislation has been resolved. This will enable a full and detailed consultation on these issues.

X AI AND MACHINE LEARNING

46. There is an interesting discussion of the concept of fairness in this section which rather suggests that it is a term which has multiple meanings and may be misunderstood. I would take serious issue with this position. Fairness is a central concept in many areas of law. It is one of the first and clearest judgements that children learn to make. How you determine fairness and how it is applied in different contexts will vary. The examples given on Page 24 recognise those variables. However the basic concept of being fair remains constant. We have a pretty strong sense of when something is fair or unfair. It can be characterized as the "sniff test", (does something pass the sniff test? If it's a bit "iffy" it's probably unfair). Or as the elephant test, (it's hard to describe an elephant but you know one when you see it) and in various other colloquial ways. We need to distinguish the debates about how fairness applies in specific cases, such as AI development, from the fundamental obligation of fairness in processing.

47. As a matter of historical interest it is noted that the paper states (page 27)

"The concept of fairness was also originally understood as aking to transparency". It is not clear why this is stated. The concept of fairness has, to my knowledge and experience, always been focused on the way processing is carried out and the effect of the processing. As an example, the cases brought by the Data Protection Registrar in the 1990s in respect of the processing of personal data by credit reference agencies by automated systems were brought and argued on the basis of the fairness of the processing with no reference to transparency. There is a link between knowledge and fairness/expectation but fairness is a far broader, more encompassing requirement.

48. The specific questions posed are (in effect):

(a) Whether the legal obligations relating to fairness are clear when developing or deploying AI systems;

(b) Whether the concept of fairness in the DP regime in relation to AI is currently unclear

(c) What legislative regimes and associated regulators should play a role in assessment of fairness, especially outcomes, in AI context; and

(d) Whether the development of a substantive concept of outcome fairness only, so other aspects of fairness are not taken into account, in the DP regime (whether linked or not to other regimes) poses risks.

49. Legal obligations of fairness, including DP regime, in developing AI regimes

As a society we are still not agreed on the extent or application of obligations of fairness in the online world, yet the Internet has been with us since the 1980s. It is inevitable that in any developing field there will be different views about how aspects of the law apply, or should apply. We can see this in social media - where one person's freedom of expression is another's hurtful trolling; in the huge gap in perception of how we deal fairly with the trans issues; in every area of social

change and development. If the position were clear we would not have the inflorescence of thoughtful analysis and development referred to in Page 27 with the work being undertaken by UNESCO, the Council of Europe and others on ethics, fairness and AI. We need this thinking, this exploration of options and ides, this open-mindedness, to help us understand the challenges and the best ways forward to deal with AI. It is not an indicator of defeat but of active engagement with challenges we need to meet. This thoughtful engagement should be encouraged. So it is right to recognize that concepts of how fairness applies in AI are still being developed, both generally and in relation to the DP regime, but that is not a negative and does not argue for removing the obligation to be fair.

50. Relevant legislative regimes in relation to AI

As with other areas e.g. credit and consumer law, the regulation of medical practice and research, financial regulation, regulation of online behaviours to give a few examples, AI may be subject to, or at least intersect with, numerous regulatory regimes including DP. The fact that DP reaches into almost all areas of activity is an aspect of the DP regime which has grown with the development of computing power over the past 35 years. It is not specific to AI. It is a significant challenge for DP regulation in nearly all areas. In relation to AI which uses personal data (and much does not) the intersecting regimes may be dependent on the particular AI application under consideration, for example if the AI development is in the area of medical research or practice,, the supervisory regime and laws applicable to that field will intersect with the DP regime. It should be recognized that the common factor among AI application developments remains the DP regime. As such it is critical that the DP regime remains the central and main vehicle for the supervision of AI development which includes personal data. This will avoid regulatory fragmentation and help to deliver comparable treatment and consistency of approach. It will also foster the development of core expertise and help build reasonable and foreseeable outcomes across different sectors.

51. Whether the development of a substantive concept of outcome fairness only, so other aspects of fairness are not taken into account, in the DP regime (whether linked or not to other regimes) poses risks.

In effect this suggests that, where AI is being developed, the bulk of DP principles should be disapplied. It is not clear what “outcome fairness” consists of. If the data entered into an AI application is of uncertain quality, having been collected without due care, or has been unfairly gathered with the effect that potentially those affected by the outcome have no awareness of the use or say about being involved in the “outcome”, if the processing is biased and weights elements wrongly etc.. these will all affect an outcome. The unfairness runs all the way through the collection and use of the data.

