#	Topic / Relevant provision	Question	Rspndr	Response
	General Questions	Key: Elisabeth Stafford (**ES**) Robin Edwards (**RE**) Emily James (**EJ**) Gaby Anderson **(GA**) Stewart Dresner (**SD**) Marcus Evans (**ME**)		
0		When will legislation be introduced?	**ES** **RE**	ES: You may have heard Jenny Hall speak last week, this is a question everyone is asking, especially in light of recent political changes. When you get a new minister there is a period of taking stock. We are making progress as quickly as possible but can't yet give a firm date. RE: We think it will still be introduced this session and will have to go through parliamentary passage by Spring next year. Providing that the current government can make quick decisions the bill will be introduced fairly soon, if not in the next few weeks surely shortly after summer recess but we don't have a definite date yet.
0		How will it be introduced? Consolidation and restatement or amendment?	**ES**	We are not repealing or replacing the GDPR or the Data Protection Act. The new bill will amend but not replace the existing legislation. The legislation.gov website will update to show the legislation as amended. The existing changes are already updated. We thought this would be the best way forward to symbolise that we're not getting rid of GDPR we're building on it.
0		Overview	**ES** **SD**	SD: Note that this is the current opinion of the government, it may be changed. ES: Our reform is much more of an evolution than revolution. We are keeping the foundation and principles, rights, enforcement and key components. Seeing as it has been 6 years since the GDPR has been reviewed we're looking at other areas of uncertainty with organisations or data subjects. We're also looking at other areas where the same level of protection can be achieved through different means. The published consultation had almost 3000 responses. In particular this chapter is about improving what we have whilst maintaining strong protections
1.	**REDUCING BARRIERS TO RESPONSIBLE INNOVATION**			
1.1.		Overview of Legitimate Interests	**RE**	One of the key proposals in the consultation was around Art. 6(f) (the lawful ground of legitimate interest). Consultation stakeholders reported that the legitimate interests ground is difficult to use, on the basis that the balancing test was burdensome and confidence about when the ground could be relied on was sometimes low, with some organisations reverting to consent and some being deterred from processing altogether. The consultation paper included a fairly radical proposal suggesting that if organisations were relying on legitimate interests there may be circumstances where they didn't need to undertake the balancing test. In the consultation paper there was a long list of areas where the balancing test was not needed. These were divided into two groups: public interest and low risk business administration processing, where it was considered that the balancing test was not necessary. This included transfers between group companies. Responses to the consultation were quite polarised. Some businesses were in favour whilst others felt the balancing test was a valuable safeguard, helping to protect not only privacy but also consumer trust. Ministers were alive to the arguments put to them about consumer trust, rights of data subjects etc but they were also worried about reports of delays to processing for important public interest purposes whilst the balancing test was applied. This is particularly important in relation to safeguarding. The response to the consultation was a compromise position, removing the balancing test for a narrow range of public interest activities in connection with which the view was taken that it would simply always be met. Parliament retains the power to designate further purposes for which a balancing test is not required. Initially, this won't include the business purposes that were consulted on, but we anticipate businesses requesting for further purposes to be added. The changes are intended to remove delay, reduce burden and increase confidence.
1.2.	**Legitimate interests.** *The intention is for the balancing test to be dispensed with in connection with certain identified processing purposes. Examples provided are public interest processing and innocuous business purposes.*	Removing the balancing test for the purposes of crime prevention risks crossing into egregious surveillance. The balancing test is a critical control to prevent privacy-intrusive processing such as with CCTV, software and new technology. If there are reported thefts in the ladies locker room, it is a crime prevention purpose to put up CCTV and the controller has a legitimate interest in doing so, but it is the balancing test that prevents CCTV being installed inside the locker room. Without the balancing test, what does DCMS think would stop the security team putting up the CCTV inside the ladies locker room? The necessity test is arguably met on these facts. DPIAs, for instance, are only advisory. The right to object places the burden on individual and only applies when they exercise the right, which is too late, and in the example would require all affected women to raise an objection. (Same point for software for security but is effectively worker surveillance).	**RE**	The provisions will be designed with safeguards in mind. We will be maintaining the necessity test and there is an element of proportionality that is part of the necessity test, as demonstrated by caselaw. We don't think the example given would pass the necessity test. In addition, other protective principles such as transparency and data minimisation continue to apply. Ministers will set out policy intentions, which will be documented in Hansard records.
1.3.		Will it be as broad as eg "crime prevention" or will there be subsections?	**RE**	In terms of drafting this may be difficult and there is a reluctance to suggest that prevention of some crimes is more important than prevention of others. We do not think we can produce a prescriptive list of all criminal offences that need to be covered.
1.4.		The 'public interest' is famously undefined in English law - how does relying on this concept help businesses with clarity and certainty? In the context of the identified public interest exemptions, is there a reason why the legitimate interests ground is being eroded as opposed to adding further specific conditions within the UKDPA to meet the public interest test pursuant to article 9(g) GDPR?	**RE**	There was a question in the consultation paper asking organisations for where they felt difficulty navigating through Article 9 or Schedule 1. There won't be any changes to Schedule 1 through Parliament, we can make these changes through secondary legislation in order to save parliament time. Where the Article 9 ground is met, the new changes will often assist in identifying an appropriate Article 6 ground.

#	Topic / Relevant provision	Question	Rspndr	Response
1.5.		What are the new substantial public interest conditions / grounds for processing that the Government plans to add to Schedule 1 of the Data Protection Act 2018?	**RE**	All organisations need to identify a ground under Article 6, if they're processing special category data the need to identify a ground under Article 9. In these circumstances it will assist with identifying an Article 6. If you are a public body you may be able to identify public interest as a ground under article 6(1)(e). Given public bodies generally do not rely on legitimate interests under Article 6 (as they have their own ground under Article 6(1)(e)) this will mainly affect businesses, in connection with processing where consent isn't appropriate. In 2018 when working on the last data protection bill we added new exemptions to Schedule 1 in relation to increasing diversity in boardrooms. This provision allowed processing of data connected to race in order to increase diversity. However, we've been speaking to stakeholders who found that this has not worked as intended. We will have the opportunity to address this during this process. We will also address other issues with schedule 1.
1.6.		Is there any indication of what the Government's prescriptive list of legitimate interests (which do not require a balancing against individual rights) will include?	**RE**	Details are still being considered, however our current thinking is that this will only include activities Parliament deems to always pass the balancing test. Areas would include processing that is necessary for national security purposes, crime prevention, safeguarding and processing necessary to respond to an emergency. It possibly would also include processing necessary for democratic engagement (which is an important issue for ministers). That's our current thinking but it's unlikely that any list would go beyond these.
1.7.		Would you agree that both safety and technical updates for vehicles can rely upon legitimate interest without doing a balancing test.	**RE**	I am not sure.
1.8.		Will the balancing test be retained in connection with children's data, per the views of respondents?	**RE**	The balancing test won't be required in connection with the excepted purposes just because it is children's data that is being processed. For example in connection with voluntary organisations sharing information with social services. One of the key considerations is to carefully consider the rights of individuals, particularly children, before any changes were made to the list. If the balancing test has slowed down assistance to children why would you want to keep it?
