Written evidence submitted by the Information and Records Management Society (IRMS) (DPDIB36)

Data Protection and Digital Information (No.2) Bill: call for written evidence

The IRMS is the UK's largest professional body of information, data and records managers, data protection and privacy specialists and information rights managers. Following a survey of its members' views on the Data Protection and Digital Information (No.2) Bill passing through parliament, we would like to submit the results of our survey following the call for written evidence. We have below included the questions we asked, the response by % and a selection of the comments made (full transcript can be found here).

Question:

		% of total respondents
ersonal Data	A. Strongly Agree	1
es amending the definition of personal data to limit the assessment of identifiability to the controller or	B. Agree	18
persons who are likely to receive the information at the time of the processing rather than anyone at any	D. Neutral	13
gree that this will bring positive change?	E. Disagree	40
	F. Strongly Disagree	27

nments:

1.1. Concern how this could disadvantage citizens who are looked-after, care-experienced or have adoptive parents
1.2. This would be a damaging divergence from the EU GDPR and potentially compromise the rights of data subjects
1.3. By restricting this and only considering those who are likely to receive the information, any assessment could be flawed as it doesn't look to see if there would be a wider audience for the personal data and the impact that this may have especially in smaller communities or where someone is very easily identified (eg specific disability or identifying criteria) which may then have an impact on the data subject further down the line.
1.4. What is and isn't personal data and what is considered information which may assist in identifying a living individual must be explicit and easily understood by everyone.
1.5. This could lead to a lot of ambiguity. I am not sure why identification of an individual should be determined by the controller/processor. The term reasonable has also been debated for a number of years. As such, I think the proposed change creates more confusion.
1.6. Whilst I appreciate the attempt to provide further clarity on the meaning of "identifiable" in the context of DP Legislation, I think the proposed redefinition is no clearer, and presents much greater risks if it is misinterpreted.

In assessing whether data is anonymous, controllers will need to either:
1) Assume "persons likely to receive the information" consists of everyone in the world, or,
2) Adopt a narrower definition of "persons likely to receive the information", and then ensure that the data is never disclosed to anyone beyond this initially identified group.

Option 1 is no different to the current regime. Option 2 either means:
a) The controller now has a third category of data alongside personal data and anonymous data: "anonymous but still subject to controls" - i.e. data that can be treated as anonymous in most regards but which still needs to be held in a way that prevents it being disclosed beyond the originally identified group of "persons likely to receive it", or,
b) There is a risk that the controller ceases to apply any controls whatsoever to the data (as there is no requirement under GDPR to keep anonymous data secure.

a) seems needlessly complex and confusing; b) carries the risk that data is reused and reidentified by someone not originally envisaged by the controller as likely to obtain it.

1.7. The definition of personal data is quite well established and broadly understood, at least in our continent. I would question why there is even a need to start messing with the definition.

1.8. There are huge risks here around reducing the scope of data protection law - and the ability for building profiles from partial, yet disparate data sets using AI - that again, may be now out of scope..
The definition also includes the concept of indirect personal data at the time of processing. No one else defines it this way; whislt it may require a balancing assessment on whether indirect data is personal data (what sort of balancing test and what sign-off would be required in a Bill designed to reduce 'the burden' on businesses)- and if the controller thinks it isn't, there will be no transparency or rights available to the data subject.

1.9. I agree: in many cases it is impossible to identify all those who - at any time in future - may receive a given set of information

1.10. Although this will make the publication and use of certain pseudonymised datasets easier, on balance this represents a weakening of data protection rights for all persons.

Question:

	% of respon
2. Defining 'vexatious' Data Subject requests	A. Strongly Agree
The Bill proposes amending the terms "manifestly unfounded" or "excessive" with "vexatious" or "excessive" in Article 12.	B. Agree
Do you agree that this will bring positive change?	C. Neutral
	D. Disagree
	E. Strongly Disagree

2. Comments:

2.1. It aligns with terms in FOI Act. 'Manifestly unfounded' is difficult to apply (ICO don't seem to know either!) so any clarity on this is welcome

2.2. Yes, it will be a positive Change as it would provide the clarity needed for controllers to refuse certain requests

2.3. In the absense of any significant case law, there is a lot of uncertainty in terms of when controllers can rely on the "manifestly unfounded" exemption. Changing this to "vexatious" is a positive step, assuming it allows controllers to rely on previous FOI caselaw when determining whether the exemption is likely to apply. The "vexatious" exemption under FOI does its job effectively without unfairly restricting individuals' rights to access information, and I see no reason why a different standard ought to be applied to requests under UK GDPR.

