19th November 2021

Access Now's comments to the United Kingdom's Department for Digital, Culture, Media and Sport consultation - "Data: A new direction"

Introduction

Thank you for the opportunity to provide comments to the United Kingdom's government's proposed reform in the area of data protection.

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world. We work on data protection and privacy around the world and we maintain a presence in 13 locations around the world.[1]

We wholeheartedly agree with the vision outlined in the ministerial foreword of the consultation: "The protection of people's personal data must be at the heart of our new regime". Regrettably, this objective is not reflected in the proposal advanced in this consultation.
On the contrary, a number of measures proposed in this consultation would eliminate important data protection rights currently in place in the United Kingdom (UK). The UK government played a huge part in advancing these rights for citizens across Europe during the negotiations of the EU General Data Protection Regulation (GDPR). Yet, specific measures proposed in this consultation would end or limit existing rights and freedoms that are crucial, in particular for a sustainable development of Artificial Intelligence (AI) technologies in the UK.
Other proposals risk undermining the independence and powers of the Information Commissioner's Office (ICO), and, with it, would put in jeopardy the adequacy decision granted by the EU. Having an independent supervisory authority is critical to ensure adequate oversight and enforcement of data protection measures in the UK. It is also an important criteria analysed by the European Union when deciding to grant an adequacy decision. Maintaining the EU-UK adequacy decision is fundamental for the protection of citizens' rights on both sides of the channel and for the UK economy. In 2018, the value of UK potentially-ICT enabled services exports going to the EU represented £84.9 billion.[2] As noted by the Department for Digital, Culture, Media and Sport

[1] Access Now, https://www.accessnow.org/
[2] Data from: Department for Digital, Culture, Media and Sport, International data transfers: building trust, delivering growth and firing up innovation, August 2021. https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation, Department for International Trade,

(DCMS), “International data transfers underpin modern day business transactions and financial institutions”. The EU-UK adequacy decision is a fundamental tool for economic growth and to avoid billions in losses across many sectors in the UK. Guaranteeing the independence and adequate functioning of the ICO is therefore of paramount importance for the UK.
Beyond the risk of losing the EU adequacy decision, the collective set of measures proposed under this consultation would effectively put every UK company offering services in the EU under a dual compliance regime, adding red tape and costs for business owners in the UK.

Our response to the consultation will focus on these three issues, which simultaneously affect the protection of privacy and data rights and the economy in the UK,:

- Rights of citizens, in particular in the deployment of AI systems
- Role, powers, and independence of the Information Commissioner’s Office
- Cost of the measures for the UK economy and companies established in the UK

1. Rights of citizens, in particular in the deployment of AI systems

A number of measures proposed in the consultation would eliminate important data protection rights currently in place in the UK, in particular some that are critical for a sustainable development of AI systems. Below, we provide comments to some of these proposed measures that we have identified as particularly problematic and, if carried out, would run contradictory to the government’s objective to ensure a high level of data protection.

In paragraphs 60 to 62, the government proposes to create a list of legitimate interests for which organisations can use personal data without applying the balancing test currently required by the GDPR. The government proposed list mixed issues that have already been identified under the GDPR as legitimate interests including “Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority”.[3] Others that are commercial activities currently under regulatory scrutiny across Europe due to their possible intrusive impacts on data subject's rights, including “Using audience measurement cookies or similar technologies to improve web pages that are frequently visited by service users”. We therefore disagree with the suggested list of activities where the legitimate interests balancing test would not be required. Even in the cases where issues have been identified as legitimate interest under the GDPR, a balancing test is necessary to ensure that the rights of data subjects are guaranteed and for data controllers to be able to assess if the processing is compatible with a legal, professional or other binding obligation of secrecy.

Understanding and measuring cross-border digital trade, May 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885174/Understanding-and-measuring-cross-border-digital-trade.pdf, and POLITICO Europe, Digital Bridge, September 2021. https://pro.politico.eu/news/140567

[3] See: Recital 50, EU General Data Protection Regulation, Regulation (EU) 2016/679 https://eur-lex.europa.eu/eli/reg/2016/679/oj

In paragraph 101, the government presents the proposal from the "Taskforce on Innovation, Growth and Regulatory Reform that Article 22 of UK GDPR should be removed. The report recommends that UK law should instead permit the use of solely automated AI systems on the basis of legitimate interests or public interests. Such a change would remove the right not to be subject to a decision resulting from 'solely automated' processing if that decision has legal or 'similarly significant' effects on data subjects." We strongly disagree with this proposal. Article 22 is perhaps one of the most forward looking rights included in the GDPR to ensure that the development of AI systems goes hand in hand with robust data protection measures. It enables data subjects to keep control on the use of their information and is paramount for trust in these systems to exist.

In paragraphs 114 to 125, the government worryingly discusses scenarios where data could "be regarded as anonymous" and therefore escape the scope of many data protection obligations. The section mixes several important yet different concepts from data minimisation, to pseudonymisation, and anonymisation. While these techniques are important, we must recall that several studies have concluded that it is nearly impossible for data to be fully anonymous and not be re-identified.[4] In suggesting that the threshold for considering when data is anonymous could be lowered, the government may expose data controllers to liability issues if data was to be re-identified, breached, or abused.

In paragraphs 188 and 189, the government proposes measures to "help to ensure that organisations are not overburdened by wide-ranging, speculative subject access requests", including by introducing a fee and a limitation on the size of data access requests that can be made. Data access rights are crucial for data subjects to be able to control their information, know what and how their data is being used by controllers, and to be able to exercise other data rights such as the right to rectification or to object. Data access is critical to reduce or restore a balance of powers between data controllers and data subjects.
The concerns identified by the government in the consultation have been taken into account and covered under the GDPR which foresee mechanisms for data controllers to act "Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character".[5] The proposal by the government to introduce a fee and restrictions to *any* data access requests is unnecessary, disproportionate, and would tilt the balance of powers towards the data controller to the detriment of the data subject.