1.9.		What is the interlock between the Economic Crime Bill & the Data Reform Bill regarding data sharing for financial crime (fraud, AML) investigation purposes?	**RE**	The Home Office are very keen on this measure partly for that reason. We have been talking to that team in the Home Office because it will allow financial institutions to share the data if there is a concern about money laundering, sanctions evasions etc.
1.10.		Can you say any more about the innocuous business purposes?	**RE**	The original consultation included a long list including some innocuous business purposes. There was a lot of public concern and ministers listened to this. This has been narrowed down to the public interest grounds that we identified. In the original list for Parliament there will not be business purposes, this may change after lobbying but the starting point will be focussed on public interest grounds.
1.11.	**AI and machine learning (generally)** *Many of the key AI questions have been deferred until the government publishes its AI white paper, including what the ICO should take into account and how the ICO should interact with other regulators in this context.*	Overview	**ES**	Our concern when publishing the consultation is that there was a lack of clarity in how the Article was structured and its key terms. There was sufficient uncertainty around safeguards that we were worried about them being applied correctly or even at all.
1.12.		When will DCMS publish the forthcoming AI White Paper? Will there be alignment with existing provision (eg. the AI Assurance Roadmap).[1]	**ES**	We are aiming to publish as soon as possible
1.13.		How to define fairness in the AI context and who should define it. Unlawful – easy (eg. breach anti-discrimination laws or SYSC); Transparency – easy (can't have unexpected uses/ outcomes); Procedural – harder (but not too subjective); Outcomes – very subjective (ethics). Did DCMS consider whether outcomes fairness should be left unregulated (and addressed by the other types of fairness, public opinion or specific subsequent prohibitions (such as those in the EU AI Reg))? Or is it seriously contemplating using a word as malleable and subjective as "fair" as a legal standard to hold AI and automated decision making processes up to (as the ICO suggested in its comments on the initial consultation)? Can DCMS shed any light on how the Office for AI is thinking about this? For example, will an overarching legislative approach that applies across all regulators (DRCF) be developed?	**ES**	It is a difficult challenge to identify what is or is not fair but we hope the white paper will largely address these issues. Whilst the reforms mentioned are going to be covered by the bill, the fairness question will be covered by the white paper.
1.14.		Are there going to be prohibited practices, similar to the EU's AI act where a list of "definitely unfair" prohibited activities has been identified? Or any other method of calling out what is or isn't fair beyond a balancing test? It is virtually impossible to define this up front.	**ES**	The broad processing activities will be set out on the face of legislation. We've also been talking to the ICO recognising that the changes we make will require corresponding updates to ICO guidance. There will be a combination of legislative provisions backed up by secondary legislation.
1.15.		Can you give us more details about what changes are planned that will impact laws relating to automated decision making and profiling? How much thinking has gone into safeguards relating to the new condition?	**ES**	This speaks to what Robin was saying about adding conditions to schedule 1. The existing lawful bases already have a number of safeguards. There is a plan to create a new processing condition to limit bias, it will fit into schedule 1. I can't confirm if this will be covered in the public policy document as yet.
1.16.		Will a policy document be created?		Yes. The explanatory document will be clear and easy to understand (ie. directed at laypeople).
1.17.		Is there any consideration of processing for training AI tools as opposed to processing of the data once the AI has been trained and is being used in real life?	**ES**	This is not a policy I led on but the new condition would be around training the AI rather than what is being done with it subsequently.
1.18.	**Automated decision making.** *Uncertainty about when automated decision making is "solely automated" and when "it produces legal*	Will the Art 22 reforms have to wait for the govt position in the AI White Paper or might they be revised following that consultation?	**ES**	ES The AI white paper is being worked on simultaneously but we wouldn't anticipate any contradiction as the bill goes through parliament

[1] Published in 2021. A data-sharing governance framework, which is intended to help organisations. It includes a set of principles on how to set up an effective governance that is open and transparent, and enables trusted data sharing. More consistency in how people apply such standards and frameworks will help. Almost like a kitemark standard for the application of the algorithm. Referred to in the Select Committee for Science and Technology 8 June 2022.

#	Topic / Relevant provision	Question	Rspndr	Response
1.19.	*effects or significantly affects" the data subject means the government is considering how to amend this provision, including recasting it as a right to specific safeguards rather than as a general prohibition on solely automated decision making. However, the precise approach will be set out in the AI white paper.* .	We read this as DCMS proposing to do away with Art 22(2) (ie limiting SADM where one of 3 grounds are met) completely – is that correct? In which case will the obligations to provide ex ante explanations, to hear complaints and explain decisions ex post be the only safeguards? If not, what other safeguards are being considered? Would this apply to public sector automated decision making too? In this light, perhaps outcomes based fairness becomes more important?	**ES**	No. One of the proposals was to remove Article 22 but we decided against this as human review is a key safeguard that we wished to retain. What we wanted to achieve could be addressed with targeted changes to the Article eg re-casting the Article as a right to human intervention, as opposed to a prohibition. Human review will not be the only safeguard.
1.20.		Do we need to implement safeguards at a lower threshold? Is the clarification looking like it's going to lower standards or raise them?	**ES**	We're not lowering the standard but this is going to make automated decision making easier through increasing clarity, with a focus is on solely automated decision making with significant effects.
1.21.	**Processing special category personal data for AI bias mitigation purposes.** *A new processing ground will be introduced for monitoring and correcting bias in AI subject to safeguards, such as limitations on re-use and the implementation of privacy-preserving measures.*	Is DCMS considering creating non-govt organisations subject to similar obligations as "data intermediaries" under the EU Data Governance Act with fiduciary duties that can be enforced by regulators that individuals can trust to hold and police special category personal data provided to AI developers to monitor and correct bias in AI systems? There are lots of examples of well-intentioned D&I programmes hanging onto this data beyond the initial research question with the intention of showing improvement over time – unfortunately increasing the risk of misuse, rather than fixing it. We are not sure the Smart Data schemes proposals would cover this type of data sharing.	**ES**	Agree that the proposals are unlikely to cover this. The Smart Data schemes are not managed by DCMS but rather, Business Energy and Industrial Strategy (BEIS).
1.22.		We note the specific provision relating to use of special category personal data in the context of testing bias. Is DCMS proposing a general obligation to undertake testing/accreditation to ensure that algorithms actually perform the way they are intended to / data subjects have been notified of? If so, given the widely discussed ethical concerns around the use of AI, will organisations be prevented from offering an algorithm to the public until such testing / accreditation has been undertaken?	**ES**	This measure concerns firms that cover smart data, this is about the government's ability to mandate their participation. Allowing customers to switch accounts etc. There is no specific obligation, the law will be enabling. Bias mitigation measure will be encouraged but not compulsory.
1.23.		To echo the concerns raised by Lord Kamall (Minister for Technology, Innovation and Life Sciences at the Department for Health and Social Care) to the Science and Technology Select Committee. What steps will be taken to manage bias arising not from a flaw within an algorithm, but from inherent lack of representation within reference data sets? The example given was of observed vaccine hesitancy within particular ethnic communities.		Question not posed due to time constraints.
