



Sir Chris Bryant MP
Minister of State for Data
Protection & Telecoms
Department for Science,
Innovation & Technology
100 Parliament Street
London SW1A 2BQ

www.gov.uk/dsit

To: The Lord Alton of Liverpool, Chair of the
Joint Committee on Human Rights

2 May 2025

Response to the letter dated 28 February on the Data (Use and Access) Bill

Dear Lord Alton,

I am writing to provide a detailed response to the letter from the Joint Committee on Human Rights, dated 28 February 2025.

I want to thank you and the whole of the Committee for their time, and for raising important questions regarding the content of the Bill. I have responded in detail to each question below, and will also deposit a copy of this letter in the House library.

Data Protection

Notification exemption for further processing for research – Clause 77

Clause 77 addresses an issue specific to research where, due to the long-term nature of studies, it is not always possible to recontact individuals about a change of purpose. The clause provides an exemption to notification for researchers who directly collect personal data from the data subject, so that potentially innovative, life-changing research can continue unimpeded, while providing safeguards to avoid misuse. This includes a requirement to 'take appropriate measures to safeguard the data subject's rights, freedoms and legitimate interests'.

To ensure that the exemption is used appropriately, we have made it explicit as part of this requirement that researchers must make the information publicly available. This provides greater clarity for researchers and transparency for individuals and brings it in line with the existing equivalent exemption in Article 14(5)(b) when data is collected from a different source.

You asked about how the requirement to take appropriate measures would be interpreted, applied and enforced, and whether pseudonymisation of personal data would be sufficient. As with the existing exemption in Article 14(5)(b), controller's obligations under the requirement beyond publication will be considered on a case-

by-case basis. It is also important to note that where patient data is involved, controllers must also comply with the common law duty of confidentiality.

Subject Access Requests – Clause 78

Clause 78 codifies the principle currently established in case law that, when responding to a subject access request, a controller is only expected to undertake a reasonable and proportionate search for the information requested. This ensures continuity, despite the EU principle of proportionality no longer applying in the UK due to the effect of the REUL Act.

Under data protection legislation, the complexity of the systems adopted by the controller cannot be an excuse to reject subject access requests. Article 25 of UK GDPR requires controllers to implement data protection principles and integrate necessary safeguards into the data processing. This rule is called ‘data protection by design and by default’. According to this rule, controllers should not design data processing systems in a way that would prevent the exercise of data subject rights. Arguably, controllers capable of adopting complex data processing systems are also more likely to have access to a state-of-the-art search tools, which might make their application more likely to be “reasonable and proportionate”.

The burden of proof is on the controller to be able to justify why a search is unreasonable or disproportionate. Data subjects have the right to complain to the controller or to the ICO if they feel that their rights are not being observed. Complaints to the ICO can lead to investigations and potential financial penalties against controllers, if the ICO deem it necessary.

Following Royal Assent of the Data (Use and Access) Bill, the ICO plans to update its relevant guidance, which could include updates around reasonable and proportionate searches. The government will feed in views as necessary and appropriate to ensure controllers fully understand their requirements when responding to a subject access request.

Recognised Legitimate Interests – Clause 70/Schedule 4

Clause 70 and Schedule 4 of the Bill create a new lawful ground for non-public bodies under Article 6 of the UK GDPR where processing is necessary for a ‘recognised legitimate interest’. These interests are specified in Schedule 4 and include processing activities which serve important public interest objectives such as safeguarding vulnerable people, preventing crime, safeguarding national security, and responding to requests for disclosure from other bodies to help deliver public tasks that are sanctioned by law.

Unlike the existing ‘legitimate interests’ lawful ground under Article 6(1)(f), data controllers will not be required to undertake a detailed assessment of whether their interests in processing the personal data are outweighed by the rights and interests

of individuals. Current ICO guidance recommends that the outcome of such an assessment is documented. The aim of the measure is to give data controllers greater confidence to share personal data quickly in these circumstances without worrying about completing paperwork or displaying risk aversion in sharing data in light of the balancing test. This could be hard for them to assess when they are responding to a request made by a public body for its own purposes.

You asked how the measure would ensure that personal data was not shared with public authorities upon request in a manner that involved a disproportionate interference with the rights of the data subject.