2.4. The interpretation of these terms will ultimately be determined by the courts and relevant case law

2.5. I don't particularly like either wording, "manifestly unfounded" or "vexatious". Definitely the latter gives too much leeway to avoid dealing with requests that are perfectly legitimate but "inconvenient" for one reason or another.

2.6. This amendment weakens the rights of a data subject.

2.7. Agree, but this has a significant opportunity for misuse.

2.8. For example, if the requirement for an SRI, rather than DPO, is in place, the SRI would likely be the individual assigning the vexatious label. However, in many organisations, the SRI could be involved with the requestor in another capacity - (e.g. a Headteacher in a primary school) and have an existing relationship that may be detrimental to a balanced judgement on whether the request, rather than the person is vexatious.

2.9. This is a positive change as it clarifies the position. It also followed EDPB guidance to a degree.

Question:

		% of total respondents
3.Controller first Data Subject complaints The Bill proposes that complaints made to the Data Controller should be acknowledged within 30 days of receipt and responded to substantively without "undue delay". The ICO will not be entitled to accept a complaint if the Data Subject has not complained to the Controller first. Do you agree that this will bring positive change?	A. Strongly Agree	15
	B. Agree	49
	C. Neutral	15
	D. Disagree	18
	E. Strongly Disagree	3

3. Comments:

3.1. Again, brings it in line with FOI, but could be seen to be a 'watering' down of the importance placed on control of personal data and may increase the time that a data subject has to wait for an acceptable resolution to their complaint.

3.2. This does not provide enough clarity for the data subject or the data controller. We consider it is fair for the ICO to require data controllers to consider a data subject complaint before the ICO investigates. However the lack of an actionable legal deadline for the controller to respond (unlike under FOIA/FOISA) potentially weakens the rights of the data subject

3.3. Yes as we often see issues go straight to the ICO that could have been dealt with quickly and appropriately by ourselves

3.4. Gives data controller opportunity to acknowledge and address the problem rather than the ICO be overwhelmed with minor/unfounded complaints. This is likely to benefit the data subject as well as the controller.

3.5. It will only deliver a greater workload for hard-pressed IG and DP teams who are unlikely to amend their original decision/rationale and thereby delay independent review and satisfaction (or otherwise) of the complainant. ICO decisions, where a complaint is upheld, should result in improvement in the challenged organisation, so delaying that outcome can only be counter-productive

3.6. The open ended timing is concerning - it would be clearer and easier to enforce for data subjects if there was a quantifiable timeline.

3.7. 30 days for a first response is too long. 21 days is sufficient in most cases.

3.8. Whilst treating complaints formally is a good thing - the risk here is that a data subject is continually stonewalled by a controller. It potentially adds a significant amount of time to a process where the complaint may be related to a SAR that was not delivered on time.

3.9. I think it would be fair that a complainant has to complain to the Data Controller first, but not without a specific deadline for a response. 'without undue delay' isn't good enough.

3.10. Although I am concerned about the requirement to make it possible to complain electronically. This may well be disproportionate and burdensome for small organisations. I represent schools who have comprehensive complaints policies already. There is no requirement for other school complaints to have electronic submission methods. This may create a two-track complaints system in schools, where the requirements to deal with data protection complaints are different to other complaints.

Question:

		% of total respondents
	A. Strongly Agree	1
4. Removal of the Data Protection Officer (DPO)	B. Agree	4
The Bill proposes to remove the requirement to appoint a DPO but some public bodies and organisations undertaking high risk processing will need to appoint a 'Senior Responsible Individual' (SRI). Do you agree that this will bring positive change?	C. Neutral	18
	D. Disagree	22
	E. Strongly Disagree	54

4. Comments:

4.1. As a DPO, I have mixed feelings about this (self-interest and job preservation springs to mind!). I believe my organisation has benefited from having a DPO - staff have become more knowledgeable and have a greater understanding of their responsibilities (and also understand more about how their own data is being used/abused). Organisations are likely

to appoint a SRI who will delegate to the existing DPO. Will organisations be making their DPOs redundant - more likely they will continue as there will still be a requirement to demonstrate compliance with the new Bill. For smaller public sector bodies whose processing is limited risk, this will probably be a welcome revision.