1.24.		A recurring issue is that one controller says the data is anonymised to GDPR standards but the other controller disagrees. This is where both parties are looking at the GDPR and recitals, not national guidance. Has DCMS taken into account that any perception of variation or difference from the GDPR will exacerbate what is already a disputed area in research?		The standard of anonymisation was not discussed during the session.
1.25.	**Research purposes** *The definition of research requires amendment, with the proposal being to retain the definition provided for at recital 159 but to move this into the main body of the legislation.*	Overview	**ES**	Research processing is subject to a number of relaxations under the UK regime. The definition of research is an important provision and is quite unclear in the UK GDPR. When we were working with the EU we spent a lot of time ensuring that we struck the right balance between data protection and facilitating research. We identified that there is scope for improvements to make it simpler for researchers to navigate this landscape. This is consistent with the general themes of the whole consultation. We want researchers to focus on research as opposed to onerous compliance, providing important context to give a solid legal footing. Relevant proposals are (1) clarification of the definition of research; (2) exemptions from transparency requirements; (3) relaxation in connection with re-purposing data and (4) innovative data sharing.
1.26.		Only a third of respondents to the consultation agreed that this definition represented "a clear and broad base that was understood by researchers." The remainder did not feel that it was suitable [or were undecided]. Given that Recital 159 is very wide and DCMS is relaxing various other safeguards (eg broad consent; requirement to provide fair processing information), would a clearer definition of research be appropriate rather than leaving this to the ICO and/ or the courts to determine?	**ES**	The definition is very important as the GDPR contains derogations for research, so if we widen the scope we are widening exemptions. We have had to approach this very carefully to avoid causing negative consequences. There was no clear or united position on what the definition should be. Different organisations wanted different definitions for different purposes. We did get a few interesting ideas for things to include but we didn't have a majority steer. We have therefore modelled our clause on the existing recital to avoid inadvertent negative consequences. The ICO guidance is quite detailed and it will be of help to the organisations. This level of detail is more appropriate for guidance than legislation. The guidance can be amended more easily than legislation if it is not working. We are not aiming to change the scope despite putting it on a more legal footing.
1.27.		The DPA2018 provides for an exemption for some of its requirements where "personal data is processed for the purposes of approved medical research" defined as research approved by a research ethics committee (REC) or equivalent body. Each of those bodies has threshold criteria. This results in a body of medical research that is not "approved medical research" on the basis that it doesn't represent a sufficient risk to meet the criteria triggering the requirement for a REC review. This creates the somewhat perverse position that, even though the medical research is considered sufficiently "low risk" not to require REC approval, the Provider cannot rely on the DPA research exemption by virtue of the fact the research has not been subject to the approval it does not require. Will the new law clarify whether medical research can be treated as "approved medical research" on the basis that (1) it is being undertaken by a body that is subject to duties of confidentiality and (2) all requirements to seek approval have been met, by virtue of the fact that none of the triggering criteria are engaged?	**ES**	We haven't heard this point before, I think the concern is that medical research must be approved for this exemption to be considered. In some cases the research is so low risk that it will not be required to get approval. This is something we need to take away and discuss with stakeholders and the ICO. We will not address this in the new bill.

#	Topic / Relevant provision	Question	Rspndr	Response
1.28.	**Research purposes: transparency** *Proposal to replicate A14 "disproportionate effort" exemption into A13 for research purposes.* *Recital 62 GDPR: It is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.*	The majority of consultation respondents disagreed with this proposal. In addition, studies have shown that public willingness for data to be linked and shared is high where it facilitates research for healthcare, but that willingness relies on the ability to explain clearly what people's data is going to be used for, who is going to be using that data and what the safeguards are for the public around patient data. The Science and Technology Select Committee was advised that lessons have been learned from the failed GP Data for Planning and Research initiative, which was subject to a rapid erosion of public trust, leading to people withdrawing their consent. Taking all this into account and the clear importance of transparency in this context, why is DCMS proceeding with this proposal?	**ES**	We want to reduce barriers to research. For example Article 13 UK GDPR focusses on providing information where you have collected the data. Article 13 (3) imposes an obligation to provide information where there is a change of purpose. Our reform creates a derogation from this where it would constitute a disproportionate effort. We did look at all evidence. The reason to pursue this is that a minority of organisations have validly collected the data and held it for a long time but now are unable to contact the data subjects. I think it is worth noting that this is not a new proposal. What we are doing that is new is expanding the number of situations that can be provided.
1.29.		Would it not be better to encourage more confidence around anonymisation in the research context rather than an exemption from transparency?		Question not posed due to time constraints.
1.30.		How will the transparency requirement be met in connection with research processing (where there is no requirement to notify of re-purposing in the event that to do so would represent a disproportionate effort)? For example are you envisaging some form of public register?		Question not posed due to time constraints.
1.31.	**Further processing.** *The government will simplify the legislation to address this, making it clear to organisations how personal data can be re-used lawfully, and giving transparency to data subjects to understand how their data may be reused.* *Clarifying further processing when the original legal basis is consent.*	Overview.	**ES**	Further processing can enable research and is important for innovation and for purposes in the public interest. Eg disclosure to the police about a crime. Through our consultation, engagement and literature we have seen there is a lack of consensus on a number of issues. There is confusion on whether it is legal to further process data for purposes other than the original one for which they were collected. Are these processes compatible even where they are different? There is also uncertainty about undertaking further processing where the original lawful basis relied upon was consent.
1.32.		The government plans to legislate to provide further clarity on the distinctions between new processing and further processing. Has a decision yet been made as to whether processing by a new controller (for example, in order to leverage the specialist skillset of that controller) amounts to new purposing or further processing? An example is sharing an NHS database relating to dementia outcomes with a private pharma co.	**ES**	When there is a change of controller, the new controller is undertaking new processing as opposed to further processing. The NHS may not be undertaking further processing in these circumstances if, when they collected the data, they specified that it would be collected for this purpose. If not they will be doing further processing. The NHS will need a lawful basis and for the further processing to be compatible under the new Article. The pharmaceutical company will be undertaking new processing. The pharmaceutical company will not need to do a compatibility test. It would be impractical for a new controller to go up the chain and find the original reason for processing. .
1.33.		The intention is to codify that further processing cannot take place when the original legal basis is consent, other than in very limited circumstances. What are these limited circumstances likely to be, and does this not undermine the standard and purpose of consent (which is typically only relied upon in connection with relatively sensitive / high risk processing?)	**ES**	We want to make it explicit that there is a prohibition as we feel that it is important that consent as a lawful basis is not undermined. When it is used we need people to trust that it will be respected, to avoid long term consequences arising from data subjects being uncertain or suspicious of providing consent in the future. In terms of the limited circumstances where personal data obtained on the basis of consent can be re-purposed, we recognise that there are situations where this should be permissible. For example, reporting a crime to the police is an instance of further processing and it would not be reasonable to revert to the data subject to obtain further consent. When a controller wishes to anonymise or pseudonymise personal data, this is technically further processing, but further consent is not required. The proposed reform would make it clear that this will not be the case.
