**Data -a new direction**

**Comments on the consultation from the BRC**

**November 2021**

**Contact: graham.wynn@brc.org.uk**

**About the BRC**

The BRC is the trade association for UK retailers and our membership comprises over 170 major retailers - whether operating physical stores, multichannel or pureplay online - plus thousands of smaller, independent retailers through a number of smaller retail Trade Associations that are themselves members of BRC. Our members deliver an estimated £180bn of retail sales and employ just over 1.5 million colleagues. Our purpose is to make a positive difference to the retail industry and the customers it serves, today and in the future

**Overview**

Retail is the sector that relies more than any other on maintaining consumer trust – whether it is consumer protection, product safety or in this case personal data security and protection.

Customers supply their data trusting it will be kept secure and that it will be used for the purposes intended and described, in compliance with applicable rules and ethically. If consumer trust is lost, years of goodwill and good reputation can go to the wall in this sector in a way that is far more direct in its consequences than in a less competitive sector.

With the strong move to online selling and the introduction and potential of other new technologies, retail businesses have invested, and continue to invest, in systems, processes and people to ensure customer data is safe and its usage is ethical and compliant.

The key to any acceptable reform is that it allows businesses to retain customer trust; that customers can understand how their data is used should they wish to do so; that there is a simple means for the business to understand the data it holds on a data subject; that the data it holds can be kept secure; that there is a means of redress when things go wrong; and that the system does not unnecessarily inhibit innovation and competitiveness but rather facilitates it in a responsible manner.

In assessing the proposals, the BRC has applied some basic tests:

* The Customer/data subject – are the proposals good for the customer in maintaining a high standard of data protection and customer trust – not least when competing with global businesses for customers in the UK and the rest of the world.
* Burdens on business – do the proposals genuinely lead to reductions in the burdens on business or do they either substitute one burden for a similar burden under a different name or even add to the burden by requiring businesses to work to both the UK regime and the EU regime, for example, in order to maintain an EU customer base.
* Growth and innovation – do the proposals support the objective of continued innovation and development of new technologies and services in the rapidly evolving and increasingly digital global economy by encouraging responsible use of data.
* Adequacy – do the changes potentially undermine adequacy with the EU without securing offsetting gains? While there are areas that could be improved in the current UK data protection legislation and the UK should not feel obliged to reflect every change the EU may make for evermore regardless of our own assessment of its desirability, changes in the UK should only be made based on real evidence of overall value for the UK. Adequacy with the EU should not be sacrificed for small changes of no great importance or slight changes in roles or their titles which, regardless of their value, might be perceived by others as undermining adequacy.

Overall, judging against these tests:

* We are of the view that some proposals could work to improve consumer/data subject trust. The cookie regime has fallen into disrepute with data subjects simply agreeing to everything in order to get to the information or purchase they are seeking. The changes proposed could increase the trust that consumers have in appropriate data management as the mass requirement for cookies has decreased trust- in the belief that it is purely a tick-box exercise, rather than a well-thought out proposition. By making everything high risk, you end up making nothing high risk. Additionally, by reducing the burden on SMEs to get things right, this provides overall greater trust in the system. So those changes could be beneficial for both businesses and for customer trust. On the other hand, our concerns about some proposals are based not only on whether they would assist businesses and innovation – which some might – but whether they could potentially undermine customer trust (and adequacy). For example, these include proposals on breach reporting, removal of DPOs (at least for some consumers who understand their role); voluntary undertakings if businesses are fined for the same action in the EU but not the UK; and the suggestion that the ICO might not assist with or investigate all complaints.
* Some proposals could potentially (though the jury is still out on these) help relieve the burdens on business and encourage innovation such as SARS, Cookies, voluntary undertakings, ideas for research and reuse of some data with protections; an understanding of AI as the need to regulate its uses in various different scenarios rather than the technology itself; and potentially the changes to legitimate interests assessments.
* Many of the proposals in the first chapter should serve to assist innovation and technology – or at least have the potential to do so provided it is understood that regulation in general should not regulate a technology but how it is used in a range of different situations and provided that private business research, technology and development is included in the definition. Clarification of the approaches to further processing, the legitimate interests tests, data anonymization and AI and machine learning concepts could assist this process.
* Several of the proposals, however, raise concerns that they do not help sufficiently to overcome the potential threat to adequacy. Some are marginal like prior consultation with the ICO; some like changes to DPOs and DPIAs bear the hallmarks of a substitution of one type of requirement for another very similar but with reduced efficacy and a similar workload; others like breach reporting do not eliminate the need to do the work but eliminate the need to properly report it.

We welcome the commitment to place the protection of people’s personal data at the heart of any new regime. That is vital to maintain the trust of our customers and data subjects – in turn vital for them agreeing to share their data, and particularly to any desire to have them agree to share it for unconnected purposes.

