**KONP’s response to the Government’s consultation on data use**

**Introduction**

Towards the end of last year, what is now the ‘KONP data working group’ responded to the 140 page, ‘technical’ consultation on data use produced by the DDCMS. We were pleased to receive help and advice from the Open Rights Group and medConfidential.

The consultation appeared at the same time as the Police, Crime, Sentencing and Courts Bill, the Health and Care Bill, The Cabinet Office review of the Digital Economy Act of 2017, and follows fast on the heels of the Taskforce on Innovation, Growth and Regulatory Reform May 2021. These represent a huge concerted effort by government to weaken the rights and protections governing the sharing of personal data and allow increased access by government and the commercial sector.

The changes will affect all of us but in particular the rights of workers, students and pupils, and vulnerable or marginalised groups. It will be harder to uncover and challenge discriminatory practices and more difficult to get help and support from the Information Commissioner's Office (ICO).

Our particular area of concern is the effects on sensitive health data, and our response to the consultation largely focused on questions related to this.

**Chapter 1.Reducing barriers to responsible innovation**

**We rejected i) the call to consolidate and bring together research-specific provisions to allow interested parties to navigate the relevant law more easily; ii) the creation of a statutory definition of ‘scientific research’ to ‘bring greater certainty’ for researchers; and iii) the creation of a new, separate ‘lawful ground’ to help researchers to select the best one for processing personal data.**

i) The UK GDPR already provides a clear legal framework to govern responsible use of personal data, with clear additional guidance from the ICO. Any supposed ‘barrier’ still allowed the UK to be ranked second in the world for science and research, and this without any extra risk to our rights and freedoms.

ii) Recital 159 provides clarity about the kind of research activities covered by the UK GDPR with flexibility for future social and technological change. Amendment of the legal definition of ‘scientific research’ is likely to include commercial activity and damage public trust that personal data for research will only be used in the public interest. Recent attempts to extract patients’ GP data without consent (‘care.data’ 2013 and ‘data grab’ 2021) generated fears that this could be to make data available to the private sector, and a concern is that following such actions, patients will then refuse to allow their data to be extracted for any purpose.

iii) We are concerned that the introduction of a new lawful ground would blur the fundamental distinction between publicly funded university research ‘in the public interest’, and the major legal duty of companies’ directors to ‘act in the way they consider, in good faith, would be most likely to promote the success of the company for the benefit of its members as a whole.’ The grounds for public and private research and the benefits they seek must be dealt with separately to allow the public to choose where to place their data. User-friendly guidance from the ICO can help decide on the best lawful ground for processing data and meet legal requirements without affecting our current legal protections. The development of powerful businesses with unfettered access to, and control of, data in order to achieve our government’s stated wish for ‘super-power’ status in AI technologies[[1]](#footnote-1) will put us in direct opposition to any global vision of universal health care[[2]](#footnote-2), fragment global governance approaches and erode multilateralism.[[3]](#footnote-3)

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

**We rejected the statement that ‘the accountability framework’ as set out in current legislation should feature fewer prescriptive requirements, be more flexible, and be more ‘risk-based’.**

People need certainty that any agreement for the use of their personal health data will be followed. Clear accountability rules are absolutely necessary for legal certainty, enforceability and to ensure redress is possible when required by any individuals. Fewer prescriptive requirements will diminish the rights of individuals.

The government presentation within the proposal misread the UK GDPR. Generally, responsibilities under the UK GDPR **are influenced by the level of risk involved**, with increased risk requiring stronger data policies and stronger data security. Also, the UK GDPR accountability framework is flexible providing proportionate accountability depending on the ‘nature, scope, context and purposes’ of data use. This includes differences in the use of records, security measures and contractual safeguards in ‘data use’ agreements.There are also a number of tasks that organisations only have to carry out if a certain risk threshold is met.