52. However to the extent it suggests the disapplication of all the DP principles in the development of AI this would be a very high risk from an adequacy point of view. To effectively exempt the most significant developments in technology and social change from the principles designed to protect personal data from misuse would likely be perceived as abandoning the core obligations of DP. Leaving that aside, it is difficult to understand a logical justification for this suggestion. The purpose of the DP regime is to protect and support the position of individuals in relation to

their personal data: its collection; its accuracy; its dissemination; its use. The fact that fairness is a matter of debate and review in the development of a new field is not a reason to abandon it. Moreover I would submit that the points made in para.59 above on the importance of the DP regime acting as the common governing supervisory regime for development in this area is a critical consideration.

53. Building trustworthy AI systems and bias detection

Several of the questions posed here are mainly of fact for those using AI. The issues raised are broadly the same as those canvassed in the first section on research, re-use and compatibility and it would have been helpful if they had been considered together. AI appears to be simply a specific example of a wider question. On the specific question of whether the law should include an exemption to allow the use of personal data for AI development free from aspects of the DP regime I have not found it possible to comment. It would have to be clear how the potential development uses were to be defined, what kinds of data could be used, any safeguards and the DP provisions from which exemption would be provided.

54. On the further question of whether there should be an additional use in the list of uses deemed to be within legitimate interests to cover the use of personal data for AI purposes and/or an exemption for the use of special category personal data. It seems unarguable that it is important to ensure that AI systems do not deliver biased results which disadvantage particular groups. The issue of whether a consent requirement will undermine the representative nature of the group may well be a question of fact depending on the size and scale of the group, its demographic and the AI use.

55. It is unfortunate that the question of another deemed legitimate ground for processing is raised separately to the other possible purposes which might be deemed to be within legitimate interest. It would be helpful to discuss this issue as a whole not by reference to piecemeal proposals. It occurs to me that there must be a question as to whether this would legally take effect as an exemption because it excludes such processing from the requirement of the balancing test and as such should be evaluated bearing in mind the requirements of Article 23 UK GDPR. It is noted that this is proposed for special category personal data and it might be better to create an exemption applicable to all types of data subject to appropriate safeguards.

56. AI and data rights

In this section one proposal is to remove the Article 22 UK GDPR rights in relation to automated decision-making. The paper notes that this is a difficult question and seeks views. At the same time it puts forward a specific proposal from the Taskforce on Innovation, Growth and Regulatory Reform (Taskforce) that Article 22 should be completely repealed. It is not clear therefore how far this is meant to raise open questions and debate or how far the Taskforce position is being advanced. The Taskforce position appears to be that, as other DP rules apply (such as grounds for processing) the individual right to object can be removed. However the rights in relation to the impact of automated decision-making are individual rights, not part of the general regulatory regime. The existence of

individual rights in the DP regime is an important part of the whole. The rights reinforce a central tenet of the regime: that individuals should not become subservient to the activities and decisions of machines. I agree that Article 22 is not wholly clear; there is still a debate as to whether it operates as a prohibition or as a right of objection. It seems important to establish a stronger basis of evidence on how it applies and impacts before canvassing options for review.

57. Effectiveness of data tools and further potential provisions to ensure trust

As set out in paragraph 59 above, I consider that the DP regime needs to remain the core regulatory regime for developing the regulation of AI to enable innovation and build public trust. Spreading the regulatory supervision between different regulators would undermine trust in a generally applicable consistent approach. The ICO is a well-recognised and respected regulator in the digital sphere and is the obvious place for controllers and users to look for guidance and support. The willingness to consider additional specific provisions and tools for AI supervision to increase transparency and evaluate potential harms is an interesting one. I do not follow the suggestion at page 41 that inferred data is somehow exempt from disclosure (presumably on a subject access request) because it was created by the controller. An individual has the right to access the personal data held about them; it is still personal data held about them if it is inferred from other data. If this needs to be emphasized possibly it should be covered in ICO guidance or a code of conduct.

58. There are obviously resource issues in developing a fit-for-purpose approach to AI supervision. If the view is reached that specific obligations of algorithmic transparency are required these could be built out from the current FOIA regime. While that regime currently impacts primarily public sector bodies it could be extended and a hybrid function created which draws on aspects of DP regulation, such as audits and assessment, plus elements of the FOIA regime such as publication obligations and obligations to respond to specific enquiries. It might be necessary to limit individual rights of request for reasons of resource and to deter mischievous requests but the building blocks are already present in the ICO structure, legislation and skill sets.

59. Minimisation and anonymization

I have no comments on this section.

60. Intermediaries

I have no comments on this section.