We also welcome the understanding that the current rules do place some burdens on business – the test being whether those burdens are necessary to maintain trust and confidence. We welcome the commitment to support vibrant competition and innovation, here as elsewhere, and to keeping pace with rapid innovations in data technology through future proofed, risk based, outcome facing regulation. Indeed, any regulation should always be targeted at the uses of technology not at the technology itself - it should be technology neutral if it is to meet that criterion.

However, there seems to be a degree of conflict between some of the statements in the opening parts of the consultation – both in the Introduction and the Minister’s foreword. For example, the Minister states that the UK now has the freedom to make a ‘bold new data regime’ and ‘aspects of the current system remain unnecessarily complex or vague’ after three years. These statements suggest the Government is intent on quite dramatic change. Set against this is the optimistic, perhaps over optimistic, view that there remains a potential for maintaining EU adequacy while making fundamental changes and other changes that may at least be perceived by others – not least those in the European Parliament which often tends to move in a more restrictive way in this space – as fundamental. In reality the question has to be asked: if the changes are just tinkering – why make them if they may undermine the higher prize? The issue goes beyond the EU to whether other jurisdiction , many of which follow EU standards, may not recognise our regime for adequacy if the EU does not do so. Issues would then arise for onward transfer mechanisms

The BRC believes that it is in the interests of business that maintenance of adequacy should be seen as a strong counter-balance to any proposed changes unless and until the EU moves in a direction that so potentially undermines innovation and change and increases burdens unnecessarily that adequacy is no longer sustainable as an objective.

We agree that some aspects of the system are vague and complex, but in reality the previous regime was still subject to new guidance and interpretation years after being introduced- simply because society, business, technology and potential uses of data change. There is good reason to incorporate some of the recitals in the legal text to give them the force of law – provided it is remembered that in the EU Recitals are in fact taken into account by the ECJ if they are needed to interpret the actual Articles and therefore play a role in the legislation without being a rigid definition. In bringing them within the law, it would be necessary to ensure they do not become rigid requirements. Indeed, we suspect that there will always be complexities that need reinterpretation of the rules. In the absence of that, the rules are likely to be so rigid as to inhibit the innovation and growth the government desires.

Finally, it needs to be recognised there is a danger that businesses will end up having to operate dual systems – which is not simplification -or simply move to the EU regime as the higher level requirement (and this should be permitted). When two businesses are co-operating there will need to be agreement on the regime to be used. For example, would an EU DPO deal with the new UK responsible person?

**Reflections on Chapter 1 – Reducing barriers to responsible innovation**

The BRC will always support reducing barriers where such a reduction is both real and responsible. In assessing the proposals in this chapter, we have taken into account that many of the proposals – re-use of data; technological research; legitimate interests; fairness in AI; automated decision making; profiling; data anonymization - have a wider relevance, use and implication than research and innovation alone albeit they are placed here in that context. They need to work not just for emerging technology but for everyone.

As a general comment on the ideas relating to AI, we would recommend that decisions be made in the overall context of the upcoming AI strategy rather than piecemeal. Having said that, we do not believe that there should be a general AI regulation covering all uses of AI. The use of AI in one industry or sector may well not have the same potential for harm as in another. For example, use of AI in the supply chain has less potential for harm than in a medical or credit situation. While looking at the issue in an overall context, it is the issues not AI that should be regulated.

Research purposes (Q1.2.1 to Q1.2.7)

1. The BRC can support the consolidation and bringing together of research specific provisions. Such changes are nearly always helpful rather than having to wade through a whole range of rules in different places.
2. We note that there seem to be a number of uses of the word research in the consultation that often seem to be used interchangeably. Either the term can be left loose or any definition would need to be absolutely clear as to whether or not the rules apply to technological research in the business context as well as pure scientific research as normally understood- and whether university research means just that ie only in a university. Likewise the definition of technological research would need to be clear – does it include product and service developments, for example? In other words, while a definition may be useful, it may also be challenging to ensure it covers what is genuinely intended and excludes the potential for manipulation at the margins and endless debates over whether a particular activity falls within the definition or not.
3. If business based research is to be included, as it should be, it would seem that a separate lawful ground would assist more than a university specific definition.