**Chapter 4: Delivering better public services**

**We rejected i) the statement that Public service delivery powers under section 35 of the Digital Economy Act 2017 should be extended to help improve outcomes for businesses as well as for individuals and households; ii) the statement that private companies, organisations and individuals who have been asked to process personal data on behalf of a public body should be permitted to rely on that body’s lawful ground for processing the data under Article 6 (1) (e) of the UK GDPR; iii) the proposal to clarify that public and private bodies may lawfully process health data when necessary for reasons of substantial public interest in relation to public health or other emergencies; iv) the idea that compulsory transparency reporting on the use of algorithms in decision-making for public authorities, government departments and government contractors using public data will improve public trust in government use of data; and v) the statement that it may be difficult to distinguish processing that is in the substantial public interest from processing in the public interest.**

i)While work is already underway by the Cabinet Office to address barriers to data sharing and explore how to extend the public service delivery powers under Section 35 of the Digital Economy Act 2017 to the business sector, neither the barriers, nor the type of powers involved are explained. Section 35 already allows for information sharing between public authorities and ‘specified persons’ providing services for specified public service delivery objectives, while additional objectives can be set by regulations. Such sharing of information must be shown to be necessary to achieve the desired objective in order to be allowed. So the legal basis for sharing government-held data with the private sector already exists and can be extended when this is *in the service of a public authority*. It seems that government wishes to allow data to be shared with the business sector when this is *not* in the service of a public authority.

ii)We support the status quo that health data is classed as ‘sensitive personal data’ and should be subject to heightened safeguards by all users. *It should only be processed where the individual has given explicit consent*and used when it is necessary for a) health, social care or public health purposes overseen by healthcare professionals; b) other specified purposes, such as scientific research; c) or it is necessary for other reasons of substantial public interest, as defined in Schedule 1 to the Data Protection Act 2018. Pragmatic and helpful guidance issued by the ICO should be used to remove any uncertainties. These existing lawful grounds for processing sensitive personal data are already clear, and do not appear to have hampered access to health data for a range of companies during the pandemic.

iii) What the proposal seeks to do is further facilitate the private sector’s access to individuals’ sensitive personal data, without saying ‘how substantial public interest’ is to be defined, and what safeguards should be in place to protect the sensitivity of the data. The consultation document claims that the experience of fighting Covid has demonstrated the power and benefit of collaboration between the public and private sectors. However, we suggest that there has not always been transparency about the motivation behind this ‘collaboration’. We completely reject any notion that the private sector: provided ‘value for money’, used personal data responsibly in the public interest, and that collaboration with them created increased benefit. Our argument included evidence from ‘openDemocracy’[[4]](#footnote-4) concerning the contracts to Palantir, the Public Accounts Committee concerning NHST&T[[5]](#footnote-5),[[6]](#footnote-6) highlighting the legal action over the contract awarded to Immensa[[7]](#footnote-7) and The Centre for Health and the Public Interest (CHPI)[[8]](#footnote-8) about the absurdity of private hospital sector commissioning.

iv)Algorithms are not neutral tools; created by humans, they are inevitably value laden and designed with particular outcomes in mindthat will privilege some outcomes over others. In the health service, the growing dependence on algorithms runs the risk of undermining clinicians’ use of clinical judgement while relying on under-skilled staff who may not recognise when an algorithm’s decision is unsafe. Where algorithms are used there needs to be transparency so they can be scrutinised for bias and other shortcomings. However, if the personal health data used to develop algorithms is extracted without individuals’ consents or appropriate safeguards, it is hard to see how transparency – for example about an algorithm’s technical specifications or which data sets it has used - will in itself improve the public trust in government use of data.

v)The ICO already clarifies the difference between ‘public interest’ and ‘substantial public interest’ and provides guidance on determining whether processing is in the ‘substantial public interest’. The conditions for processing data in the ‘substantial public interest’ are set out in Schedule 1 of the Data Protection Act 2018. Data controllers have to demonstrate that they meet the relevant condition.