XI REDUCING BURDENS ON BUSINESS PRIVACY MANAGEMENT PROGRAMMES

INTRODUCTION

61. The essence of the proposal is that a number of specific obligations set out in the UK GDPR will be repealed and replaced by a broad, generally applicable

obligation on all controllers to develop, maintain and comply with a new Privacy Management Programme (PMP). The obligations to be removed would be:

- Data protection impact assessments
- Consultation with the ICO in (the rare) cases that a DPIA shows that a high risk cannot be ameliorated but the controller wishes to go ahead with the processing in question
- Record keeping under Article 30.

There are other proposals in the same section (a change to breach reporting standards, amendments to the DPO regime and making the power to accept voluntary undertakings explicit for the ICO.) These are all brought under the general banner of "accountability" however the PMP is a specific proposed new obligation.

62. Overall I would suggest that data controllers could be offered a choice of using the existing tools or of choosing to adopt a PMP. Such a choice should be notified to the ICO and the party obliged to adopt the necessary internal policies and practices. The default would be the current rules but a controller could have the option to elect to adopt a PMP instead.

PMP

63. The adoption of policies, processes and practices to deliver compliance with legal requirements is a traditional compliance /standards model. As is noted in the paper, the UK GDPR already requires organisations to implement appropriate technical and organizational measures and be able to demonstrate compliance. DPIAs have developed as a tool from the original PIAs introduced in the 1990s in Canada and elsewhere. The ICO has been a major influence in the use and development of the tool. It is very much a UK initiative and it is now well-understood, well-used and there is a wealth of guidance and expertise on DPIAs available. The obligations to keep an accurate central record (effectively a Single Point of Truth) and to carry out DPIAs before new processing are specific requirements that are aimed at delivering accountability. The fact these are set out clearly and mandated is helpful to smaller organisations that have to find their way around the GDPR. In particular, over the years, I have found that the process of carrying out a DPIA is often an invaluable practical exercise for organisations. It makes the organization address the nature of the processing and often crystallises thinking around compliance issues. It is an invaluable tool for the DPO and those charged with compliance on the ground as a way of bringing issues to senior management. It is mandatory, structured and helps really focus issues. Particularly for medium sized organisations without the range of staff or expertise which big controllers have, the DPIA is one of the best and strongest compliance tools they have.

64. The obligation to maintain a proper central record is also a great tool for the ordinary controller. It means that all notices, access requests, retention schedules, audits etc.. can be checked against the central point which has to be maintained as up to date. It is practical, useable and easy to understand

65. The removal of these tools and replacement by a broad information management obligation would make no difference to large and sophisticated data controllers which have staff and resource and huge expertise available. Such organisations are likely to have sophisticated accountability systems in place already. The choice of a PMP rather than the use of the UK GDPR tools may offer them a helpful option in managing their compliance. However to remove these tools from the "ordinary" organization will be potentially a real detriment. There is no need to do this. As recommended it should be possible to offer flexible options to controllers to select the system that suits them best.

66. Removal of the DPO role

The requirement to appoint a DPO in certain cases is limited. Small local government bodies are excluded and organisations can save resource by sharing a DPO. Nevertheless most organisations have someone who holds a central role and acts as the point of reference. There seems no point in removing the role of the DPO which is now well-understood and utilized, and replacing it by a "suitable individual responsible for the privacy management programme".

67. Changes to breach reporting

There seems only a shade of difference between a breach being unlikely to result in a risk to rights and freedoms and a breach which causes some risk but where the risk to individuals is not material. I have no comment on the proposal.

68. Voluntary undertakings

The use of voluntary undertaking was common at the ICO during my time working there and I am not aware that there is any current barrier to accepting such undertakings under the current law. However I would seriously challenge the suggestion that such undertakings could only be taken where the organization can demonstrate historic proactive accountability e.g. by engagement with the ICO. The relevant consideration should be not historic actions but whether there is a credible basis to accept the undertaking in respect of future activity. A reference to historic accountability and working with the regulator may have the perverse incentive of encouraging controllers to "cosy up" to the regulator. This can be a surprising drain on the regulator's resources.

69. Prior consultation

This is not a provision used in the private sector to any extent. High-risk processing which cannot be mitigated but where the risk can be justified on public interest grounds is generally carried out in the public sector. I think this is the reason that few organizations approach the ICO under Article 36. There does not seem to be any problem associated with Article 36. However it is noted that the paper proposes for the ICO to create a list of "high risk processing". I would caution that attempts to define and list high risk processing effectively in the past never seem to have been successful. It can take a huge amount of time and effort to no real impact.

70. Subject access

I have no comments on this section.