Further processing

1. Guidance would be needed on the conditions for claiming an ‘important public interest’. If there were an interactive tool that could be used to provide assurance, that would be useful

Legitimate interests Q1.4.1 to Q1.4.4

1. Legitimate interests are an important basis for data processing alongside consent. It is important that businesses can rely on a clear understanding of when legitimate interest is appropriate as the basis, and the balancing tests that should be applied to determine whether the legitimate interests outweigh the rights of the data subject. Greater clarity, including potentially a list of exclusions from the balancing test, could reduce any barrier to innovation subject to the right exclusions and subject to maintaining customer trust in their application.
2. For the most part Members are on balance supportive of an exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test. It could be helpful to business but it would need to be understood that a business would still need to consider whether its desired action fulfilled *all* the conditions including the needs test and whether the action is proportionate. The implications for the right to object are unclear.
3. The main danger is that organisations would try to fit their project into the list - resulting in debates at the margins on applicability. Some of the activities on the list are very general – using audience measurement cookies to improve webpages frequently used by service users could easily cover a wide range of purposes as could using personal data for internal research and development or business innovation purposes aimed at improving services for customers; and improving the safety of a product.
4. There is also a potential for arguments within a business as to whether the proposed action is covered by the list or not, given the list is relatively generic. This would be exacerbated by removing the respect for the advice of the DPO if the role were removed.
5. In fact the current proposed list tends to be biased towards the use of legitimate interests to overcome harmful actions. That is one sensible aspect – but it does not address the innovation objective even in a modest way such as where use of data could be an intrinsic and expected element of the product or service being supplied or for business intelligence or testing and developing AI systems for internal research and development. Other useful additions to the list could be clarification and detection of fraud, crime and abuse; personal data provision for a service; deidentification for anonymization; improvement of products or services through AI; personalisation of content; use of functional preference cookies.
6. It needs to be clear that actions outside the list remain legitimate and the status of the right to object in relation to the list needs clarification.
7. There will remain a need for and accompanying ICO Guidance - which could be an alternative way forward in its own right – especially guidance on difficult use cases.
8. While we believe it is right to maintain the balancing test for childrens data, it would be necessary to have some sort of de minimis protection for circumstances where limited childrens data may be embedded in wider data.

AI and Machine Learning

1. The top line, as indicated above, is that a General AI regulation is not desirable. Many of the issues raised here are not specifically data protection issues. Defining ‘outcome fairness’ in the context of AI within the data protection regime would not be feasible for all uses. Fairness depends on the context and application.
2. The use of AI in one industry does not carry the same level of harm as in another. Its use in the supply chain does not compare with its use in medical or credit applications. If AI is used to control a car remotely that is different from AI controlling supply lines. It is necessary to consider the risks and then how AI affects them. Based on that any regulation of AI should be in terms of specific uses.
3. The application of AI/machine learning has potential benefits including enhanced accuracy and consistency; safer products; more innovation; and cost savings. Use of personal data in a more free fashion to improve such developments should be part of the commitment to a pro-innovation regime but it would be vital to ensure balancing safeguards.
4. Legislative amendments could improve the operation of Art 22 – but it should be retained as a safeguard for individuals and to retain their trust and provide opportunities for redress.. Greater clarity on the meaning of ‘legal and significant effects’ and ‘solely automated’ and ‘similarly significant’ effects is needed. More flexibility to permit automated decision making with those legal or similarly significant effects if the decision is subject to human review processes or other safeguards such as rigorous testing, validation of results and ongoing monitoring would help. This could be achieved by an exception or a revision to state that this category of decisions is not a decision based solely on automated processing.
5. The wording on solely automated decision making needs improvement to clarify exactly what is meant
6. Essentially the call is for more clarity rather than new law; and higher safeguards for higher risk activity.

Data Minimisation and Anonymisation

1. The proposal to clarify anonymisation in legislation could be helpful but it could be just as helpful to provide clarification in regulatory guidance. For example, there are many different methods for rendering some data anonymous (such as differential privacy, minimum dataset sizes,) but to assess whether they are effective to meet the legal standard is often either beyond the competence of the organisation in question or involves too much risk. Thus, specific guidance on whether certain technologies and approaches are effective in rendering something anonymous in the eyes of the law would be helpful – and with changes in technology would need to be kept updated.
2. We agree that enabling an assessment of the capacity to take into account the extent to which the organisation has the ability to reidentify the data subjects could be useful. However, as technology evolves the situation could change rapidly. The issue really needs to be assessed as technology develops against the overall objective rather than in relation to any given technology in time so that Guidance would be preferable to legislation.

**Reflections on Chapter 2: Reducing burdens on businesses and delivering better outcomes for people**

This Chapter provides the meat of the proposals as they affect business. It needs to be considered in light of the fact that businesses have already made the investment in the current system and changes would increase that cost further. International competitive advantage could also be undermined if the UK is thought to have lower standards or if privacy is not thought to be paramount.

The BRC appreciates the understanding by the Government that the GDPR places significant burdens on business to ensure compliance – and the attempt to reduce those burdens while maintaining high standards of data protection.

The consultation has indeed identified areas of the GDPR requirements that can cause problems – breach reporting; SARS requests; PECR issues; need for a DPO or not; completing DPIAs.