1.34.	**Innovative data sharing solutions.** *Responsible data sharing solutions can help drive growth and boost innovation, and the government aims to encourage new and innovative ways that confidential (personal or other) data can be shared.*	Citizen Juries have consistently reported that trust and transparency are of the utmost importance in the context of data sharing. For example, they identified that the Government was right to use emergency powers to share patient data to support research objectives during the pandemic, but that greater transparency is needed. If this is not approached correctly, we anticipate that individuals will opt out and it will be very difficult to get them to opt back in again. Is DCMS considering periodic refreshment of opt outs, to take into account improving privacy technologies?	**RE**	This is an important issue, particularly in the field of medical research and we've been liaising with the Department of Health on issues like this. The point about transparency being important to maintain trust will be important to future proposals.
1.35.		What other steps are being considered in connection with responsible data sharing and Smart Data Schemes, in addition to use of intermediaries?		Question not posed due to time constraints.

#	Topic / Relevant provision	Question	Rspndr	Response
2.	**REDUCING BURDENS ON BUSINESSES AND DELIVERING BETTER OUTCOMES FOR PEOPLE**			
2.1.		Overview	**RE**	The second main area of the consultation is reducing burdens on business. This was politically popular for certain ministers. That chapter was divided into main themes that we will cover today. One of the biggest areas was in relation to the current accountability provision in Chapter 4 which organisations have to put in place to demonstrate compliance. There were proposals in the consultation looking at Chapter 4 of UKGDPR for something more prescriptive. When the consultation was drafted drafters were thinking about the Canadian model. The Canadian regulator supplements this with detailed guidance. There are a lot of questions about the current Chapter 4 and whether that can be improved. The consultation also covered changes to PECR, particularly in relation to the cookies laws. The sort of things we deal with in correspondence, the cookies laws come up the most. Members of the public get irritated by constant popups but also businesses get angry at the need for popups non-intrusive cookies. Ministers were keen to include proposals on cookies in that proposal. Whilst on the subject of PECR there are also proposals on extending the soft opt-in. The third main area is on subject access requests which many struggle with. There are proposals to address the burden of these being received in very high volumes.
2.2.	**Reform of accountability framework** *New approach to accountability based on risk-based privacy programmes (PMPs). The aim is to strike a balance between an accountability framework and a more flexible and risk-based approach, which takes into account the volume, sensitivity and types of personal processed by the specific organisation. PMPs would include internal policies; designation of responsible individuals; personal data inventories; risk assessments; and transparency.*	A number of the requirements of a PMP appear to mirror existing UK GDPR compliance requirements. Whilst the aim of the PMP is to reduce organisational workload, could it in fact increase workload (at least initially) as UK organisations would be required to assess whether their existing UK GDPR compliance program can work as their PMP? Can an existing GDPR program be recast as a PMP program? • If both the EU GDPR and the UK GDPR to organisations, what is the recommendation to reduce administrative burden? Should the GDPR standard apply as it appear to be a higher standard? Will the GDPR standard meet the PMP requirements? Will organisations need to segregate EU and UK data and apply separate regimes?	**RE**	We received mixed views on this proposal generally. We did hear that the 2018 act is very new in legislative terms, organisations have spent time implementing requirements and so they were keen that we do not implement a whole new system. Some organisations were in favour of less prescription to give organisations the freedom to manage risks as they felt fit. Some targeted improvements may well still be justified. If organisations have invested time and money putting systems in place to comply with the UK GDPR, they are unlikely to have to put in place more provisions to meet new provisions increasing flexibility. We are not looking to move away from the high standards of the GDPR, but move more towards a flexibility in approaching these requirements (whilst likely useful for many organisations, this flexibility will in particular be useful to small and medium organisations). When the bill is published it will not be the Canadian model and the requirements will not be hugely dissimilar to Chapter 4. One of the main areas was in the requirement to appoint DPOs. This proposal was designed to give organisations more flexibility and this will be reflected in the legislation. If organisations are currently happy with DPOs advising them on compliance risks they will not necessarily have to change that system and may continue with the arrangements they have in place now.
2.3.		With increased flexibility comes a reduction in certainty and consistency. Is there a risk that a potentially more vaguely defined PMP could result in many diverging and somewhat less rigorous approaches to data protection compliance? • For example, the proposal to remove structured approaches to conduct DPIAs and instead leave it to the organisation to determine risk assessment as per their PMP could result in higher risk processing being undertaken with less oversight. • Is the PMP program aimed at smaller/medium sized organisations?	**RE**	We are hopeful that will not be the case. In trying to give organisations more flexibility, we are hoping that there will not be a reduction in protection. There will still be a requirement to reduce risk in relation to high-risk processing. Whilst the formal DPIA approach may be removed, the intention is to replace this with a more streamlined process focussing on evaluating risks in relation to high-risk activities (and such process may also form part of wider business assessments that may be undertaken to assess risk). One of the other areas is around records of processing. In the current provisions there is a small business exemption but this does not work very well in practice We are looking to clarify this. We are not removing important requirements, we're trying to streamline them where possible and the information required to be mapped under the reforms will not be dissimilar to the existing requirements under Article 30 (i.e. more a change of form rather than substance)
2.4.		If you are keeping high level in the legislation, does this mean the ICO will fill in the blanks through guidance or eventually clarification comes in the courts?	**RE**	There will be enough information but we have been in discussion with the ICO about what will be needed in terms of guidance. We have been talking with the ICO in terms of how long it will take to update regulatory guidance. From an officials point of view we need to make sure that both organisations and the regulator have sufficient lead in time to allow for guidance.
2.5.		The majority of respondents disagreed with the proposal to remove a data protection officer. However, the government is proceeding with the proposal to replace the DPO with "a responsible individual(s)", which does not need to meet the specific requirements/responsibilities of a DPO under the UK GDPR, including independence. However, we also note in the response that an organisation may opt to retain a DPO (e.g. if there is high-risk processing) to independently monitor data protection compliance. • What is the rationale behind requiring an organisation which may already have a DPO to appoint a separate responsible individual for the PMP regime? • Why has the government retained the concept of the DPO? • Are there differing knowledge requirements between a DPO and a "responsible individual"? • How are the DPO and the "responsible individual" intended to interact with one another?	**RE**	What we are hoping to do is ensure that all organisations take data protection risks seriously within their organisations. The new provisions have a requirement to designate a senior person who would have responsibility to ensure compliance within the organisation. If this senior person was on the management board they may not have qualifications in data protection, and it would be their responsibility to delegate to someone with expertise i.e. adopting a culture of compliance from the senior level downwards. The terminology of a DPO may not be used and the DPO label will not be included in the new legislation. The senior person within the organisation must perform certain tasks – if they are unable to do this themselves, they will need to delegate to an organisation or appropriate individual that can (and that organisation/individual can be a DPO). The legislation has to provide flexibility to do that, particularly in relation to very small businesses or public authorities processing sensitive data. SD: Further questions arising from this point include: 1. Is the renaming of this function really necessary? Surely, it would be better to retain the well-known term "Data Protection Officer" understood by both large and small organisations. 2. If a company retains a DPO (required by the EU GDPR) and also appoints a senior person as the "Responsible Individual", might that cause tension over the independence of the DPO and a possible conflict? 3. Does this possible conflict need to be addressed with dropping the "Responsible Individual" role, or clarification in the Bill, or left to guidance from the ICO?