XII PECR changes

71. In June 2020 Apple took steps to stop third party cookies tracking users see

    https://www.apple.com/uk/newsroom/2021/06/apple-advances-its-privacy-leadership-

    - with-ios-15-ipados-15-macos-monterey-and-watchos-8/

    As of September 2021 it was reported that only 21% of users had actually opted in to the use of tracking technologies. See report here:

    https://www.statista.com/statistics/1234634/app-tracking-transparency-opt-in-rate-worldwide/

72. This provides cogent evidence that users do not find tracking technologies acceptable. In the face of this it seems extraordinary that the DCMS is raising a question as to whether prior consent should be removed for all cookies. Given the overwhelming rejection of tracker cookies in the Apple experience it may seem at first sight surprising that cookie banners are not more universally used to reject cookies. However there are numerous reasons for that. The DCMS paper cites the use of "nudge" techniques . A study in 2020 by researchers at MIT CSAIL, Aarhus University and UCL concluded that under 12% of the most used management tools for cookie consent could be regarded as meeting the legal requirements for cookies and consent .

73. Despite this it seems to be the case that cookies are gradually becoming less and less effective. Users are blocking them by browsers, apparently increasingly on mobile devices, and as options become clearer e.g. "Decline All" on the face of the initial banner, more and more users are directly rejecting cookies.

74. Users may not like banners but it seems that they dislike being tracked even more and once it becomes a real open option to refuse, block or disable – they are taking those options. This is a significant development in consumer choice on the internet. The DCMS could lead the way on this. It could support the increased development of browser settings to block cookies, while recognizing that not all consumers have the technology or skills to use these techniques and at the same time outlaw the use of nudge techniques and require the simple choice of "Reject All" offered on the initial cookie banner. In doing so it would ride a wave of consumer choice and approval which is already growing to a tidal swell.

75. The topic of the use of cookies and their equivalents is complex as the CMA investigation into the decision by Google to stop using third party cookies on privacy grounds shows. Nevertheless there are clear signs that users are realizing the effect of cookies in tracking them and turning against the use of cookies. Over

the last few years the ICO has thrown light on the privacy problems involved in the use of AdTech (albeit slowed down by the pandemic pressures).

76. Specific proposals

(a) Remove consent for analytics.

In practical terms this would not appear to change the position for users unless all consents are removed. If users still have the right to reject/give consent to tracking cookies the users still have a consent/reject action to take. It does not simplify matters for consumers but is a lessening of current standards and therefore arguably a retrograde step. Analytics cookies collect user data – there is no question about that. There is also the odd potential outcome that, if legitimate interest is used as a processing basis, the controller will have to give notice and opt-out which means there is little difference in practical terms anyway.

(b) Removing cookie consent requirements in a range of other case.

This runs counter to the interests of users. Consumers are voting with their choices and actions against cookies and all the elements that non-necessary cookies entail in terms of collecting extraneous data on individuals. There is no justification for this in practical terms and it is a detrimental and retrograde step.

(c) Remove prior consent for all non-essential cookies

77. This is a surprising suggestion in relation to the governance of the online world. The policies being espoused in other areas, notably Online Harms, are to force companies to take responsibility for their actions, to make them accountable, to impose proper governance. There is no justification for this. All the evidence suggests this is contrary to consumer wishes and it would be detrimental and retrograde step.

78. Other tools, codes, browsers settings etc.

A mandatory Code would potentially offer a vehicle to require appropriate design and outlaw the use of nudge techniques. It would need to have a similar reach to the Design and Children's Code so the ICO could effectively enforce on the specifics of banner/options design and come down hard on the transgressors. It would be popular among users and could significantly improve browsing experience for many e.g. once a cookie option has been selected by a user it could be clear that it is legitimate for the site to retain and reapply that option. At the moment many sites repeat the option on every visit – presumably just in the hope of wearing users down.

Browser settings have been available for some time but the technical problems remain. They can be a part of a wider menu of options but are not solutions in themselves.

XII REFORM OF THE INFORMATION COMMISSIONER'S OFFICE INTRODUCTION

79. As with other elements of the proposal there is an over arching risk that the EU will regard the changes as undermining the UK commitment to maintain equivalent levels of protection and the independence of the data protection regulator. As with other elements of the proposal this should have been clearly confronted and specifically addressed as a relevant consideration in reviewing the proposals. The absence of this means that a proper and relevant policy consideration is missing from the analysis of the proposals.

80. Generally the move to more joined-up regulation of the digital space is welcome. In particular the development of formal co-operation processes and gateways however it might be preferable to take a more holistic view of the digital regulation space rather than address some elements of the position of the ICO in this proposal.

81. It is noted that this section also ties to elements covered in the Introduction which describes the proposal as being to change the basic role of the regulator from being a data regulator to having responsibility for helping and encouraging business and others to use personal data for "responsible uses". There is no discussion as to how assessments are to be made as to what are desirable or responsible uses of personal data or how the balance between these two aims is to be resolved where there is a tension.