1. The test for any change is whether or not it leads to acceptable simplification or whether it is in essence the substitution of one untested and new regime for another – a rebrand rather than something new. Overall, while there may be some useful thoughts at the margins, we are not convinced that a wholescale change is necessarily for the better.
2. The Government needs to reflect on the proposals from the perspective of a business that has sought to be compliant in spirit and the letter.
3. Many organisations have invested heavily over the past 3 or 4 years in establishing systems and recruiting and training staff to ensure they are compliant. A change to the system could undermine that work, lead to yet another bout of recruitment and retraining and requirements for new guidance; and leave everyone in limbo between now and the eventual passage and implementation of any new legislation. For example, would a business go to the bother of appointing a new DPO, if that became necessary – or look for someone who would not necessarily fit the bill for that role but might do so for its replacement?
4. Considerable effort has gone into ensuring the Board understands its obligations and the need to invest in appropriate procedures; in ensuring the DPO is respected and independent and is properly authorized to give impartial advice to the highest levels in the business as is required – advice which is accepted even if reluctantly at times; and recognises its role in ensuring the processes and procedures necessary are implemented.
5. To challenge all that risks undermining what has already been built up in favour of a belief that the procedures are not necessary and were too restrictive – even though the outcomes that ought to be produced by the new system often should be the same as before. The overall message to business from the changes, albeit incorrect, would be that data protection is a less important consideration than hitherto.
6. Overall, those privacy light people in any organisation would believe that their view that there had been too much concern with data protection was justified and the capacity of privacy professionals to constrain non-compliant approaches would be far more difficult.
7. An upheaval could be justified if the current system were not working. We believe that to a large extent it is and that the problems that exist could be overcome by some lesser tweaks. We are not convinced by the suggestion that the current system leads to a box ticking approach – one justification in the consultation for these changes. The best organisations do indeed engage in proactive consideration of their obligations and have in place systems and personnel to oversee compliance.
8. It is true that some may adopt a tick box approach – but that is inevitable with any system where there is such a huge range of diverse businesses that are required to comply. With any system many businesses will want to know what to do and have a list that they can implement so they know they are compliant. That is the case with nearly all regulation – and even more so when the legislation is not prescriptive.
9. The key should be in guidance on the approach to be adopted – so that the first question for any business should be – Is my business and its use of data low or high risk? Both for enforcers and the business that should be the launch pad for what to expect and what is required. If that were to be the basis for assessment – and there were more guidance on how to assess that – some of the issues noted as problems in the consultation (such as the burdens on smaller businesses without much data use) would be reduced.
10. We note para 141 that businesses will not be required to change many of their current processes if they already operate effectively – but the changes that follow seem to belie that statement.
11. While we acknowledge that the EU has granted adequacy to other regimes that do not follow the requirements of the GDPR in detail, as we have also indicated elsewhere, we are concerned that making the changes outlined, such as the removal of the use of independent DPOs and the need for DPIAs and substituting new roles and procedures, could in the UK context be provocative and lead to adequacy being withdrawn – with a flow on effect to other non-EU regimes assessment of UK adequacy. We do not believe that would be a price worth paying for changes of this nature, many of which are in many ways cosmetic or involve the substitution of one type of approach and title for another. In any event, the need to convince others that the changes are not fundamental which is identified in the consultation suggests that indeed the changes cannot be fundamental if adequacy is to continue.
12. Where a business has EU interests as well as UK, it will not help to reduce burdens if it needs to implement 2 regimes – or if its partners in the EU require a DPO to deal with a DPO, for example. When drafting any legislation, the Government should accept that compliance with the current UK regime is evidence of compliance per se. It should not require adoption of the new approach by all – though that does not seem to be the current intention.

Reform of the Accountability Framework/Privacy Management Programmes (Q2.2.1-2.2.3)

1. As the consultation makes clear, organisations already have a responsibility under Art 24 to implement appropriate measures to ensure processing is performed in accordance with the legislation. In many ways this is more flexible than a requirement for a Privacy Management Programme that can be judged at some later date (it is not clear whether the ICO would be expected to audit businesses in the absence of a breach or complaint) by the ICO as satisfactory or not and which places certain requirements on an organisation to have certain roles in place without being clear as to how it should fulfil them. In many ways, this requirement codifies the expectations on a business while removing the more helpful aspects for data professionals and imposing new ones that have hidden requirements. Thus, with breach reporting there is a reduced requirement – but the assessment still needs to be made; DPIAs are abandoned in favour of new undetermined concepts. The work still needs to be done.
2. The consultation itself admits that ‘a strong privacy management programme is likely, in practice, to exhibit many of the same features as the current legislation’ while removing some of the specific requirements. ‘Organisations may wish to use many of their existing GDPR compliance practices to meet the requirements of the PMP’. This is a confusing message – on the one hand the consultation suggests radical reform is needed and on the other that the changes are in name rather than concept.
3. It is indeed clear that smaller businesses – and maybe others – would need guidance on how to approach the development and implementation of a PMP which rather undermines the suggestion that they would reduce the burdens on such businesses, remove the tick box element, and in reality allow greater flexibility.