4.2. Keep the DPO for all public, private, third-sector orgs - just offer exception for very small & micro businesses

4.3. Again an unhelpful divergence from the EU GDPR. Organisations that process personal data of EU residents will need to retain the DPO. The SRI role is a useful addition in that it assigns senior management responsibility for compliance. However this does not address potential conflicts of interest or require the SRI to have the requisite detailed knowledge of data protection law. Also the change weakens the protection for the DPO to act independently.

4.4. 'Senior Responsible Individual' does not necessarily ensure expertise is maintained. The DPO is an 'expert' and independent role, separate from the SIRO role - these should not be conflated. One looks at adherence to the law, the other takes a view on risk for the organisation - both are needed to ensure compliance and business need is balanced.

4.5. In practice I don't think this will change much. Most organisations with DPOs at the moment have experienced operational staff doing the work and reporting to a senior manager who has that area of responsibility but not necessarily the knowledge to do the work.

4.6. Very concerned about this, a data protection officer is a very clear term for what the role does, a senior responsible individual could get lost with other roles such as SIRO, the members of the public and colleagues won't necessarily realise the difference. Since the revised DPA IG people have worked hard to establish specific terms and people understand these, the change will just confuse. It also may open up organisations to have a SRI who isn't independent and does dual roles therefore creating a conflict of interest which the DPO shouldn't have.

4.7. DPOs are engrained in a number of organisations. If the roles and responsibilities are broadly the same I do not see the sense of re-naming the DPO.

4.8. This measure will have the effect of making companies believe the government no longer takes data protection seriously (which seems to be the intent), thus reducing the resources they put into it. This will lead to many more breaches (particularly breaches of the non-security principles in the GDPR) which cannot be adequately addressed by an already overworked regulator.

4.9. `The EDPB has indicated that the role of the DPO will be enforced more (see Lithuania SA decisions) - this defines a clear difference in direction between the UK and the EU - which potentially has an adequacy impact

4.10. This is a disastrous move for schools, which will make the burden of complying with the law much harder. At the moment, it is economical for them to have an outsourced DPO which means that they can pay a lot less than if they had to train up an internal member of staff. The fact that an internal member of staff now needs to have all these responsibilities will cause significant stress and anxiety for school staff who will need to have an internal person with all the logistical and strategic oversight. School data protection work is highly complex, fraught with issues. To burden an internal member of staff with this responsibility is perverse when the stated aim of the bill is to reduce the burden of compliance. At the moment the DPO can be external and advise a board, with one person internally acting as a 'data lead'. This is working well for our 350 clients!

4.11. Losing the independent DPO will be very negative; it will be placing the responsibility on people who have little interest and less time, and who have a vested interest in the processing happening. It again allows "groupthink" without challenge.

Question:

		% of total respondents
5. Changing Data Protection Impact Assessments (DPIAs)	A. Strongly Agree	9
The Bill proposes replacing the current Data Protection Impact Assessments (DPIA) with a leaner and less prescriptive	B. Agree	25
'Assessments of High-Risk Processing'. Do you agree that this will bring positive change?	C. Neutral	6
	D. Disagree	45
	E. Strongly Disagree	15

5. Comments:

5.1. DPIA system works, why break it?

5.2. Agree as I liken DPIAs to risk assessments which is terminology most lay people understand

5.3. We consider that each organisation already can apply proportionality to its DPIA. Limiting the legal requirement for a DPIA weakens its power as it is an essential tool to apply data protection by design and default to any processing activity. This would weaken the protections for data subjects

5.4. People know what a DPIA is - it is well trained out and understood. A new regime is confusing and pointless. It creates work for companies and institutions to replace something they already have that works well.

5.5. This may allow for more flexibility in how it is done (most follow ICO/EDPB guidance at the moment). As most organisations have a process in place already, I can't see this changing much.