**Chapter 5 - Reform of the Information Commissioner's Office**

**We rejected: i) the idea that the ICO would benefit from a new statutory framework for its objectives and duties; ii) the proposal to introduce a new duty for the ICO to have regard to economic growth and innovation, and competition when discharging its functions; iii) the proposal to introduce specific language recognising the need for the ICO to have due regard to public safety when discharging its functions; iv) the proposal for the SoS for DCMS to periodically prepare a statement of strategic priorities which the ICO must have regard to when discharging its functions, along with the requirement for the ICO to deliver a more transparent and structured international strategy, and a new statutory objective for the ICO to have to consider the government's wider international priorities when conducting its international activities; v) that the ICO would benefit from a new governance and leadership model including the use of the Public Appointment process for the new chair, the non-executive members and the new CEO of the new ICO board, and that the salary for the Information Commissioner (i.e. the proposed chair of the ICO) should not require Parliamentary approval; vi) that the ICO would benefit from a more proportionate regulatory approach to data protection complaints by the introduction of a requirement for the complainant to attempt to resolve their complaint directly with the relevant data controller prior to lodging any complaint with the ICO, and the setting out in legislation the criteria that the ICO can use to determine whether or not to pursue a complaint, so apparently providing clarity and enabling the ICO to take a more ‘risk-based’ and proportionate approach to complaints.**

i)As our data becomes increasingly important for competition, innovation and economic growth, this government wishes to force the ICO to take greater account of impacts in these domains and to introduce a power for the SoS for DCMS to prepare a statement of strategic priorities to inform the ICO how to set its own regulatory priorities. This weakens the ICO’s independence as it supervises and enforces the UK's data protection regime.

ii)The ICO will be expected to a) provide evidence of how the development of regulatory policy takes account of the need for economic growth and innovation, especially in emerging technologies, and undertake in-depth market condition analyses via business surveys; and b) ensure regulatory objectives do not unnecessarily inhibit any pursuit of better competition outcomes that may require for instance increased access to personal data.

iii)The government wishes to provide the ICO with ‘more clarity’ with regard to its statutory functions when dealing with bodies serving to protect the public; to have more due regard to public safety when balancing this against protection of our data.This indicates more pressures on the ICO’s independence.

iv)From a business perspective the importance of data to our economy and the broad, cross-sectoral scope of the ICO’s remit makes the ICO probably the UK’s most significant regulator. Its decisions on how personal data can be used may affect innovation (business enterprise) and the performance of many parts of the UK's economy. The application of pressure on the ICO by this government on behalf of business to gain improved access to our data is therefore not surprising.

v)Government believes that the ICO needs the right governance structures in place to provide greater diversity, challenge and scrutiny in order to deliver its ongoing ‘transformation’ programme: to build the capability and processes necessary to regulate effectively in an increasingly data-driven world.The Public Appointment process and the loss of Parliamentary overview of the Chair’s salary would, alongside the requirement to publish key strategies and processes that guide its work, the duty to use expert panels from the ‘primarily affected groups’ (businesses) to help make recommendations, and the empowerment of the DCMS SoS to be able to initiate a review of the ICO’s activities and performance and to be able to veto any code of practice or guidance, bring the ICO much more under control of government.

vi)The government believes that the ICO currently uses up too much of its resources on dealing with complaints and that there are far too many vexatious complaints. Their plan will simply set up barriers in the way of redress for any misuse of our data.

1. <https://www.cnbc.com/2021/09/22/uk-publishes-plan-to-become-ai-superpower-and-rival-us-and-china.html> [↑](#footnote-ref-1)
2. <https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(21)01824-9/fulltext> [↑](#footnote-ref-2)
3. <https://www.fhi.ox.ac.uk/wp-content/uploads/GovAI-Agenda.pdf#page46> [↑](#footnote-ref-3)
4. Fitzgerald M Crider C. Controversial ‘spy tech’ firm Palantir lands £23m NHS data deal Exclusive: UK government sneaks through new COVID data contract, despite legal challenges. Open Democracy 21 December 2020 [↑](#footnote-ref-4)
5. <https://www.tussell.com/insights/covid?hsLang=en> [↑](#footnote-ref-5)
6. <https://www.theguardian.com/politics/2021/nov/01/law-group-threatens-to-sue-over-immensa-covid-testing-scandal> [↑](#footnote-ref-6)
7. <https://www.theguardian.com/politics/2021/nov/01/law-group-threatens-to-sue-over-immensa-covid-testing-scandal> [↑](#footnote-ref-7)
8. Leys C. Private hospitals have no doctors. Centre for Health and the Public Interest June 1, 2021 [↑](#footnote-ref-8)