There are two specific safeguards in paragraph 1 of new Annex 1 to the UK GDPR (as introduced by Schedule 4) that guard against this. Firstly, the organisation that requests the personal data must have a clear legal basis for processing it under Article 6(1)(e) and 6(3) (read with recital 41) of the UK GDPR and must make this clear in their request. Article 6(3) requires that the legal basis is a proportionate measure set down in law and recital 41 adds that such a basis should be clear and precise and foreseeable to the persons subject to it, in accordance with ECHR case law. A public body could not therefore request and process received data that involved a disproportionate interference with the rights of the data subjects, as this would breach the underlying legal basis and Article 8 ECHR. Secondly, any processing under the new lawful ground must be necessary and proportionate, so this will still require some case-by-case consideration on the part of the data controller who receives a request for disclosure to ensure that what is disclosed is necessary for the stated purpose. In addition to these specific safeguards, the general data protection principles under Article 5 of the UK GDPR will continue to apply to any disclosures made by a non-public body to other organisations. Amongst other things, this means that the processing would have to be lawful, fair, transparent, and secure. This will also help to ensure that use of the new lawful ground is necessary, proportionate, and fair to individuals. In addition, the data minimisation principle requires that data be adequate, relevant and limited to what is necessary in relation to the purpose for which they are being processed.

The difficulty for controllers asked to share personal data with public authorities under current law is that it is not clear whether they can rely on the Article 6(1)(e) lawful ground, which would allow them to rely on the other body's lawful ground and would have a similar effect to para.1 of new Annex 1 to the UK GDPR in Schedule 4 to the Bill. However, they will not necessarily have all the information needed to carry out the legitimate interests balancing tests under Article 6(1)(f) because the interests/purposes are those of the public body, not the controller.

Automated Decision-Making – Clause 80

Automated decision-making (ADM) is increasingly AI-driven, and the government wants the UK to make the most of the opportunities presented by AI underpinned by high data protection standards.

Organisations will be able to base significant decisions solely on automated processing in wider circumstances, but they must implement measures to provide these stringent safeguards.

The Data (Use and Access) Bill consolidates existing safeguards for ADM and articulates them in clearer language: organisations must inform individuals if they take decisions that have legal or similarly significant effects for them based solely on automated processing; an individual will always be able to challenge such decisions; obtain human intervention for them, and make representations to the controller about them. Therefore, these safeguards will allow a data subject who feels that an automated decision made about them was biased to ask for that decision to be retaken with human intervention.

Under the law enforcement regime, the same safeguards apply. In limited circumstances, an exemption to the safeguards may be exercised, for example to avoid obstructing an investigation, or to safeguard national security. However, to rely on such an exemption, the automated decision must subsequently be reviewed by a human as soon as reasonably practicable, and the review must be meaningful: this means any bias in the initial decision is more likely to be addressed than if the review simply “rubber stamps” the automated decision.

The government has committed to using secondary legislation to require the Information Commissioner’s Office (ICO) to produce a statutory code of practice on AI and solely automated decision-making. This code will support controllers in complying with their data protection obligations through practical guidance. The ICO, as the independent data protection regulator, has the discretion in the scope and content of the code.

It is also noteworthy that the regulation-making powers in the reformed Article 22, and section 50 of the Data Protection Act, future-proof our reforms in the Bill, ensuring that the government will have the powers to bring greater legal certainty more quickly, where necessary and proportionate, in light of constantly evolving technologies. These powers could be used, for example, to bring in additional safeguards to address issues relating to bias in ADM if the evidence shows that this is necessary following implementation of our reforms.

Additionally, the data protection principles, such as the requirement that the processing is accurate and lawful, and transparent (under the UK GDPR) or lawful and fair (under the law enforcement regime) and the need to ensure that appropriate technical and organisations measures are employed, will continue to apply to all ADM activities that process personal data, regardless of the technology being used.

Moreover, when a public authority carries out automated decision-making as part of the exercise of its functions, the authority must have due regard to the public sector equality duty. This includes having regard to the need to eliminate discrimination, which would ensure that the public authority pays due regard to any potential bias against individuals with one or more of the protected characteristics. Where it is likely that a high risk to the rights and freedoms of individuals are anticipated, a data protection impact assessment should be carried out.

When it comes to monitoring and enforcement of these provisions, the ICO will be responsible. The new statutory code of practice, which will be considered by a panel of relevant stakeholders and experts, will support organisations in their application of the law in such use cases and set out the expectations of the regulator.

As an independent regulator, the ICO has discretion over the allocation of resources across day-to-day operations, and over any enforcement activity and decisions which take place. However, the ICO will be expected to monitor and enforce these new provisions appropriately and proportionately, as is the case across all elements of the UK's data protection framework (including those provisions you highlighted in clause 77, and which are discussed above). The ICO remains accountable to Parliament in the delivery of its work and DSIT will continue to engage with the ICO in its role as sponsoring department.