5.6. As with the DPO, the terms DPIA are well embedded in organisations culture and to change these will cause confusion, may lead to risks as if we are only looking at 'high risk' and not risk assessing every new use of data there may be occurrences where things go ahead which needed more review and tighter controls.

5.7. The process is generally complex and time-consuming however, it is essential that an organisation conducts a thorough risk assessment of every activity which processes personal data. A leaner and less prescriptive process is unlikely to ensure appropriate consideration of the risk to the rights and freedoms of data subjects.

5.8. This will enable organisations to take a more flexible approach to such assessments, making them more meaningful rather than a tick box exercise.

5.9. Much of the burden which DPIAs put on controllers currently comes from the fact that they are often carried out even when not strictly required. Better messaging around what is/isn't required under the current regime would have a much more positive impact on reducing the strain than this measure.

5.10. Agree only on the basis that the DPIAs I have seen and worked with were really excessive in length and complexity, so the idea of a "leaner" approach is appealing. Data protection law should ultimately make it easier (or at least possible) for organizations to be compliant.

5.11. Again, this is just tinkering at the edges and playing with words, isn't it? If you have to do an assessment, you have to do an assessment, whatever you call it. And if the new arrangement is less prescriptive, that is just watering down the requirements, which is a bad thing.

5.12. Our organisation has seen a lot of benefits from DPIAs. My DP colleagues are now involved in projects (which they weren't always) at the right point (which they never were previously). This means they have become facilitators, rather than obstacles. Far better all round. This change could undermine that progress.

Question:

		% of total respondents
6. Accessing adequacy under International Data Transfers	A. Strongly Agree	4
The Bill proposes a new approach to the test for adequacy applied by the UK Government to countries (and international	C. Agree	30
organisations) and when Data Controllers are carrying out a Transfer Impact Assessment or TIA. The threshold for this new	D. Neutral	31
"data protection test" will be whether a jurisdiction offers protection that is "not materially lower" than under the UK	E. Disagree	28
GDPR. Do you agree that this will bring positive change?	F. Strongly Disagree	6

6. Comments:

6.1. It will all be in the wording and whether their is a reasonable definition of the threshold. Will interpreting this prove more of a headache and therefore not result in the efficiencies and reduction in bureaucracy that the Goverment perceives (for those organisations who have not already updated their contractual provisions for transfers)? Will the EU view this in a good light?

6.2. We are concerned that economic rather than human rights considerations may drive adequacy decisions that may compromise the UK EU adequacy decision

6.3. It might make it less arduous to assess each time, especially if more guidance on this is released.

6.4. How will we know if another jurisdiction's protection regime is ' not materially lower'? I suspect that change will undoubtedly cause the EU to withdraw their adequacy decision. Whilst that may not prevent data transfers to the continent, it will result in UK organisations to jump through a lot more hoops.

6.5. Disagree on the basis that if the rest of the Bill goes through 'as is' I believe the UK GDPR will be weakened and not necessarily an appropriate yardstick to compare other territories' data privacy laws against.

6.6. Would ordinarily agree but this legislation is arguably weakening UK legislation

6.7. This is problematic because the threshold is low, and the Secretary of State has a direct control over the ICO due to other changes. This will weaken protections.

Question:

		% of total respondents
	A. Strongly Agree	6
7. Changing the ICO to 'Information Commission'	B. Agree	10
The Bill proposes that the Information Commissioner's Office will transform into the Information Commission; a corporate	C. Neutral	49
body with a chief executive. Do you agree that this will bring positive change?	D. Disagree	18
	E. Strongly Disagree	16

7. Comments:

7.1. Again, this is all in the fine print - will it be truly independent? Who will appoint to the roles? If organisations are spending more of their time dealing with both FOI/EIR and Data Protection complaints what will the new body be doing? The ICO already seems to be transitioning into a different organisation - prioritising FOI re significant public interest.

7.2. It i s important that the ICO remains independent of government for the governance of data privacy and protection in the UK.

7.3. Risk of compromising the ICO's independence as a regulator though undue influence of the Secretary of State

7.4. I think that this change will ensure greater clarity in terms of the function of the ICO (i.e. role and purpose, what they are accountable for etc)

7.5. I would question the independence of an Information Commission as described in The Bill

7.6. It brings the ICO in line with other regulatory bodies.

7.7. The problem here is not the change to a corporate body, but the removal of independence by making the whole organisation under secretary of state direction. Further, not having a commissioner - a visible face that leads on data - will be a negative.