2.6.		We note the desire to simply the record of processing activities requirements by the proposal to replace the Article 30 requirements with a more "flexible" personal data inventory. Could you give some more details around the format and level of information you anticipate being set out in such inventories?	**RE**	Really the focus is sorting out the small business exemption. We have been looking at the language of Article 30 to see if it can be streamlined. There are similarities with the current Article 30 on the list of things you have to record under the reforms. The key priority however is making sure the small business exemption works.
2.7.		Currently the DPO is independent and there must not be a conflict of interest. How do you see the interaction with different pressures when managing the new role?	**RE**	If there is a conflict of interest there will be a provision requiring delegation. We have been working with the Home Office on a number of the bill's provisions. In a law enforcement context, where you have a senior police officer whose mission was to cut crime there may be a conflict of interest.

#	Topic / Relevant provision	Question	Rspndr	Response
2.8.		The data broking world has a lot of identity verification and fraud prevention but may have a small number of employees and millions of records. Most of the organisations do employ an external DPO, the current provisions seem to be saying to these people (who are profit over people focussed) that this is not required. How do the provisions help the population of the UK not to be "sold down the river" by data brokers.	**RE**	We are not removing the accountability principle. Whichever way you do it, you will have to demonstrate compliance. Either by appointing a senior person or an external expert, you will still have to demonstrate compliance and the fundamental principles will not change data subjects will still be able to complain.
2.9.	**DSARs** *The government considers introducing a structured fee regime for access to personal data, a cost ceiling to address data controller's capacity constrains and amending the threshold for responding to DSARs, potentially allowing controllers the ability to refuse requests that where access to personal data is not the purpose of the request.*	As the cost ceiling for the DSAR response is not being taken forward, can you provide us with any input into what, if any steps, the government is considering to make responding to DSARs more manageable for businesses.	**ES**	We are looking at altering the threshold from "manifestly unfounded or excessive" to "vexatious or excessive"
2.10.		The current threshold to refuse a DSAR ("manifestly unfounded") appears to have little practical effect because controllers are generally reluctant to refuse a fundamental right including where DSARs are "weaponised", such as within the context of some employment disputes. The consultation paper and ICO response again stress the fundamental nature of this right so there is risk again that changing the threshold to "vexatious" may have little practice effect particularly given the high standard applied to the word as a result of FOIA case law: *"the starting point is that vexatiousness primarily involves making a request which has no reasonable foundation, that is, no reasonable foundation for thinking that the information sought would be of value to the requester or to the public or any section of the public…… The decision maker should consider all the relevant circumstances in order to reach a balanced conclusion as to whether a request is vexatious"*	**ES**	I would absolutely agree that businesses are nervous and this is our rational for our proposal. This is a fundamental right that underpins the other right: access leads on to rectification or erasure. However, companies are struggling to deal with the subject access requests because of the volume or they are nervous about refusing requests. We are looking at excessive or "vexatious" instead.
2.11.		"Vexatious" is currently used in FOIA and there has been significant case law and guidance on this word which, in practice, may also make it difficult to rely on so organisations may be reluctant to refuse requests not withstanding the change in threshold (i.e. will it make much difference in practice?).	**ES**	Acknowledge that the FOIA interpretation carries complexities. We are not yet decided whether to import the FOIA version of the word, or to define our own criteria for "vexatious" (i.e. the FOIA case law/interpretation may not apply to DSARs).
2.12.		What do you consider to be the practical differences between "manifestly unfounded" and "vexatious". E.g. in a FOIA, organisations can look to the "value" of the request – does this mean that intention behind a DSAR becomes a relevant factor?	**ES**	You will have to wait for this.
2.13.		Will there be more clear-cut guidance on what the ICO considers a vexatious request in the context of DSARs, particularly with respect to weaponised DSARs? Or bulk DSARs from claim management companies?	**ES**	Our reform is how we define "vexatious", we are looking for more clarity. We are looking for all kinds of things in our toolkit. "vexatious" may not necessarily follow the FOIA definition.
2.14.		If DSAR approach is being modelled on FOIA, will individuals be given additional appeal rights if dissatisfied with the ICO's response to complaints e.g. appeal to the First Tier Tribunal?	**ES**	Question not posed due to time constraints.
2.15.		My understanding is that EU GDPR imports proportionality, but our law requires writing in proportionality if we want that to apply. I do not think you find this in legislation. Is that right? And if not, shouldn't we write this in?	**ES**	I do not know the answer to this, as Robin alluded to before, proportionality can be hidden in UK terms, for example "necessary" has proportionality baked into it. One of the things we can do is remove the term "proportionate" because it's already included in the term "necessary". The overall aim is to ensure that DSARs are done in a proportionate way. Audience: I think proportionality has come across with Brexit but the UK courts and the ICO have interpreted it differently, a nudge may be helpful.
2.16.		Having clear ICO guidance will comfort people, will this be there?	**ES**	In terms of guidance, I cannot speak for the ICO but given the nature of the reform the guidance on DSARs will likely need updating. We will have to see what the ICO put in it.
2.17.		Relating to the "excessive" part of the threshold, the key change with excessive is that "manifestly" is coming out from beforehand. Will this also impact the "excessive" threshold (i.e. "manifestly excessive" vs "excessive"). Can you give any practical examples of this?	**ES**	I will have to take this away to the person who leads on this.
2.18.	**PECR** *The government considers removing consent for the use of analytical cookies and potentially other limited purposes (e.g. detecting technical faults or enabling enhanced functionality) and extended the "soft opt-in" exemption to non-commercial organisations, such as charities and political parties. The government is also considering aligning the ICO's powers under PECR with the ICO's powers under the GDPR.*	We understand that the government intends to legislate to remove the need for cookies banners and that in the immediate term, the government will permit non-intrusive cookies and similar tech to be placed on user devices without consent. • Does this mean that UK organisation may now use analytical cookies and email pixels without consent? Can you give more examples of non-intrusive cookies? How will this be implemented – by guidance, or by changing PECR? How quickly do they anticipate this being implemented? • Is consent still expected for advertising cookies and marketing pixels?	**RE**	Some of you might have heard Julia Lopez on the radio setting out the approach to changes to cookies legislation. In the immediate term there are certain types of cookies that can be treated as strictly necessary. We have been discussing with the ICO which cookies will fall into the non-intrusive categories. If you are collecting statistics on audience traffic to your website and not sharing this with anyone else this may be an example of a non-intrusive cookie. Further examples are functionality cookies presenting the website to the user in the way they have selected. Increasingly people use apps and connected watches to send emergency alerts to relatives or emergency services - cookies that control this may not require consent in the future. We are going to have to build flexibility into the legislation. There would be an initial list on the face of the legislation with an order making power allowing ministers to return to that list without going through the primary legislation process again. If we remove consent requirements for non-intrusive cookies, web users will still get a lot of pop-ups since they relate to advertising cookies etc. Even if we removed the consent requirements for non-intrusive cookies it would not solve the problem. Ministers want us to promote the development and uptake of automatic solutions (see response to 2.16). Not all of this is legislative, some technologies are more developed than others. Alongside legislative measures ministers are keen for us to push forward the technological solutions. This will take a bit of time. We use cookies as a shorthand to cover similar technologies – the above reforms will also cover similar technologies such as email pixels. Reg 6 of PECR does not specify cookies.