Section 19(1)(b) Statement

Clause 45(6)

At the First Sitting of the Data Bill Committee on 4 March, the Government overturned new clause 45(6), inserted in the House of Lords, to ensure the legislation complies with Convention rights and because it has the potential to cut across rights granted under the Equality Act and the Gender Recognition Act.

It also overturned this clause for the important reason that it would seek to require public authorities to release more information than may be needed for the purposes of a digital verification check and is therefore at odds with the data minimisation principle in existing data protection legislation. A key benefit of choosing to use a digital identity is that only the specific information required about a data subject is shared for each separate digital verification check, and this clause would have prevented such privacy benefits.

As regards alternative provisions for ensuring data accuracy, the Government takes the view that this clause is not only at odds with existing data protection legislation regarding data minimisation but also duplicates the requirement under that legislation for personal data being processed to be accurate, and where necessary kept up to date. For these reasons, the Government will continue to resist any amendment that we consider duplicates existing legislation and also would require disproportionate sharing of information.

Clause 141(2)

The Government thanks the Committee for their questions on the reasonable excuse defence attached to the creating offence in clause 135, and can reassure the Committee's members that it has continued to consider the issues very carefully.

As a starting point, it is important to reiterate that the Government considers that it is necessary and appropriate to include a reasonable excuse defence for the creating offence. From a policy perspective, this ensures that there is protection in the limited circumstances where it is genuinely required (noting the breadth of the offence), for example in relation to those who have genuine reasons to test the limits and guardrails on AI image generation systems through 'red-team' testing, which necessarily involves seeing if the systems can be prompted to create images that are unlawful, in order to establish whether their existing limits and guardrails are sufficient to prevent this, or whether they need improving.

The reasonable excuse defence also ensures compliance with ECHR rights, for example, in respect of the narrow category of legitimate works of satire.

It is the Government's view that in the case of images appearing to show a person engaged in sexual activity, for example, it is extremely unlikely that the person creating the image will be able to satisfy the legal burden of proving that they had a reasonable excuse for doing so.

However, the Government considers that it is possible the proposed defence will apply in a very small minority of cases, for example those involving genuinely satirical images that are not sexually explicit, but are nevertheless captured by the offence. The fact that such circumstances exist make the defence necessary.

It is important to recall that the offence of creating a purported intimate image will capture a wide array of images, some of which may show something that is sexually explicit. However, it will also capture images that appear to show something less graphic, such as a person sitting on the toilet or standing at a urinal (without also showing their genitals or buttocks), or a person wearing boxer shorts. For some examples of less graphic images, which are not sexually explicit, the Government considers that there are more likely to be circumstances in which the balance between competing rights may lean towards Article 10, and it is for that very rare sort of scenario that we consider a reasonable excuse defence is necessary.

An example of such a scenario may involve an artwork by a professional artist, which was clearly satirical in nature, appearing to be an intimate image of a public figure, but of the less graphic nature set out above, rather than being sexually explicit.

In such rare cases, it cannot be assumed that a court would avoid finding a defendant guilty by finding that the defendant had a reasonable belief in consent. It is part of the nature of satirical artwork (and particularly satirical artwork such as this) that its subject would likely disapprove of it, were they even aware of its creation.

Therefore, if the creator claimed to believe that the subject had consented to the image, it would be very unlikely that a court would find that they in fact held such a belief, or that such a belief (if held) was reasonable.

Therefore, without a reasonable excuse defence, it could be an offence to create such an artwork, but not an offence to share it due to the reasonable excuse defence set out in section 66B(8) of the Sexual Offences Act 2003.

In this context the Government wishes to emphasise that it does not consider that this example gives licence to individuals to create any deepfake intimate images of any high-profile person - it would be a matter for the courts to determine on the facts of the case whether this was one of the exceptional cases where the image was in fact satirical and of a nature to justify a reasonable excuse defence.

Finally, the provision transfers the legal burden for the defence to the defendant, which means they would have to provide enough evidence to satisfy the court that on the balance of probabilities, they had a reasonable excuse for creating an image. Where spurious or unconvincing excuses and evidence are put forward by the defendant, the prosecution can challenge this, and the court will test this in the usual way. The courts are experienced in testing evidence and are well placed to take decisions in individual cases. However, the Government will keep the operation of the defence under review, in order to understand how it is being interpreted and applied in practice.

Article 8 rights

There is no case law specifically on creating or taking intimate images, therefore we have considered the case law on sharing such images.