Question:

		% of total respondents
8. New 'Business Data' and 'Customer Data' requirements The Bill proposes that the Secretary of State and the Treasury will be given the power to issue regulations requiring "data holders" to make available "customer data" and "business data" to customers or third parties, as well as regulations requiring certain processing, such as collection and retention, of such data. Do you agree that this will bring positive change?	A. Strongly Agree	4
	B. Agree	7
	C. Neutral	27
	D. Disagree	33
	E. Strongly Disagree	28

8. Comments:

8.1. In certain circumstances (for example National Security) this could be a good thing, however, their must be some clear definition of the circumstances to which this regulation would apply, and that is not open to re-interpretation when it suits.

8.2. Less concerned about business data as we do get a lot of requests for this in different forms so having to release some may be useful. I would be concerned about regulations forcing us to release customer data as that may affect the relationships we have as a local authority with the customers- also need to consider what the lawful basis would be and if there was any scope for this to be an optional thing and if it was consent based how could that be managed. Also think that if it was mandatory there would need to be very clear communication to show that its a requirement from central government.

8.3. The general public are in general, far more cyber aware and conscious of their personal data and how it is used. I believe the majority of the public will be horrified to learn that a Minister or Government department can, at the drop of a hat and on a whim, require that their personal data is made available to someone or something to whom they would not choose to give it.

8.4. Sounds like deregulation to favour business to me- and mot to maintain the protection of the individual's data. I

8.5. Current processes are fit for purpose, This feels like a land grab by Home Office, Security Services etc

8.6. I feel uneasy about how this would work in practice and how transparent it would be eg how can data subjects know whether their customer data will be further processed or be used in a way that may be objectionable or incompatible with their initial contact

8.7. This effectively extends government powers to be able to call in any data they wish for pretty much any purpose. It's a money-making scheme for Tory donors, pure and simple.

Question:

		% of total respondents
9. Updating PECR The Bill proposes that cookies will be allowed to be used without consent for the purposes of web analytics and to install automatic software updates. Furthermore, non-commercial organisations (e.g. charities and political parties) will be able to rely on the "soft opt-in" for direct marketing purposes, if they have obtained contact details from an individual expressing interest. Finally, there will be an increase in the fines from the current maximum of £500,000 to UK GDPR levels i.e. up to	A. Strongly Agree	9
	B. Agree	39
	C. Neutral	13
	D. Disagree	24
	E. Strongly Disagree	15

9. Comments:

9.1. Higher fines for more severe breaches is a good thing as it will send out a strong message to high turnover companies and may have more of an impact. If the revised legislation is to include a caveat that provides for opt-out on each piece of marketing that is received.

9.2. The expansion of the use of the 'soft opt-in' will be very useful for organisations that aren't selling a product or service.

9.3. Think its an improvement for analytics and updates, would be interested to know what level of interest people need to express for the soft opt in, is it emailing or filling a form in for more

info or is it a case of you've looked at a webpage and that automatically signs you up as I think that would be quite intrusive.

9.4. The current cookie provisions under PECR are clearly not fit for purpose, but it's hard to see how this change will reduce the prevalence or irritation of cookie banners, as most websites use cookies that would still require opt-in consent under the new regime. One change which -would- improve things would be an explicit allowance (or perhaps even a requirement) for websites to place a cookie storing a user's cookie preferences, thus eliminating the need to constantly re-affirm them. Additionally, a requirement to have "reject all" AND "object all" (for cookies relying on legitimate interests) options on all cookie banners would be welcome.

9.5. Not sure on the definition of web analytics - my view is that all non essential cookies should default to 'off' and require a positive action to give consent.

9.6. I object to the exemptions but agree with the increase in fines. I welcome the ability to identify geographical location in some emergencies (e.g. medical emergency, fire or other immediate danger, also crime in progress), but not all.

9.7. Cookies - methinks it will have limited impact and a cross-jurisdiction approach would be preferable. I really don't see the point of us going it alone, even though there is a degree of common sense involved.

9.8. This is another one of those legal loophole generators. The increased fine limit is encouraging, but if the law becomes too woolly, I doubt companies will ever actually be fined such amounts.