2.19.		With the intended move to an opt-out model, would this (in practice) be achieved by using a cookies consent mechanism which is available on the website (and set to opt-in by default) which allows users to toggle cookies to opt-out? Will the opt-out apply to more intrusive cookies such as advertising cookies?	**RE**	

#	Topic / Relevant provision	Question	Rspndr	Response
2.20.		When do you think browser-based solutions could be available?	**RE**	The automated solutions are attractive. If you engaged in an automated system, you would spend more time selecting your choices once (as opposed to click away multiple cookies pop-up boxes and not engaging with these). The benefit of automated technology is that a person can engage in more detail than they would with a tick box that can be switched on or off. An automated solution would be our preference. Key industries will work with the ICO to bring more of these technologies to the market and there will likely be a push at ministerial level to bring these solutions to the market.
2.21.		With extending the soft opt-in to non-commercial organisations, will this mean that the soft opt-in is also extended for non-commercial activities of commercial organisations e.g. can it be used where there has not been a sale or negotiation for monetary consideration?	**RE**	You cannot make a direct comparison between commercial and non-commercial organisations. We are trying to provide a sensible equivalent. For example if a person has shown an interest in something that is not a business e.g. political conference, charities, paying for a membership. There would have to be a previous relationship for that organisation to rely on the soft opt-in.
2.22.		Some commercial organisations offer free products (e.g. webinars, samples, downloads, conferences etc). and are reluctant to rely on the soft opt in since this currently requires a "sale" or negotiation for a "sale", which in turn suggests monetary consideration be paid. If the soft opt-in is to be extended to non-commercial organisations on the basis of a "previous relationship", this suggests that non-commercial organisations will be able to rely on a broader application of the soft opt-in that commercial organisations. Should the soft opt-in be extended to commercial organisations to allow them to benefit from this where this a "previous" relationship as opposed to a sale/negotiation of sale for a price?	**RE**	This was not the focus of the government response but is it an interesting point. We will consider this further.
2.23.		Will the extension of the soft opt-in to non-commercial organisations have retroactive effect? • What type of safeguards do you envisage to protect individuals that do not wish to receive marketing communications?	**RE**	When we extend the soft opt-in there will be safeguards that will be mapped across. There should be an easy way for individuals to opt-out of further communications. None of the measures in the bill will have retrospective effect.
2.24.		Will charities be able to use the new extended soft opt-in?	**RE**	It is in scope, a few of the charities responded to the consultation and were supportive of the extension of the opt-in. There does need to be some safeguards around it. The soft opt in works on the basis of the basis of a previous relationship. This does limit it a bit but charities do have supporters who have attended events or donated before who will be allowed to be contacted. People that have registered a previous interest would definitely be in scope
2.25.		Will we get more communications from political parties on the basis that we pay council tax?	**RE**	No. We would have to define previous circumstances quite carefully.
3.	**BOOSTING TRADE AND REDUCING BARRIERS TO DATA FLOWS**			
3.1.		Overview	**ES**	International data transfers are really important to international commerce and trade, they underpin cooperation for financial institutions, law enforcement, national security etc. Facilitating the free flow of international transfers is very important. Countries, sectors or territories can be found adequate following a thorough assessment of the GDPR regime. We want to strike these agreements with our partners to develop innovative alternative transfer mechanisms. There is a large team in DCMS which is purely dedicated to this (led by Joe Jones). They've been developing the capability and designing processes with this in mind. What they've seen in the past few years is that there was a decrease in stability and increase ambiguity about what is required under the EU process. Our reform is an opportunity to put the UK framework on a more solid footing. Providing stability is a key driver of reform. Reforms will be risk based, outcomes based and reflect that other countries have different frameworks etc. You will have to wait for our draft legislation to see exactly how we will take this approach. One of the countries that is prioritised is South Korea, agreements have been reached after an assessment. Other ones are US following the Schrems II decision, prioritising Colombia, Dubai International Finance Centre, long term work with Kenya, Brazil, Indonesia and Singapore.
3.2.	**Risk based approach to adequacy decisions.** *The government will take forward reforms that enable the UK to approach adequacy decisions by taking a risk-based decision, accounting for the different cultural and legal traditions in which countries operate (and allowing it to take into account administrative as well as judicial redress in the assessment). Decisions will not be reviewed every 4 years.*	In order to find more countries adequate, the criteria are going to have to change/ be less rigid. Which areas will the government allow flexibility on which will be non-negotiable? An obvious example, is whether it will put less weight on overbroad surveillance laws. We saw in the initial proposal that administrative redress rather than judicial redress would be an explicit factor that could be taken into account – this seems targeted at the sort of solutions the US are putting forwards under the TADPF. Can you give any indication as to where the flexibility will be given.	**ES**	I think there is a case for a lot more adequacy decisions to be made even with the existing approach. We want reforms to be more transparent. Reforms will be about maintaining the high standard but better reflect the approach that different countries can protect data through different means. We will be looking at privacy on the ground, to see how it will be implemented in practice. I can't speak to specific criteria but we have published the UK adequacy manual, this includes when it comes to redress what is important is the outcome not the process.
3.3.		Will there be any change to the consideration of the importance of surveillance?	**ES**	The approach is covered in the manual but we will have to see how it is reflected in the actual decisions.
3.4.		Will the UK assessment decisions be a bit shorter than the EU ones?	**ES**	I can't say. Having been part of the UK team that went through the EU adequacy assessment of the UK's safeguards we were keen to make this a more streamlined process. It was very intensive and stressful, we added up the number of questions we had received from the EU and it was well over 1000.
3.5.		If you don't monitor laws every 4 years, what triggers will there be to review (will the UK just let the Commission do the leg work and only act when the Commission/ CJEU has made a finding about a country's adequacy)?	**ES**	there will be ongoing monitoring. This is the best way to be agile, we want to ensure the robustness of framework. It is a very large team with an autonomous power to revoke or grant adequacy. Use of international precedents will be useful but we will do our own assessments. All the Commission adequacy decisions up to the date of Brexit were imported into UK law. The Commission Korea adequacy decision was finalised afterwards which is why it was not imported and has necessitated a UK decision (Korea has recently been found adequate in principle by the UK). We will look back and constantly monitor developments.