DPOs (Q2.2.4 – Q2.2.6)

1. In our view the removal of the requirements to appoint a DPO would be unwise. There is already considerable flexibility in determining whether or not one is necessary – with the clear intention that one is necessary for an organisation that deals with considerable amounts of personal data whether that organisation is small or large.
2. The DPO is now a familiar role throughout the UK and EU and recognised by Boards. To throw that away in favour of something that appears very much like a re-brand for something that is functionally very similar or the same does not seem in itself to reduce the burdens on business.
3. Far more information would be needed on the aims and objectives of this change before a full assessment could be made – but it is possible that the objectives could be achieved by underlining that not all companies are required to appoint a DPO, giving more guidance on which do not need one, and improving the understanding of when data processing is regarded as high risk and when low risk and ensuring that criterion is built in to the assessment.
4. The point is not whether small organisations may struggle to appoint an individual with the requisite skills who is sufficiently independent from other duties as suggested in 162 – but whether its data processing activities are such that it should do so. To maintain consumer and data subject confidence in the system would surely require that the new ‘suitable individual’ responsible for the organisation’s data protection compliance should have almost the same, if not the same, skills as a DPO and be sufficiently independent to stand up to pressure from within the business to act or not to act in accordance with the assessment of the ‘responsible person’.
5. At the same time, the Government would be removing the requirement to appoint someone who is recognised – at last – by businesses as having the authority and knowledge to be able to prevent it straying into unwise territory. The existing requirement is for a DPO to report to the highest level of authority.  Unless a DPO has the gravitas and position within an organisation to be able to influence those at the top, it would be extremely difficult to have any teeth and remain independent. The DPO position also comes with the need for an organisation to provide an appropriate budget, skilled colleagues etc – losing that could be disastrous, particularly for large, complex orgs
6. For some businesses, appointment of a DPO in addition to the responsible person (the consultation suggests that such a person would be in addition) would be necessary to deal with EU interests.

DPIA (Q2.2.7 – Q2.2.8)

1. The replacement of the requirement to produce a DPIA for high risk processing with new procedures in regulatory guidance that businesses should consider adopting, risks confusion, failure to properly assess the risks and is no less a burden on responsible businesses than a DPIA with which businesses are now familiar. It could result in businesses trying to squeeze their activities into one or another of the possible approaches if one seemed more likely to be acceptable – or to avoiding a proper assessment altogether. DPOs have built up the authority to require a DPIA and for it to be followed – this would be lost in the confusion of a variety of requirements.
2. There is an issue of how a business with a DPO and DPIAs structure should deal with a supplier that does not engage in DPIAs and does not have a DPO – ie the supplier and the supplied are not acting on the same basis - with potential concerns not least in the event of a breach. Further explanation is necessary.

Prior consultation with ICO (Q2.2.9 – Q2.2.10)

1. The objective of encouraging a more proactive, open and collaborative dialogue with the ICO on how to identify and mitigate risks can be supported. However, there is no reason why an administrative change in approach, if the current system is felt to not be meeting that objective, should not deliver the required outcome.
2. Such an approach is the hallmark of many enforcers these days and is supported in local authorities by the provision of assured advice – which could also be an approach adopted by the ICO which would encourage prior consultation whether or not this proposal is adopted. Whether an organisation had approached the ICO should not just be a matter of mitigation but should be a proactive exchange whereby the organisation receives clear advice on which it can rely.
3. The requirement for prior consultation should be a fallback to try to ensure high risk processing is fully considered by an organisation.

Record keeping (Q2.2.11)

1. The removal of a clear record keeping requirements – which would seem to be necessary for an orderly approach to data protection management – and indeed while still requiring the means to meet the requirements of the GDPR for SARS and other information to be kept - seems bizarre. It can only encourage organisations to be less strict about their records and potentially undermine confidence of data subjects should it be found the right records have not been kept.

Breach reporting (Q2.2.12)

1. For organisations, the proposed changes do not really reduce the burden of breach reporting – albeit it may reduce the burden on the ICO. Whether or not it is necessary to report would still require the same assessment to be made by the organisation – even with guidance on what constitutes a ‘non material’ risk (guidance which could be produced in any case and which might reduce over-reporting).
2. Clarification on the breach threshold and which breaches should be considered serious would be helpful to organisations as any breach requires pulling senior, valuable people from critical tasks to investigate. If it were possible to establish more quickly that a breach is not reportable such investigation and internal reporting could be spread out over a more reasonable period of time and have less acute effects on business productivity.
3. Finally the DCMS does not seem to have considered the position of a business where the breach may affect data subjects elsewhere, especially the EU. To have 2 standards of breach reporting would involve additional work – and data subjects in one jurisdiction with lesser rights and a lesser obligation to report -or at least a different standard – may well have less confidence in the system and wonder why they have fewer rights for the same breach. For the business, the need to report to both the ICO and the EU under different rules would require additional work.