82. The other new suggestion in the Introduction is that the regulatory regime would incorporate "preventative supervision". This would be wholly new. The ICO has never had preventative powers; no licensing, no permissions, no ability to issue generally preventative bans on processing. I cannot trace where this is detailed in the rest of the paper but it warrants a comment.

83. To transfer responsibilities for "preventative supervision" positive actions by the regulator would be new and effectively amount to a transfer of regulatory risk from the controller/processor to the regulator. Any increase in regulatory risk to a regulator has a tendency to breed caution, if not timidity, and circumspection in the approach of the regulator. If the regulator gets it wrong they will be subject to blame. If they fail to spot the next big problem, take the wrong punt on a new technology and it goes wrong they are in the firing line in a way that does not apply in a regulatory construct in which the regulatory risk lies squarely with the controller/processor as it does now. As an example the agreement that other jurisdictions are adequate by the EU Commission has been painfully slow and ineffective over the years.

84. In relation to the proposed dual aims there is potentially a conflict between different aims e.g. to promote innovation on the one hand and to deliver compliance on the other. This raises a number of points:

    - In any case where a regulator has potentially competing aims/priorities it provides a basis for legal challenges to the decisions of the regulator and potentially fuels litigation. For example the first aim, to uphold data rights of individuals, may not sit wholly comfortable with an aim to reduce the resource spent on individual complaints. It raises a risk that an individual whose

complaint was not pursued with adequate resource might seek to challenge the approach on the ICO on the basis that the overriding tasks of the ICO include upholding individual rights. A similar issue arises with the inclusion of a duty to promote innovation. A controller who was subject to action by the ICO in respect of some particular form of processing would be able to mount challenges on the basis that insufficient attention had been paid to the need to promote innovation.

- Where there is a tension between the various aims, in the current proposals it is not clear how that would be resolved.

- There is also a possible unlooked for effect of transferring elements of regulatory risk to the ICO

85. Overall the risk is that changing the aims and objectives of the regulator to embrace more diverse aims will lessen the effectiveness of the ICO in practice rather than support the aim of delivering effective, targeting regulation.

As noted in opening, these potential issues and tensions might be better addressed in a holistic way looking at the roles of all the regulators engaged in the digital space and building in stronger obligations to consult and consider the aims and interests of others but retaining clarity about the central focus of individual roles.

86. Overriding objectives

The introduction of the two overarching objectives (para 322) appear to largely reflect the current role of the ICO. But see the comment above in relation to introducing more complex and possibly diverging aims.

87. Growth and Innovation and Competition duty

These are similar proposals; one to promote innovation and the other to have regard to competition. These are new elements, to the extent that the duty would go beyond the current general duty in the Regulators' Code to have regard to economic factors, including competition, in making regulatory decisions. In practice the ICO, as with all regulators, must take a 360 view of any guidance, enforcement or other regulatory action. This can mean policy may take time to develop, require consultation and detailed work and often difficult discussions.

88. As an example the ICO's Code of Practice on Employment was one of the most successful pieces of guidance work it has produced. It led the way in Europe (and more widely) and remains a reference point today, albeit in need of updating. However it took well over a year to complete and involved extensive consultation and discussions with industry, some of which was distinctly challenging, particularly on how the use of technology was changing the workplace. This raises a couple of points. First these duties look uncomfortably one-sided. There is no corresponding duty on controllers to be open with the ICO about the nature of new developments or the threats that they may raise. Indeed if controllers cease to have a clear duty to carry out formal DPIAs it is possible that there will be a paucity of material for the ICO to review on new innovations. Second there is no clarity

about how the ICO is to evaluate competition issues. This is not the skill set of the ICO. Should there be corresponding duties on data controllers to provide information to assist in the ICO fulfilling this duty? Should the CMA be required to provide formal advice on competition matters in relation to requests from the ICO to assist in the ICO evaluation of competition issues? This may be covered by the next part of the proposal but it would be helpful if the duty was made explicit. As well as it being explicit that the ICO must have regard to such matters but they are not dominant or overriding considerations.

89. Second the focus on new business and innovation may be misplaced. Much of the need to take regulatory positions and to develop guidance arises not particularly from new businesses but the application of new practices and technology in existing systems and business. Perhaps it needs to be clear that horizon scanning is not limited to, or even focused on, new businesses but on the application of new technologies to existing practices?

Information sharing gateways

90. This proposes duties to consult and cooperate and to be able to share relevant information with other regulators. In theory the proposals look helpful however in these cases the specific and details have to be examined once these are available.

91. Statement of strategic priorities

This element of the proposal is not wholly clear. It states that,

"…as an independent regulator the ICO will not be bound by the statement of strategic priorities" and that the ICO's statutory objectives, duties, functions and tasks would take precedence in any conflict. It is not clear how this would work with the proposed duties to take account of innovation and other regulatory aims as described in the preceding part of the proposal. It introduces another potential element to which the ICO must have regard but is not bound by.