3.6.		Presumably by altering the adequacy test, the UK government is trying to make sure there are no Schrems type challenges about its adequacy findings in the UK courts – how does it anticipate that its adequacy assessments could be challenged in the UK courts – presumably through judicial review? If the test becomes too malleable will UK citizens as well as the EU Commission lose confidence in the UK regime? Some judicially policed standard would seem advisable?	**ES**	All adequacy assessments are subject to parliamentary review. The route to challenge will be the same as normal, through the courts. To emphasise our aim is to provide a solid footing to provide a high standard of data protection so challenges are not needed in the first place.

#	Topic / Relevant provision	Question	Rspndr	Response
3.7.		If the Irish DPC does suspend data flows from Facebook Ireland to the US as it was reported to have done last Thursday (in draft form), how do you think the Commission and Max Schrems will react to (a) a loosening of the UK adequacy criteria, and (b) an adequacy finding that the US or Singapore (which has powerful surveillance laws) are adequate before the EU does?	**ES**	I'm not going to speak for the Commission or Max Schrems. Our main point is that we're not changing the adequacy standards, we're just providing more transparency. There are a lot of candidate countries that will be of interest to us. It is possible that we have different priorities than the EU, it is normal and natural for us to find a country adequate before or after them. Our power can be territory or sector based rather than whole country based. Our power is flexible and we will use that in a way that maintains a higher level of protection.
3.8.	**Proportionality of appropriate safeguards.** *Unspecified reforms are proposed to allow data exporters to act pragmatically, practically and proportionally when using export mechanisms, whilst maintaining a high standard of protection for data subjects. This appears to be targeted at transfer risk/ impact assessments.*	Is the idea to relax the standard that Third Countries must meet for adequacy and also relax the standards that exporters must try to establish are in place when using SCCs to inadequate countries? Presumably the legislation is going to have to move away from the Schrems 2 European Essential Guarantees standard so that the ICO can write guidance that is consistent with it. Will that be possible with the ECHR jurisprudence in the background – presumably the Bill of Rights reforms will make it easier to ignore ECHR decisions that set the limits on mass surveillance? Will it say explicitly that exporters can take into account (a) the likelihood of the particular importer being subject to a govt demand, (b) the harm the individual would suffer if such a demand took place? Will it say that provided the assessment is in good faith they will not be found liable for facts that are secret by nature? Will it direct the ICO or DCMS (following the assessments it is undertaking) to make a set of second tier assessments available about the surveillance practices of inadequate countries?	**ES**	Our proposals aren't about relaxing requirements. The EDPB guidance isn't binding in the UK, the ICO is the only source of appropriate guidance in the UK. There is a diversity of opinion and a lot of uncertainty as to the requirements. We want to address the issue of controllers doing too much and being worried that they are not doing enough. This is about taking a risk based approach. We need to take reasonable and proportionate steps.
3.9.		Governments don't advertise how often they use surveillance laws or how. Is this up to the ICO to clarify how far controllers have to go in doing transfer risk assessments or will we see helpful changes to the legislation.	**ES**	Ultimately legislation will be based on the reasonable and proportionate point. In relation to ICO I can't say what they will do.
3.10.	**Power for the Secretary of State to recognise alternative transfer mechanisms.** *This is being included as a future proofing method but allows recognition of other countries mechanisms as sufficient.*	What types of specific alternative mechanisms were considered? BCRs approved by the EU? EU SCCs? Any mechanisms from other countries? The ICO was supportive of this, but it sounded like no detail had been provided to it.	**ES**	The current list of mechanisms is quite inflexible, the ICO and Secretary of State have limited power but there is not flexibility to expand this list. This limits the power to utilise multilateral solutions. This power is about giving the Secretary of State flexibility to ensure we can take these steps. All new mechanisms have to meet new standards to be approved. I can't name specific ones, the EU SCCs are already in our law. Binding corporate laws do constitute a valid transfer. EU BCRs before the end of transition period will be recognised as valid, the new ones will follow the ICO's decision process.
3.11.		If another country comes up with more SCCs can we use those?	**ES**	Yes, this will help to encourage new mechanisms to emerge.
3.12.		Binding corporate rules is a long process, under the new system do you think there will be room for simplifying the process?	**ES**	This is something we can take away and discuss with the ICO. You'll hear more about this from Emily
3.13.		With the UK's approach to adequacy are you going to take an eye on the EU's approach, if the UK starts finding more companies adequate this may challenge the EU's adequacy findings.	**ES**	We have an ongoing dialogue with the EU, they don't have anything equivalent to our manual which sets out how they will make adequacy decisions. We may well find countries adequate before the EU but we are still rigorously testing them. This isn't a real risk to adequacy.
3.14.		Is there anything you can tell us about the process of the discussions from the UK and US in relation to adequacy and how are you approaching their surveillance.	**ES**	The answer is that these will be kept confidential for the moment, I think the same thing is true for the European Commission. Last week, the agreement in principle gives the green light to make the legislative decisions they need. There is no point in the UK replicating this.
3.15.		The UK will do an assessment as part of it's adequacy decision. Is there anything that will be published alongside a UK adequacy decision that may support using the UK adequacy decisions in doing transfer impact assessments from other EU countries to countries that the UK has found adequate before the Commission finds them adequate?	**ES**	The UK adequacy decision itself will be quite specific so there will be information in there that can be drawn from.
4.	**DELIVERING BETTER PUBLIC SERVICES**			
5.	**REFORM OF THE INFORMATION COMMISSIONER'S OFFICE (ICO)**			
5.1.		Overview	**EJ** **GA**	It is not the case that the government is critical of the ICO, it is giving legislative clarity to what the ICO is already doing and allowing it to be held to account. This also enables ICO to go further and give it legislative underpinning to support compliance. There will be reforms to the governance model. Currently the power sits under the Information Commissioner. The change is to ensure that we have good diverse leadership at the top of the organisation and sharing this across the board rather than concentrating the leadership in one individual. The ICO does this already but this gives it legislative underpinning. The new structure moves it to a body corporate, the chair will be the equivalent of the current commissioner. There have been a couple of shifts in that. The chair will be a crown appointment, this will stay and the NEDs will be standard government appointments. The other point is the salary of the Commissioner, this will no longer have to be approved by Parliament since that is not necessary. This change is about retaining and recruiting talent and this does not need to go through a parliamentary process. Currently the list of tasks to be carried out are in the GDPR, the goals and considerations will but put into legislation, a framework will set out the overarching objective and encourage responsible data use. Underneath this it will need to have regard to other areas across the economy. The ICO regulates all organisations across the economy, the new laws recognise this fact and the innovation and growth duty will be reflected in the way it plans its work. The statement of strategic priorities has raised some concern around ICO independency. This is about context allowing a helpful context for government to set out international objectives. This will not be directional, the ICO should consider it when carrying out its objectives but it is not bound by it.