Voluntary Undertakings (Q2.2.13)

1. Voluntary undertakings are a common procedure in some other regulators – of which the CMA is one. Interestingly, the CMA has found them to cause significant problems and is seeking reform of the system.
2. We believe that the proposal as outlined here would replicate those problems and have others of its own.
3. There would have to be clear rules as to how an organisation would need to have acted to be eligible – the decision could not be left to the ICO alone and it would no doubt be subject to judicial review if a business believed it had been improperly rejected.
4. There would need to be a decision as to whether the voluntary undertaking should be made public or not and whether it should be considered as a precedent for other businesses that had suffered similar breaches.
5. There then comes the issue that the CMA has identified as a considerable problem. There will need to be procedures for effectively monitoring whether the undertaking has been implemented or not – and if not the appropriate punishment.
6. If the ICO believes the undertaking has not been implemented, how does it secure compliance? The CMA has found that going to court to secure compliance with an undertaking can be a lengthy and costly procedure given all the avenues for appeals.
7. Even if the court gives an order, getting compliance with that order is not straightforward – it can require further court proceedings and appeals.
8. The whole process is exacerbated where there is no admission of guilt and one of the proposals is to attach an admission of guilt to any voluntary undertaking so that there is no need in the absence of fulfilment to go back to the beginning and prove that also.
9. Thus while it may appear an easy solution, it may not turn out as expected. In our view, a more effective procedure where a business is considered generally compliant and wishes to put right what has gone wrong (though the considerations involved would still need to be appealable) would be a suspended fine accompanied by an agreement on what is required of the business.

Subject access requests (Q2.3.1 – Q.2.3.5)

1. The Government is right to identify SARS as a burden on many businesses, particularly when they are used in pursuit of a claim for other non-data protection reasons such as an employment issue or when they come via a third party that is often found to be making a request without the knowledge or permission of the data subject – but on which the ICO has failed to provide protection to businesses. The system is open to abuse by organisations seeking personal data to which they are not entitled and to use it for criminal or unlawful purposes should it be provided.
2. We believe one appropriate answer to these problems would be to require third parties to register with the ICO if they wish to submit multiple requests and to abide by a code of conduct to retain their registration under which they would ensure that such requests were made with the knowledge of the individual as to the nature and content of the request, that they supply that individual’s contact details for verification and it is for the individual to provide any information received back to the third party and not for the business to provide that information to the third party.
3. We would support the introduction of vexatious requests where they could be denied when the purpose is clearly not for data protection reasons and a better definition of ‘manifestly unfounded’ to include requests that are not for data protection purposes. These may well obviate the need for charges.
4. We are not convinced a cost threshold would necessarily help a business as we have a concern that it would lead to a debate over whether a business was simply inefficient in meeting the request, as has happened under FOI requests. Indeed it would tend to assist those whose record keeping arrangements were not as good as they should be – and could undermine a potentially legitimate request that requires time and effort and cost for a response.
5. A request fee could provide some relief especially where a business receives unfounded multiple third party requests. It could deter requests made on the initiative of a third party without the understanding or knowledge of the data subject – or in the absence of the fee enable a business to decline to act. A modest fee is unlikely to deter a legitimate individual request. Its application should be voluntary for a business in order to avoid any collection burden on a business that has minimal requests or where a business believes it might undermine trust among its particular customer base.

Privacy and electronic communications (Q2.4.1 – Q2.4.9)

1. The BRC would support simplification of the cookies regime. Customers do not engage with the consent rules – indeed nobody really gives valid consent because they believe they are forced to do so to get to the website content and generally simply agree.
2. In particular we would support the removal of consent for analytics cookies where these are necessary to provide the service or introduction of consent via a browser setting as and when there is sufficient alignment of standards and trackers to deliver consolidated settings that can allow a smooth user experience across all websites. We could also support removal for wider purposes though we have some concerns this could be open to abuse and undermine trust in the system. We would expect guidance on the status of any personal data collected were a SARS to be submitted.
3. Consent requirements could be replaced by more principles based lawful options such as legitimate interest in processing data
4. The caveats would be that it would be desirable to avoid two or more cookie regimes (UK and EU in particular).
5. We would also support further consideration of the soft opt-in regime and its extension to all the businesses within a group, for example, to allow for cross-selling to take place, especially when it is clear to the individuals that the different businesses are all part of the same organisation.