Whilst the Grand Chamber has recognised every person's right to protection of his or her own image (Von Hannover v. Germany, paragraph 96; López Ribalda and Others v. Spain, paragraphs 87-89), the principles it has set out to determine whether or not an interference in this area was necessary include the contribution to a debate of public interest, and the degree of notoriety of the person affected.

Both of these would weigh in favour of an interference being justified in the satire scenario set out above, meaning that it is appropriate to have a reasonable excuse defence to both the creation of the image and the sharing of it (since the creation is a necessary prerequisite to the sharing).

Given that purported intimate images are 'untrue' images of a person, in the way that defamatory statements are untrue statements about a person, we have, for completeness, considered ECHR jurisprudence on the law of defamation though we accept that it is not directly analogous. In Axel Springer AG v. Germany, the Grand Chamber of the European Court of Human Rights held at paragraph 83 that protection of reputation, as an element of private life, only comes within the scope of Article 8 of the Convention where a "threshold of seriousness" is exceeded. In order for Article 8 to be engaged in defamation cases, an attack on a person's reputation

must attain a certain level of seriousness and in a manner causing prejudice to personal enjoyment of the right to respect for private life.

In respect of the scenario set out above, were the situation depicted to be described in a satirical article (rather than an image being published), the Government considers that it is unlikely that this would be judged to exceed the “threshold of seriousness” in order for Article 8 to be engaged, given it would so self-evidently be satirical that it could not be said to risk damage to the subject’s reputation from it being considered to be true. The Government considers that in the context of a satirical image, there is a clear distinction between this and “malicious impersonation”, from which Article 8 has been held to protect a victim (*MSD v Romania*, paragraph 118). Therefore, in the scenario set out above, even if Article 8 is engaged, the interference is arguably not so significant as to weigh heavily in the balance against the Article 10 rights of the creator.

Article 10 rights

In respect of the Article 10 rights of the creator, sexually explicit images (and therefore, by implication other less explicit types of intimate image) can and do invoke the protection of Article 10 (*Hoare v UK* and *Perrin v The United Kingdom*; *Karttunen v Finland*).

The Court has consistently held that under Article 10(2) of the Convention, there is little scope for restrictions on political expression or on contributions to the debate of questions of public interest (*Castells v. Spain*, paragraph 43; *Wingrove v. the United Kingdom*, paragraph 58). The Court has also observed on several occasions that satire is a form of artistic expression and social commentary which, by its inherent features of exaggeration and distortion of reality, naturally aims to provoke and agitate. Accordingly, any interference with the right of an artist to use this means of expression should be examined with particular care (*Welsh and Silva Canha v. Portugal*, paragraph 29; *Eon v. France*, paragraph 60; *Alves da Silva v. Portugal*, paragraph 27; *Vereinigung Bildender Künstler v. Austria*, paragraph 33; *Tuşalp v. Turkey*, paragraph 48; *Ziembinski v. Poland (no. 2)*, paragraph 45; *Handzhiyski v. Bulgaria*, paragraph 51). Those who create, perform, distribute or exhibit works of art contribute to the exchange of ideas and opinions which is essential for a democratic society. Hence the obligation on the State not to encroach unduly on their freedom of expression. The court has considered both a fictitious interview (*Nikowitz and Verlagsgruppe News GmbH v. Austria*, paragraph 18), and a caricature (*Leroy v. France*, paragraph 44; *Patrício Monteiro Telo de Abreu v. Portugal*, paragraph 40) to be forms of satirical expression. Article 10 constitutes one of the essential foundations of a democratic society. Subject to Article 10(2), it is applicable not only to “information” or “ideas” that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any section of the population.

The Government accepts that States generally have a wide margin of appreciation in relation to balancing competing Convention rights. The Government also accepts that in the hierarchy of protected expression, sexually explicit images of a person made without their consent attracts more limited protection. However, as explained above, the offence set out at clause 135(2) (formerly 141(2)) will apply to a broader range of images than only those that are sexually explicit. The Government therefore considers that the court may well consider the creation of a satirical ‘deepfake’ image to be a form of protected satirical expression, with which interference (by creation being criminalised, with no defence available) is not justified.

Balancing Article 8 and 10 rights

Where the balance lies between a defendant’s Article 10 rights and a subject’s Article 8 rights will always depend on the facts of the individual case. It is important to note however that in *In re S (A Child) (Identification: Restrictions on Publication)* [2004] UKHL 47 at paragraph 17 Lord Steyn confirmed that neither right has precedence over the other and identified the following considerations as being of particular importance in carrying out the balancing exercise:

- (1) “an intense focus on the comparative importance of the specific rights being claimed in the individual case”;
- (2) “the justifications for interfering with or restricting each right”; and
- (3) “the proportionality” of the respective interference or restriction.