9.9. No, I do not agree as often charities and political parties may become more invasive than companies. Also, increasing fines is useless when legal loophole make life easier for trespassers

9.10. The soft opt in provisions for charities and other non-profits is distinctly welcome, and levels the playing field with commercial organisations... but will of course result in more spam for the individual.

9.11. The fine changes are positive; the cookie changes are very negative. It's pretty easy to set up a wholly-owned charity of a commercial organisation and allow that to run your website for example. Web analytics is not just web analytics - Google's web analytics includes non-identifiable processing for advertising, for example.

Question:

		% of total respondents
10. Definition of 'Scientific Research'	A. Strongly Agree	1
The Bill proposes that the definition of scientific research is amended so that it now includes research for the purposes of commercial activity. This expands the circumstances in which processing for research purposes may be undertaken, providing a broader consent mechanism and exemption to the fair processing requirement. Do you agree that this will bring positive change?	B. Agree	21
	C. Neutral	22
	D. Disagree	31
	E. Strongly Disagree	24

10. Comments:

10.1. This will be welcomed by business, the new definition is still open-ended. How will this broader definition apply to privately-funded tech development in practice? Research into public health only constitutes scientific research which seems to reflect the existing ICO guidance.

10.2. It's unnecessary - current legislation allows this already

10.3. Having worked in and around v scientific research for 26 years. No as phrased here. However when a clinical trial is ran by big international pharma this is a problem.

10.4. Deregulation to aid business not protect the individual

10.5. It's hard to see what this amendment changes, as it was already implicit that scientific research could include research for commercial purposes.

10.6. This amendment is a backdoor to poorly regulated commercial activity.

10.7. The privileging of scientific research over other types of research is short-sighted and illogical, and introduces confusion for users of research libraries and archives. A purposive definition of research that covers all academic disciplines would better serve the

customers of such institutions, and recognise the value that other forms of research contribute to UK PLC.

10.8. The challenge here is the reuse piece - which will allow reuse of data for pretty much any purpose that's defined as "scientific"- this can, and will be abused.. As an example of a use for "scientific" purposes, the Japanese Whaling fleet as been doing "scientific research" on whales under the treaty for many years!

Question:

		% of total respondents
11. Restrictions on Legitimate Interests The previous Bill proposed that businesses could rely on legitimate interests (Article 6 lawful basis) without the requirement to conduct a balancing test against the rights and freedoms of data subjects where those legitimate interests are "recognised". These "recognised" legitimate interests cover purposes for processing such as national security, public security, defence, emergencies, preventing crime, safeguarding and democratic engagement. The new Bill, whilst keeping the above changes, introduces a non-exhaustive list of cases where organisations may rely on the "legitimate interests" legal basis, including for the purposes of direct marketing, transferring data within the organised for administrative purposes and for the purposes of ensuring the security of network and information systems; although a balancing exercise still needs to be conducted in these cases. Do you agree that this will bring positive change?	A. Strongly Agree	4
	B. Agree	22
	C. Neutral	30
	D. Disagree	33
	E. Strongly Disagree	10

11. Comments:

11.1. It expands the scope for use of legitimate interests as a lawful basis within the public sector, which is welcome. We have used this in a number of instances and have always conducted the balancing test.

11.2. Seems to be giving too much power to multi national corporates, like Meta, Google, Amazon

11.3. Clarity is always good

11.4. Will weaken data subjects' control over their personal data and lead to more spam

11.5. Yet another proposal which will undermine and diminish the rights and freedoms of individuals. If an organisation wishes to rely on that lawful basis, there has to be a thorough documented assessment proving that the processing is to the actual (not perceived) benefit of individuals. In particular where that processing involves direct marketing and transfers of data.

11.6. For some companies yes, this would be beneficials if they have other strong controls to govern data proteciton and privacy. For the Meta's out there, it's a licence to do even less and get away with it.

11.7. Removing the balancing test for "recognised" legitimate interests will harm people's fundamental rights and freedoms. There is no good reason why these interests (important though they are) should be given such primacy that individuals right are not taken into account at all.

11.8. Most organisations have found alternatives to legitimate interests

11.9. The removal of needless paperwork for routine processes is welcome.

11.10. This is a reasonable change, but it has potential for abuse, so we will need to see if it is positive or negative.