PECR enforcement regime (Q2.4.16 – Q2.14.18)

1. An increase in fines would be a significant change because most ICO enforcement activity comes under PECR rather than Data Protection.
2. The balance to be struck is to determine whether a breach of PECR is as serious in its potential harm as a breach of Data Protection rules. Is it more akin to a nuisance or not?
3. In our view, it is probably not usually as serious as a GDPR breach but realise it can involve a deliberate massive breach.
4. The fining system should reflect the difference between a breach of cookie rules where valid consent is not really possible under current rules and a breach of the rules on nuisance marketing, for example. Were there to be changes to the fining system, there should be changes to the consent rules as suggested.

**Chapter 3 – Boosting trade and reducing barriers to data flows (Q3.2.1 -Q3.6.3)**

1. For the BRC the main message is as far as is possible to avoid undermining the adequacy agreement with the EU – both in its own right and for the implications of the removal of such adequacy for the decisions of other countries and onward data flows.
2. At the same time we can support new routes for international transfers that complement rather than replace existing ones – remembering that businesses have set up systems already to handle their transfers.
3. We accept that we should not be at the mercy of future EU decisions on changes to GDPR requirements. However, we believe that the existing requirements are understood in the UK throiugh our previous membership of the EU and that we have learned to live with any problems (and that it may well be possible to iron out some of these as the Government has claimed without forfeiting the benefits of adequacy).
4. Within that context – and subject to not having a negative impact on adequacy in any given instance - we can support proposals to approach adequacy decisions on a risk based basis and focused on outcomes.
5. The BRC has set out in more detail its approach to data transfers in its response to the recent ICO Consultation.

**Chapter 4: Delivering better public services (Q4.2.1-Q4.6.2)**

1. The BRC has reflected on the issues that arose in requests for sharing data in the pandemic. These included requests for access to lists of vulnerable people who could be placed on a priority list for home deliveries and also apparent requests to ask employees their vaccination or covid test status either for assessment of whether an employee should be self-isolating - or to share information with public authorities on the status of infection in a workplace especially one open to the public- and whether or not having asked these could be recorded.
2. As the consultation notes, to a large extent a way has been found to share the data lawfully with public authorities – although often after considerable time and effort.
3. The BRC believes that work-arounds are not a satisfactory way forward in such circumstances -either for the business or the data subject. We would support the proposal for private companies to be able to rely on the public body’s lawful grounds for processing the data in circumstances where the data is to be supplied to such authorities.
4. We fully support the protection of individual rights regarding sensitive data and its revelation to and recording by employers. This could easily be misused. That should remain a private data protection matter subject to all the usual rules and only be permitted where the information is needed by a public health authority for a specific purpose in a declared public health emergency – and only be used for that specific stated purpose. It should also be possible for the data subject to supply the information direct to the public health authority.
5. Issues have also arisen relating to the exchange of information between businesses and law enforcers and among businesses in respect of known or alleged criminals who may be or become present in an area. The law needs to be clarified to make the extent information can be shared and in what manner explicit.

**Chapter 5- Reform of the ICO**

The BRC is reluctant to support most of the proposals in this section which seem to amount to an attack on the independence of the ICO and excessive government interference. We also reject the idea that the ICO should not investigate all complaints – an approach that would undermine confidence and trust in the system and provide a field day for the disreputable – unless there is an alternative body introduced to deal with complaints on a legal not adr basis.

1. The BRC is a strong supporter of the work of the ICO – and we are a strong supporter of it acting as an independent enforcer and adviser that can take on public authorities as well as private.
2. We note that it has built an international reputation for a common sense, risk based, consultative approach to enforcement and guidance in comparison to the EDPB – and we anticipate that freed from the requirements of the EU it can develop that approach further.
3. We also note that an independent regulator – which we believe the new proposal would undermine – is a requirement for adequacy in the EU.
4. We do not believe the Government has made out a convincing case to change its structure. Any desirable changes can be made without a wholesale restructuring – including its horizon scanning and intelligence gathering functions to keep pace with new technologies; early intervention to prevent widespread harm; outreach to new sectors using data in new ways; and support for medium and small businesses. Such changes may require a change in funding arrangements.
5. Likewise we were not convinced by many of the proposals for regulators in the consultation on ‘Reforming the framework for better regulation’ (quoted in this consultation as evidence of a better approach) which we believed were ill conceived and poorly argued in terms of regulators powers.