It is difficult enough for a regulator like the ICO who operates in a complex environment to consider and balance the many points which can be relevant to regulatory decisions. To add yet another which in fact has no statutory effect seems burdensome. The risk is that it could be used as a form of implied political control of the ICO's policy and in fact undermine independence. Out of all this part of the proposals this appears to be the most high-risk in relation to the UK's adequacy position. The issue of a regulator being subject to political control is a sensitive one in the EU. Action has been taken by the Commission against two Member States on this basis. On balance the high risk appears to clearly outweigh any marginal usefulness of this element of the proposal.

92. ICO International role

This is another potential obligation to consider Government policy when determining the ICO activities. This time in the international area. As with the statement of strategic priorities this is potentially high-risk in relation to the UK's

adequacy position and on balance the level of risk appears to outweigh any marginal usefulness of this element of the proposal.

93. Governance, appointments and salary

The appointments and salary proposals appear to be practical and uncontentious. The proposed governance model lacks detail and hence clarity. In particular how many members of the proposed board would be appointed and what sort of job descriptions/roles would they have? This will influence the nature of those appointed and the views and skill-sets. It will be critical that the board is well-balanced with a range of skills representing those who understand the importance of data protection and individual rights as well as those with business or data expertise. It is not possible to comment without seeing detailed proposals.

94. Accountability and transparency

Currently the ICO sets strategic aims and priorities and reports against those. Requiring these to be set as KPIs would formalize this without changing the substance. However there is a risk that the inclusion of the list of reporting obligations in respect of policy objectives of the ICO and the Government would risk overshadowing the central importance of the ICO's statutory tasks and duties. These are, and should remain, the core of the ICO's activities and reports should focus on these.

95. Codes of practice and guidance

Both codes of practice and guidance are important in providing information to controllers and data subjects as to the ICO's thinking and approach. As noted above, wide consultation is important in building effective codes and has a role in developing robust guidance. It should be noted however that there is a significant difference between codes of practice on the one hand and legal guidance on the other. Codes explain the relevant rules but focus primarily on how compliance can be achieved in practical ways. Guidance is primarily used to set out the ICO's legal interpretation of the law for controllers and subjects. Treating these in the same way yokes these two completely different elements together. Panels may be useful for codes, although they seem unnecessarily burdensome and bureaucratic. The practical reality is that the ICO has no shortage of those who are ready and willing to comment on developing codes and to contribute expertise as needed. However guidance has to represent the considered view of the ICO reached independently and with proper advice. It is not generally a matter of policy. There are rarely policy aspects to the development of guidance on the law. The potential for a committee to oversee guidance and then for the approval of guidance by Parliament has a significant risk of undermining the independence of the ICO. Independence of thought and position on the interpretation and application of the law is an essential part of the role of an independent regulator.

In relation to guidance on data protection therefore this is a potentially high-risk proposal in relation to the UK's adequacy position. There seems no proper place for this proposal given the statutory independence and role of the ICO.

96. The questions also refer to an obligation on the ICO to conduct impact assessments of the effect of codes and guidance. This would be an added bureaucratic burden on the regulator and it is not apparent what use these would be. The role of such activity needs to be explained and fleshed out.

97. Complaints

The ICO process currently asks data subjects if they have attempted to resolve matters with the data controller and seeks to direct them to do so where appropriate. To that extent this would simply formalize existing practice and would be unobjectionable. However there would need to be clarity that in serious cases or where otherwise justified the data subject could refer directly to the ICO and the ICO has an unfettered discretion to address the matter, for example a massive data breach affecting many individuals can hardly be dealt with or resolved by an individual complainant.

98. The proposed obligation on data controllers to have a proper complaint-handling arrangements (which it is assumed could be through a third party for smaller data controllers?) is a helpful mirror of the requirement on a data subject to refer to the controller. A level of detail setting out the controller's obligations, timescales etc.. would be required.

99. Technical reports on enforcement matters.

It would have been helpful for this to be cross-referenced to the proposal for the ICO to have regard to innovation, economic factors and competition issues in carrying out his/her functions. The examples given are related to technical issues of security but such a power would be useful in dealing with the wider obligations on the ICO to take account of numerous factors in making decisions, many of which may be outside the ICO core skill set.

In relation to the cost of such reports it would seem wrong to make the controller pay unless there was some element of culpability such as a deliberate failure to respond to a reasonable investigation. In relation to issues of economic impact and competition these would not be appropriate to fall on the shoulders of data controllers as they concern primarily the exercise of discretionary powers by the ICO.