Question:

		% of total respondents
12. Definition of Automated Decision Making The previous Bill clarified that its proposed restrictions on automated decision-making under Article 22 UK GDPR should only apply to decisions that are a result of automated processing without "meaningful human involvement". The new Bill states that profiling will be a relevant factor in the assessment as to whether there has been meaningful human involvement in a decision. Do you agree that this will bring positive change?	A. Strongly Agree	1
	B. Agree	24
	C. Neutral	37
	D. Disagree	21
	E. Strongly Disagree	16

12. Comments:

12.1. Does the presence of profiling indicate that there has been minimal (as opposed to meaningful) human involvement. The provision may clarify when profiling should itself be considered an automated decision and therefore subject to the Article 22 restrictions.

12.2. The landscape of AI/LLMs is changing so fast this year, should re-visit when the Bill closer to final readings

12.3. I think there should be more information on what is classed as profiling for example thinking about the supporting families programme where government expects LA's to be matching families against criteria and have to undertake some level of profiling to identify if they meet the criteria

12.4. The growth of AI is inevitable and unstoppable, but will a machine ever know better than a person?

12.5. There is a concerted and deliberate weakening of oversight here in relation to automated decision-making. There appears to be an obsession with de-regulation equating to business-friendly and that reducing human oversight will attract big tech to invest in the UK where, as commercial companies, they can do all the R&D that they like using AI, without having to worry about data protection.

12.6. The rise of AI technologies (and their existing use of by the public sector) really should not be incompatible with data rights. These technologies will succeed where there is a structured framework for them to operate. Providing a wildwest for AI and automated processing will have unforeseen negative consequences for data subjects - and with the pace of change in AI that we see right now, this law will already be behind where it needs to be in relation to this area.

12.7. What does it mean? Either there is "meaningful human involvement" or not. If not, then it is inappropriate to use the term "automated processing". This modification may lead to confusion, problems and misinterpretations

12.8. Any weakening of the right to have a human decide your case erodes the rights of the data subject.

12.9. It's a weakening of the protection - and will be abused, because meaningful is not clearly defined.

Question:

		% of total respondents
13. Narrowing the criteria for ROPA (Record of Processing Activities) The previous Bill streamlined the required content of ROPAs. The new Bill exempts all controllers and processors from the duty to maintain a ROPA unless they are carrying out high risk processing activities. Do you agree that this will bring positive change?	A. Strongly Agree	10
	B. Agree	25
	C. Neutral	15
	D. Disagree	31
	E. Strongly Agree	18

13. Comments:

13.1. We have a corporate information asset register and alongside it sits our ROPA, both are proving useful tools in knowing what data we hold, where it's located and age. This helps both with ensuring that we don't hold onto personal and redundant data for longer than necessary. Staff have really got to grips with this and it reduces the amount we are storing which in turn reduces storage costs and carbon footprint. Without a ROPA it is quite difficult to manage SARs. I think many organisations will continue to work with and update their ROPAs regardless of change in the legislation.

13.2. ROPA duplicates so much of what is assessed in Information Asset Register - why duplicate?

13.3. Think it will reduce the workload however it is not clear to me as to whether the need to create a RoPA is in respect of high risk processing activities only or for all activity as long as some of what a Controller does is high risk

13.4. If an organisation does not have an accurate and up to date record of what personal data it processes, for what purposes and how long, where the data is held, including data

processors and sub-processors and with whom data is shared, how can an organisation comply with its duties under data protection law and the rights of the data subjects?

13.5. RoPAs are useful for many aspects of compliance, so not sure this will be positive - less time consuming perhaps! Only really helpful if they set out what 'high risk' means.

13.6. As with DPIAs, this makes things less clear for data controllers as the ROPA has other benefits that are necessary to comply with the legislation (eg documenting lawful basis that means you know what rights individuals have depending on the purpose of the processing). Furthermore, data mapping was already recommended in DPA 1998 and GDPR provided further clarity on what this meant.

13.7. Yes most ROPAs are overcomplicated, but it is vital that an organisation can demonstrate what personal data it processes and why.