#	Topic / Relevant provision	Question	Rspndr	Response
				The next theme is accountability and transparency, the ICO should set out a forward looking strategy (already being done with ICO 25). Under legislation it will be required to set out the strategy and will need to report against key performance indicators. In a couple of areas it will need to expand and explain how it will use complaint handling. Enforcement- there are three reforms being progressed on enforcement. Broadly the powers are fit for purpose. Where we are introducing new powers we have worked closely with the ICO to support the regulator in its enforcement function. We have given careful consideration to safeguarding powers to make sure they are enforced proportionately. This morning at ICO 25 John Edwards was clear about how the ICO would go forward. One of the words we heard a lot was about clarity and certainty to business as well as being clear about how it makes decisions. Another area of reform is to provide specialist, independent recommendations on appropriate remedial methods. The Government is looking to provide new power to Commission new reports to provide recommendations on how to enforce. We will also introduce the power to compel witnesses to attend interview and answer questions. The ICO is quite reliant on individuals to submit documentary evidence. It is quite hard to make sense of what the documents will mean. There is a lot of to and fro about what documentary evidence is required and being able to call people to interview will assist in this. We are aware that this requires careful consideration of safeguarding and the right not to self-incriminate etc Regarding the deadline following the issue of a notice of intent, the Information Commissioner must inform the individual by way of a notice of intent in order to allow the individual to put the representations together. The ICO also needs time to digest this information. In the context of this there are a number of measures being introduced to bring in accountability and transparency on how the ICO exercises this important function.
5.2.	**Independence of the ICO**	Following responses to the consultation the new chief executive will be appointed by the ICO's board in consultation with the DCMS Secretary of State and the new non-exec members will be appointed via the public appointment process. In addition the process for the Secretary of State to approve ICO codes of practice and statutory guidance is going ahead. How would you respond to the Open Rights Group which has stated that "The UK Data Reform Bill will codify cronyism into law," In particular the concerns are: "The secretary of state is being given the power to arbitrarily amend the Commissioner's salary, issue 'a statement of priorities' to their office, and veto[ing] the adoption of statutory codes and guidance, thus exposing the ICO to political direction, corporate capture and corruption." Is the ICO losing some of its independence and how will this change the way it operates?	**EJ GA**	This is something in the consultation responses that is a concern for some people. I don't think we are at a point where we change the ICO function to doing what the Government tells us. Everything we're doing is in line with other regulators. The salary does not regulate people's behaviour and there are safeguards around that. Board appointments are subject to regulation. There have been considerations of the broader public appointments. Statutory codes and the Secretary of States' consultation. Other regulators have broader powers. There is nothing that makes the ICO an outlier here. From an adequacy perspective there is a higher standard. From the statutory codes points and the ability for the Secretary of State to approve statutory codes, this is not about the ICO's routine guidance. Rather this is a final safeguard about statutory guidance being laid by parliament. This will be something which affects for example an emerging technology which is interpreting the law in a new way. The codes of practice must be robust and inclusive.
5.3.	**New statutory objectives for the ICO**	Are these new statutory objectives more than simply a codification of the existing way in which the ICO works? Although via its official statement the ICO has stated it supports the reforms, anecdotally we have heard from the ICO that these will change nothing as they are already principles by which the ICO operates. Do you agree or do you think these present a shift in focus? Or are these changes like the name change of the ICO, and in practical terms, they will change very little?	**EJ GA**	I think it goes beyond just codifying what the ICO is already doing. It's about greater clarity. In relation to the consultation duty the ICO works with other regulators. We want real legislative clarity around what is required and legislation recognising the ICO's role. It is part of the ICO's objective to encourage trustworthy use of data. Data must be allowed to be used in a responsible but also innovative way.
5.4.	**Technical reports**	These may assist in providing impartial analysis and assistance to the ICO in relation to complex or technical breaches. Will the costs of these be borne by the companies under investigation and how will the remit of these investigations be circumscribed in order to ensure that the work is not duplicative of work already commissioned by the company itself? Will the ICO have a list of skilled persons that would be acceptable to it to undertake such a review?	**EJ GA**	Speaking to the second point the first output of the report should be useful to the ICO and also to the organisation in assessing its own measures where there has been a breach and recommending how to take remedial action. In the context of how it will be used as with existing powers, and without speaking for the ICO, all these decisions are taken on a case by case basis, the nature of the harms, how egregious the harms are etc. We certainly expect that these will apply to these provisions as well. We are exploring who will pay for this.
5.5.		Will there be a list of skilled people that it will be acceptable to use	**EJ GA**	We are looking at precedent for existing processes
5.6.		You say you're looking at the Irish model, how often do they use technical reports there?	**EJ GA**	I don't have the numbers but they do use them. It is difficult to predict but we will anticipate that the powers will not be used frequently. They will be used on a case by case basis, its not something they'll jump into lightly. If the company has commissioned its own report the ICO may not need to use this power. The legislation provides a tool that they are able to use.
5.7.	**Discretion not to investigate complaints**	Other than vexatious complaints and complaints where the complainant has not tried to resolve the complaint with the data controller, what other grounds might DCMS include in the legislation to allow the ICO not to complain (eg where insubstantial harm caused to data subject)?	**EJ GA**	At the moment these are the two that we are expecting to use in the legislation. The ICO has a huge number of complaints every year. We don't want to see the regulator having a huge remit and being bogged down with low level complaints. We want to allow the regulator to avoid being involved if it doesn't need to be. This allows the ICO flexibility in how far it takes the complaint. There is a level of discretion in how you use the legislation and communicate to people. That is what they're doing and there is a wider discretion that already exists.
5.8.	**Codes of conduct**	Have there been examples of the ICO getting its guidance wrong in the past that justify the Secretary of State having veto powers over codes of conduct going forwards? Given these codes will have impact assessments and been through expert panels why does DCMS see these veto powers as necessary?		[Rationale for code of conduct review discussed in question 5.2 above]
5.9.		Will there be a fixed timescale for guidance to be published by the ICO to reduce period of uncertainty for businesses as to how to interpret and apply the reforms?	**EJ GA**	Changes in the law in their nature raise questions from the business. We are working with the ICO to work out parts of the legislation when various elements will be commenced and to ensure the ICO has capacity to provide support to businesses. There is no set timeline at this stage but we are working with the ICO to be able to produce guidance so when things are introduced they will be able to support questions.
5.10.		In the vexatious complaints points, is there going to be similar clarity around the meaning of vexatious in this context as compared to DSARs?	**EJ GA**	Yes, they will align.
5.11.		On the technical reports, will there be appropriate safeguards for legal privilege and how we go about making sure that is in place?	**EJ GA**	Legal privilege will remain in place. A lot of this depends on existing good relationships and legal privilege should be maintained.

#	**Topic /** Relevant provision	**Question**	**Rspndr**	**Response**
5.12.		Going back to talking about the governance piece and that th isn't anything new, the question that comes to mind is that whether is a genuine need for the changes to happen?	**EJ GA**	I think this is not just about precedent but it is about a diversity of decision making so the huge amount of decision-making doesn't rest on one individual. You would never design it this way now so if you can share responsibility this is what you should do.
5.13.		Is anyone worried about the ICO's objectives to being a more economic regulator and if that will affect their human rights origins?	**EJ GA**	As part of the consultation we had mixed views on this. There was a recognition that the ICO is working fine as it is. There is recognition of the breadth of the impact but this wasn't something we had huge pushback on. We do collaborate with Ofcom and other economic regulators.
5.14.		Any hints on the new name?	**EJ GA**	No hints, we won't go too far off kilter. This is a ministerial decision