100. Compulsion to respond to questions

While this is potentially invasive and would need careful handling, it would be a possible counter to the abolition of the duty to conduct DPIAs and the removal of the obligation to retain central records of processing activity.

101. Timescale for response after Notice of Intent

The proposal to allow the ICO a 12 month period between a Notice of Intent and a final notice, in the absence of evidence of obstruction etc.. by the data controller, is not an appealing one. Controllers are entitled to have enforcement decisions made with due expedition and not have the threat hanging over them. Notices of Intent are meant to be served once the ICO is sufficiently satisfied of the result of

the investigation and the conclusions he/she has reached. While representations may bring up factors or matters to which regard should be had in determining the final decision, they should not be raising new issues not yet considered.

102. Biometrics and surveillance roles

No submissions.

Submitted by Rosemary Jay, Solicitor specializing in data protection. I have worked in the area since 1987 and am the author of Data Protection Law and Practice now in its 5th edition published 2020. Over the course of my career I have worked for the regulator (now the ICO) and in private practice. For the last 10 years I have been a consultant with Hunton Andrews Kurth. These submissions are made on a personal basis and do not represent the views of the practice or any clients.

ANNEX 1

Recital 50 – Background and Development

1. Recitals are potentially problematic. They are meant to give assistance to interpretation. They cannot have normative effect i.e. if the legislative text does not reflect the recital, the recital is of no effect . They should use “non-mandatory language” but not “desires, intentions or declaration”. The recitals in the GDPR do not universally meet these standards. In places they remain the sad embodiment of the hopes and (failed) dreams of lobbyists.

2. The paper appears to contemplate that elements of Recital 50 should be imported into the UK GDPR (it seems the statement that a new legal ground for processing is not required for compatible processing). There must be stringent assessment of this proposal as it is clear that elements of that recital do not meet the test of being of assistance to interpretation but instead seek to insinuate a normative provision directly contrary to the terms of the legislative text. Any prudent organization would be well advised to steer clear of relying on such a provision. In view of the potential importance of this I have looked at Recital 50 in some more detail.

3. The recital has a number of elements:

    - New purposes which are incompatible with the original purpose of collection are not permitted;

    - **Where new purposes are compatible with the original purpose of collection no legal basis separate from that which allowed the collection of personal data is required.**

      This is highlighted as it purports to make a normative statement. However it is not reflected in the legislative text nor indeed has it ever been. It appears to be impossible to reconcile with the clear meaning of the legislative text. As such it cannot be regarded as a reliable element of the recital and, applying the tests in Casa Fleischhandel (see earlier footnote), the better view is that it should be ignored in any interpretation.

    - If further processing is necessary for a public interest task etc.. Member State law can determine the legal basis

    - Further processing for research etc.. should be considered compatible;

    - Member State law can provide a legal basis for further processing;

    - The tests for ascertaining compatibility are repeated;

    - Where the data subject has given consent, further processing is acceptable irrespective of compatibility;

    - Where the processing is based on Member State law which protects important objectives of public interest further processing is acceptable irrespective of compatibility

- In any event the principles and rights of individuals continue to apply [to the processing];

- A number of examples of processing in legitimate interest are given.

4. It is not completely clear what the material about legitimate interests is meant to import. Possibly that these are a) generally assumed to be compatible and b) generally accepted as falling into legitimate interest. However if the wording in Bullet Point 2 above was a reliable statement of the legislative intent it would be otiose as they could rely on the original legal basis in any event.

5. The element of the recital which is clearly an outlier from the legislative text is the second bullet point. It did not appear in the original Commission recital (Comm 2012 recital 40, which would have been removed by the LIBE Committee of Pariament in its 2013 response). Article 6.4 of the Commission text potentially permitted processing for incompatible purposes as long as it had a legal basis in Article6(1)(a) to (e). The EDPS expressed strong reservations on this point in the Opinion in 2012 (para 121). Several elements of the recital appear largely as they are now in the Council document of June 2014 but not the reference to same legal base. It made its first appearance in the Council document of March 2015 but the relevant legislative provisions in Article 6 of that document are in direct contradiction of the recital. Article 6.4 providing that,

   "..where the purpose of further processing is incompatible with the one for which the personal data have been collected by the same controller, the further processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1.

6. The sentence continued to appear in recital 40 in the Council text of May 2015 as did the contradictory legislative text, followed by the same in the version of June 2015, although by June 2015 at least one representative (Germany) appears to have noticed the disconnect and suggested an amendment to the recital that made it a proviso that the original legal basis actually covered the new processing, but this sensible suggestion clearly went no-where.

   The sentence continues to appear in the recital in the versions of November 2015 and December 2016 but para 4 of Article 6 was deleted.