13.8. Having a RoPA (including Asset Register) is essential in locating information

13.9. Those organisations that have a RoPA, maintain it and use it not only for data protection but for informing business decision-making and looking and processing risk and efficiencies, will continue to do it, because it makes business sense.

13.10. TThe removal of meaningless paperwork for low value, low risk routine processes is distinctly welcome.

13.11. This will simply allow controllers and processors to document less, which will lead to more errors in handling because things will be done without careful consideration.

Question:

		% of total respondents
14. Impact on UK adequacy by the EU (decision 2025) The proposed changes to the Bill will not affect the UK's adequacy decision. Do you agree with this statement?	A. Strongly Agree	3
	B. Agree	13
	C. Neutral	24
	D. Disagree	28
	E. Strongly Disagree	31

14. Comments:

14.1. The Government think not, but if the UK moves further away from GDPR the the EU may feel it has no choice but to withdraw adequacy, which ultimately could result in more work for organisations in setting up individual contracts with EU partners resulting in a two-tier system for UK and EU data subjects.

14.2. With statements like "not materially lower" for overseas transfers the EU may take that this is at odds with their standards.

14.3. The European Commission have already stated their concerns in this area and we should also be concerned. Loss of adequacy will cost businesses much more than the government propose they can save with this Bill.

14.4. Clearly the EU were already conscious of a likely divergence by the UK, hence the sunset clause. That decision being lost will bring nothing but pain, effort and extra costs for UK data users with ties to the continent.

14.5. The amendments appear to provide more flexibility. However, how would that work in relation to UKs adequacy status is the key question. Will the EU remove their UK adequacy decision and, then what would that mean for UK organisations that need to process the personal data of EU citizens? and also how would UK organisations deal with the onward transferring of data.

14.6. The Bill is clearly geared towards reducing perceived "burdens" on businesses at the expense of individuals' data/privacy rights. It is very hard to imagine the adequacy assessment staying in place if these changes are passed.

14.7. There are numerous ways in which data protection legislation could be carefully amended to clarify and simplify the requirements on controllers whilst ensuring (or even improving) the level of protection for data subjects. These changes would be an opportunity for the UK to lead the way globally, inviting the EU to play catch up. Unfortunately, this Bill

includes several irresponsible, headline-seeking changes purely designed to cut costs (real or perceived) with little care for the consequences.

14.8. The focus of The Bill seems to be on making things easier for organisations who process personal data. Many of the key changes I feel will negatively impact on the rights of data subjects / control over how their personal data is used. I am definitely worried about this, and also about how it will impact on the UK's adequacy decision. I think we're already on 'thin ice' with the EU in terms of data privacy/human rights.

14.9. The UK appears to be diverging quite far from GDPR principles, I would be surprised if this does not create problems down the line in terms of cross-border collaboration and trade. Particularly if the UK messes with the very definition of personal data (as per #1 in this survey).

14.10. That said, I do believe that certain aspects of GDPR have always been unworkable in practice, even more so with the rapid changes in technology and how data (not just personal data) is processed on an everyday basis. The problem is that the UK cannot enact these changes on its own as it seems to think it is able to. No country works in isolation anymore. UK needs to consider more the global landscape in which it operates, in particular its dealing with close European neighbours.

14.11. We are diverging from the EU and indeed much of the world in relation to data protection.

14.12. I can foresee adequacy being at risk from the approaches of the DPADI, but even more so by the Bill of Rights.

14.13. Adequacy is likely to be maintained as a political decision initially, but there are bound to be Schrems-like challenges that would very likely invalidate any such decision.

14.14. Probably my personal politics coming into play, but this government has previous for giving blatantly false reassurances that their actions will not negatively impact relations with the EU. It was clear when the EU originally gave us our adequacy decision for a finite period of time that they 100% expected the UK government to change the UK's DP legislation for the worse in the near future. This is what is now happening. For those proposing the changes to be so blase about how the EU will react is naive at best, possibly dangerous to the areas of the UK economy that rely on data transfers with the EU.

14.15. Given that the EDPB proposed an investigation into independence of DPOs as this year's audit, that proposal in the bill alone is likely to result in loss of adequacy. Added to the reductions in other rights, it seems very likely we will lose adequacy - not even taking into account the terrible mishandling of the meeting with the EDPB last year!

May 2023