2. Role, powers, and independence of the Information Commissioner's Office

We are particularly concerned with the proposals that would risk undermining the independence and powers of the ICO, and, with it, would put in jeopardy the adequacy decision granted by the

[4] The Guardian, 'Anonymised' data can never be totally anonymous, says study, July 2019. https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds
[5] See Article 12, EU General Data Protection Regulation, Regulation (EU) 2016/679 https://eur-lex.europa.eu/eli/reg/2016/679/oj

EU. We support and echo the following message from the ICO in their own response to this consultation:

> *"To ensure high standards are met, and that people have the trust and confidence to contribute positively to the digital economy, the UK needs a strong, effective regulator."*
>
> *"(...) there are some important specific proposals where I have strong concerns because of their risk to regulatory independence. For the future ICO to be able to hold government to account, it is vital its governance model preserves its independence and is workable, within the context of the framework set by Parliament and with effective accountability. The current proposals for the Secretary of State to approve ICO guidance and to appoint the CEO do not sufficiently safeguard this independence.I urge the Government to reconsider these proposals to ensure the independence of the regulator is preserved."*[6]

In paragraph 345, the government "proposes to introduce a new power for the Secretary of State for DCMS to periodically prepare a statement of strategic priorities to which the ICO must have regard when discharging its functions." This would give powers to DCMS to influence the ICO's work and priorities. We strongly disagree with this proposal.
Similarly, we strongly disagree with the proposal laid down in paragraphs 329 to 336 where the government suggests introducing new duties to the ICO as part of its regulatory approach. The ICO would have to report on "how intends to comply" with these new duties "and report against how due regard to the duty was given when discharging its functions".
Additionally, in paragraphs 349 and 350, the government proposes to include "as part of the new framework of objectives and duties, a new statutory objective for the ICO to consider the government's wider international priorities when prioritising and conducting its own international activities." We strongly disagree with this proposal.
To conduct its duties, the ICO must remain an independent authority and must not be subject to direction by the government. We urge the government to not move forward with these proposals as they would undermine the independence of the ICO in relation to the government.

If carried, these proposals are extremely concerning for the future application of the UK data protection regime and for the UK digital economy. The success and robustness of any data protection regime requires the existence of an independent supervisory authority with sufficient powers and resources to conduct audits, oversee compliance, and enforce legislation. In proposing to put the ICO under greater control and direction from the UK government, the UK would critically undermine the independence of the ICO and with it, risk losing its adequacy decision with the EU. In determining whether a country fulfills the criteria for adequacy, the EU pays close attention to the independence and powers of the supervisory authority as well as to the remedies available for data subjects rights to be protected. In fact, the European Commission has

---

[6] Information Commissioner's Office, ICO response to DCMS consultation "Data: a new direction", October 2021.
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/10/response-to-dcms-consultation-foreword/

already warned that the UK proposals "raises questions", in particular the issues surrounding the independence of the ICO, and that it "may raise issues" in relation to the EU-UK adequacy.[7]

3. Cost of the measures for the UK economy and companies established in the UK

In addition to the risk of losing the EU adequacy decision, the collective set of measures proposed by the government under this consultation would put every UK company offering services in the EU under a dual compliance regime, adding red tape and costs for business owners in the UK.

A number of proposals advanced under the consultation would create conflicting or diverging requirements for data controllers and processors operating both in the EU and the UK. The following proposals are particularly problematic for that matter:

- paragraph 54 on further processing of data,
- paragraphs 160 to 164 on requirements on organisations to appoint a data protection officer,
- paragraphs 165 to 169 on requirement for organisations to undertake a data protection impact assessment,
- paragraphs 170 to 173 on requirement for prior consultation with the ICO,
- paragraphs 174 to 177 on record keeping requirements,
- Paragraphs 178 to 184 on data breach reporting and accountability processes.

Report suggests that "UK reforms designed to ease some of the burden of appointing data protection officers could end up being difficult for small businesses."[8] Companies and law firms advising businesses for compliance are raising concerns as to how these requirements would apply and "that this divergence from GDPR could end up creating more issues for companies than it solves." This uncertainty not only increases difficulties for companies' daily activities but also raises questions as to how important requirements for the protection of data subjects' information will be operationalised.

At a time where global convergence for the protection of personal data is growing, we urge the UK government to maintain clear standards that provide legal certainty and mutually benefit the protection of data subjects' rights and companies operating on both sides of the Channel.

Conclusion

[7] POLITICO Europe, Top EU official fires warning shot over UK data reform, November 2021. https://pro.politico.eu/news/142821

[8] Global Data Review, UK GDPR overhaul could cause DPO headache, November 2021. https://globaldatareview.com/policy/uk-gdpr-overhaul-could-cause-dpo-headache?utm_source=UK%2BGDPR%2Boverhaul%2Bcould%2Bcause%2BDPO%2Bheadache&utm_medium=email&utm_campaign=GDR%2BAlerts

We urge the government to reconsider measures proposed in the consultation that would end or limit the application existing data and privacy rights. We further urge the government to not undermine the independence and powers of the ICO and, with it, put in jeopardy the adequacy decision with the EU. We call on the government to maintain convergence with the EU data protection regime to avoid creating a double data protection compliance system that could isolate UK companies, limit their revenue, and undermine their contribution to the global digital economy.

We look forward to engaging with the government and the Department for Digital, Culture, Media and Sport to ensure that the protection of people's personal data must be at the heart of the UK regime.

Estelle Massé
Global Data Protection Lead
Access Now
estelle@accessnow.org