When balancing Article 8 and 10 rights, the Court also considers that the extent to which any report or image have been disseminated may also be an important factor (*Karhuvaara and Iltalehti v. Finland*, paragraph 47; *Gurgenidze v. Georgia*, paragraph 55; *Klein v. Slovakia*, paragraph 48).

As set out above, the Government considers that in the majority of cases, the Article 8 rights of the person who appears to be shown in the image will carry more weight than those of the person creating the image. However, in relation to the satire scenario set out above, we consider that the case law suggests that where the image has been created, but has not been shared, as is the case with the creation of a purported intimate image offence in clause 135(2), it could be that the balance should be struck in favour of Article 10 by not criminalising the act of creation. This is more likely to be the case in relation to an intimate image that is not sexual in nature. Therefore, a reasonable excuse defence for the current measure is necessary in order to avoid the criminalisation of the creation of such an image.

As set out above, the Government’s provision transfers the legal burden for the defence to the defendant, which means they would have to provide enough evidence to satisfy the court that on the balance of probabilities, they had a reasonable excuse for creating an image. Where spurious or unconvincing excuses and evidence are put forward by the defendant, the prosecution can challenge this, and the court will test this in the usual way. The courts are experienced in testing evidence and are

well placed to take decisions in individual cases. However, the Government will keep the operation of the defence under review, in order to understand how it is being interpreted and applied in practice.

On 4 March at Commons Committee stage, the Government tabled Amendment 30 to the Bill, which sought to amend clause 141 (now 135) to insert a new subsection (7A) into the proposed section 66E of the Sexual Offences Act 2003. New subsection (7A) makes provision for a defence of reasonable excuse to the offence of creating an intimate image without consent or reasonable belief in consent. The amendment was accepted by the Committee.

The necessity and rationale for providing a defence for any individual offence, including a defence of reasonable excuse, is context specific. The Government does not consider that parallels can be drawn between the offence in clause 135(2) of this Bill and other areas.

As set out above, the offence of creating a purported intimate image will capture a broad range of images, including those that are not sexual in nature. While we consider that the circumstances in which a reasonable excuse defence will be satisfied will be rare, we also consider that legitimate reasons may exist. As a result, and as set out in our Human Rights Memorandum, it is the Government's view that a defence is needed in relation to clause 135(2) to ensure that the measure strikes the right balance in cases where a defendant has a legitimate reason for creating an image such that their right to create that image is protected by Article 10 of the Convention. It is the Government's view that relying on prosecutorial discretion in order to avoid the prosecution of the creator of such an image provides insufficient protection to the creator's Article 10 rights. Statutory offences need to be clear, and prosecutorial independence should not be routinely relied upon to apply an offence more restrictively than Parliament intended.

As the Committee knows, in each individual case prosecutors will consider whether a prosecution is in the public interest. However, such decisions can in practice be difficult to challenge (decisions to prosecute can be challenged in judicial review proceedings only exceptionally (*R (Corner House Research) v SFO* [2009] 1 AC 756 at paragraphs 30-32)). This is a novel offence where there is little case law, meaning that prosecutors will be put in a difficult position of making decisions where there may be strong external pressures and where the legal principles are difficult to clearly articulate. If the case involves consideration as to whether political satire constitutes a sufficient basis to avoid the criminalisation of the creator of an image, such a decision (involving, as it inevitably does, an assessment on a political issue) should benefit from the greatest possible distance from any suggestion of political interference.

Therefore it is the Government's view that for the creator's Article 10 rights to be properly protected, they should have the opportunity to make the argument (and have that argument adjudicated upon) in open court. It is important to note that the

defendant bears the legal burden of proving such a defence (such that the onus will be on the defendant to satisfy the court on the balance of probabilities that they had a reasonable excuse for creating the image). The defendant would have an opportunity to seek to appeal any conviction.

It is the Government's view therefore that the inclusion of a reasonable excuse defence in relation to this particular offence is therefore both necessary and appropriate.

Yours sincerely,

A handwritten signature in black ink, reading "Chris Bryant". The signature is written in a cursive, flowing style. The first name "Chris" is written with a large, looped 'C' and the last name "Bryant" follows in a similar cursive script.

Rt Hon Chris Bryant MP
Minister of State for Data Protection and Telecoms