   And thus it made it into the final version in 2016 with the sentence in what is now recital 50 hanging in the air, purporting to have a normative effect i.e. create a rule, but with no supporting provision in the legislative text, albeit that the clearly contradictory text has been removed.

7. As noted earlier, recitals cannot have a normative effect. They cannot be read as imposing rules separate from the legislative text. They are interpretative or explanatory only. The question raised therefore is whether this sentence can be read as an interpretative or explanatory gloss on the provisions of Article 6 (grounds for processing) or possibly Article 5(1)(b) prohibition of incompatible processing. To address this question it is appropriate to make some general points in respect of the principles (Article 5) and grounds (Article 6) and then to consider the grounds one by one.

General points

8. The principles and the grounds for processing are largely reproduced from Directive 95/46/EC and the presumption is that the meaning of the grounds has not changed. The Directive does not include the guidance on how to determine compatibility but includes the requirement that further incompatible processing is not permitted and that research etc.. is deemed to be compatible, subject to safeguards. So the basic premise in the legislation appears to have remained unchanged.

9. The principles under Article 5 create what may be regarded as a coherent code for the fair and proper processing of personal data with respect for individual rights, balanced with the needs of controllers. No one principle stands alone, nor is one principle superior to others, although the overriding obligations of fairness, lawfulness and transparency permeate the code. Any new processing must always meet all the requirements of the principles; compatibility is arguably the most minor issue a controller will need to consider. The governing considerations are generally relevance, transparency and fairness. If processing can be regarded as compatible with the original purpose it can be argued to be prima facie fair but that is only one small part of the compliance assessment.

10. The grounds for processing in Article 6 are linked to other provisions which have to be considered, such as the definition of consent. As a basic point in interpretation – if the sentence that no legal basis separate from that which allowed the collection of personal data is required where new processing is undertaken can be regarded as validly interpretative to must:

    - Be capable of applying to all the grounds (as it is not limited to specific grounds);
    - Not undermine or contradict any of the grounds and
    - Provide some useful interpretative gloss.

    It is submitted that the sentence spectacularly fails to meet any of these tests and the conclusion must be it not only has no normative effect but no interpretative effect either. It is simply another of the lost dreams of lobbyist interred in the graveyard of the recitals.

11. I have not reviewed all the grounds because clearly if the phrase can apply an interpretative gloss it must be capable of applying to all the grounds. If it fails at one it must fail at all.

    - Ground 6(1)(a) Consent is defined in Article 4 and amplified in 7. It must be informed, specific and freely given. It is an active requirement. It must be given by the data subject. It requires the controller to be able to demonstrate consent and allows the data subject to withdraw at any time. Consent is therefore a matter of fact and law. There is no provisions for “deemed consent” and any argument that consent could be deemed as a matter of law would not stand against the clear definition of consent and the interpretative provisions in Article 7, or indeed Article 8 if the data of a child were involved. It follows that the statement that a new purpose can be adopted with no legal basis separate from that which allowed the collection of personal data [being] required cannot be accurate where the legal basis of the processing was originally consent. It contradicts all the requirements

of consent under the GDPR; knowledge, active agreement, right to refuse agreement etc...

- Ground 6(1)(b) Processing necessary for the performance of a contract or in order to take steps at the request of a party prior to a contract. There are no associated definitions. There are two cases – where there is a contract and where one is anticipated. To take the second case first the data subject must actively have requested steps be taken in order to enter a contract of which he/she was aware and intended to enter. A deeming provision that this applied would contradict the requirement that the data subject must have taken steps to enter the contract. To look at an actual contract. A contract is a matter of fact and law. The only way to argue that the contractual basis could apply to the new processing would be to argue that the new processing is deemed to be covered by the existing contract as a matter of law. But this would be a radical addition to the ground; a new normative provision. It cannot be imported by a recital. Further it makes no sense practically. The contract might be about something completely different and the terms wholly irrelevant to and unsuited to the new processing.

12. Equivalent analyses as to the effect of fact and law apply to the other grounds. Under 6(1)(c) vital interests and 6(1)(f) legitimate interests. Vital interests are a matter of fact as is the outcome of the balancing test in a particular case in 6(1)(f). Legal obligations are matters of law and fact. No one can be made subject to a legal obligation to process or process in a particular way which is not in fact binding on them as a matter of general law.

13. It follows from this detailed analysis that the proposal that this odd sentence in recital 50 be imported into UK law is fatally flawed. It would undermine the UK regime by importing a completely new and unjustified liberty to allow new processing without proper assessment and compliance with adequate grounds for processing in the particular case. As the grounds for processing are a fundamental concept in the GDPR this would amount to a significant undermining of the UK regime.