Strategy, Objectives and Duties (Q5.2.1- Q5.2.5)

1. The BRC believes that the ICO has managed to fulfil the expectations of it without a statutory framework that sets out its strategic objectives and duties. There is no reason why it should not be able to take account of competition, innovation and economic growth without being forced into a statutory framework subject to change by one government after another.
2. In particular we oppose the government proposal to introduce a power for the Secretary of State for DCMS to prepare a statement of strategic priorities for the ICO. The justification that it would bring it into line with regulators such as Ofcom, Ofwat and Ofgem is not convincing. The ICO has responsibilities beyond any given sector and in particular to act on behalf of data subjects.
3. We have no objection to the overarching objectives which almost go without saying.

Growth and Innovation Duty/Competition Duty/ Duty to cooperate (Q5.2.4 – Q5.2.8)

1. The consultation clearly has little faith in the value of the Regulators Code, given the statement that this duty largely replicates the requirements therein.
2. It is difficult to argue against a duty to ‘have regard’ to such factors – whatever that may mean – but the consultation does not fully substantiate the need. The ICO has a unique and different role from economic regulators – it is there to secure trust and confidence in the use of personal data and it is difficult to do that if it has half an eye on a balancing duty. In what situation would it be expected to compromise a decision on personal data use because that use assisted growth and innovation? The decision should be made in its own right – though without undermining growth and innovation unless the specific instance used data in a way incompatible with data protection rights. Such an approach does not in any way compromise working with other regulators to ensure their approaches to issues align with data protection needs.
3. In all this, we question the need to impose duties on the ICO against which it is to be measured. There is no point wasting resources constantly reporting against duties as opposed to having an overall approach to its prime objective. The role of legislation should be to ensure the pathways for co-operation are open rather than impose new duties.

Statement of strategic priorities (Q5.2.11)

1. The proposal for the Secretary of State to periodically prepare a statement of strategic priorities to which the ICO must have regard- so that the government can convey the domestic and international priorities that form the context for ICO actions seems to reflect proposals for government interference in other erstwhile independent agencies such as the CMA. To suggest the ICO will not be bound by the statement is somewhat disingenuous given the way these things work – not least if access to funding is at stake.
2. We can see no justification for such a requirement that could equally well be delivered by a less binding statement.

The ICO’s International Role (Q5.2.13)

1. We remain unconvinced by the idea that the ICO should have a statutory objective to consider the government’s wider international priorities when prioritizing and conducting its own international activities. Once again the Government seems to be trying to put the ICO into a straitjacket when any Commissioner of any note would be likely to do just that without being required to do so, The objective is not argued convincingly in the consultation.

Governance Model and Leadership (Q5.3.1)

1. The consultation has not provided a reasoned justification for such a change – relying instead on the suggestion that other economic regulators have a different structure. We do not believe that is in itself a justification and it fails to recognise the ICO is not an economic regulator.

New Reporting Requirements (Q5.4.2 – Q5.4.6)

1. Annual reports even with KPIs are seldom fully debated in Parliament and, if they are, they are soon forgotten. The proposal runs all the risks in tying the ICO down in a bureaucratic nightmare at a time when the Government claims to want to free up regulators.

Codes of Practice and Guidance (Q5.5.1 – Q5.5.2)

1. While we support the ICO consulting on its guidance and codes we would observe that it already does so. It is not stated what would constitute ‘novel guidance’ which would require enhanced consultation or why the ICO should be forced to set up a panel of persons with relevant expertise when developing codes or complex and novel guidance – any more than the Government does. Stakeholders will be expected not only to address the ICO but also these panels which is not desirable. Nor should the DCMS Secretary of State have a veto power above and beyond the Houses of Parliament. In what other area does this exist? If he objects then he should persuade Parliament not exercise a Ministerial veto.

Complaints (Q5.6.1 -Q5/6/4)

1. This is an important and mistaken proposal that could easily undermine public trust in the whole data protection system. It seems to be based on the CMA role in Consumer protection.
2. We have no objection to the ICO taking a risk-based approach, focusing on upstream activities to identify and address problems before they cause widespread harm. As said, that is what the CMA does.
3. However, the CMA has Trading Standards to do the donkey work on the ground of trying to deal with some lower level complaints – though for the most part the whole system has broken down leaving consumers with no redress other than to go to court.
4. The suggestion that the ICO should have a threshold for dealing with complaints, potentially leaving data subjects without any recourse, could easily totally destroy confidence in the whole system, undermine willingness to share data, and leave the rogues to thrive.
5. Requiring a data subject to go first to the data controller is desirable – provided that there is a limit on time for the data controller to respond and provided that the data subject still has recourse to someone if the answer is a whitewash. If the ICO is not obliged to consider complaints – then who is? The outcome will be a system that is broken as with consumer protection – though even there fallbacks remain to some extent.

Enforcement powers (Q5.7.1)

1. We have no particular objections to the proposals for enforcement powers changes – but there is a risk that some of them such as compelling witnesses to answer questions could tie up cases in endless judicial disputes on process and legal representation and evidence requirements..