Data: A New Direction - the3million consultation response

We strive to represent the interests of the millions of EU citizens and their family members[1] living in the UK impacted by the UK's decision to leave the European Union. A fundamental part of this work is championing the various rights of these people and, where we can, ensure they are upheld and respected. Since our formation, we have and continue to be particularly concerned with rights associated with personal data and its protection. It has never been more important, than now in the digital age, especially in the context of migrants coming to and living in the UK.

We work closely with the Open Rights Group and will defer to them and their detailed submissions on the strategy proposed by the Government as far as the substance is concerned. We will cite here our general concerns from an EU citizen's perspective when it comes to immigration control.

The implications of the changes proposed will have a negative impact for now and the future. There are several and serious changes coming with the Government's planned changes for border control in the UK that will place a significant reliance on personal information and data relating to migrants in the UK.[2] The use of automation and introduction of other technologies to decision making on everything from visa applications to border control are reasons for better controls on information and not less.

We note there are potential changes to modify UK GDPR for research purposes. Innovation and research is improved and protected by high data standards not hindered (a view we understand is shared by the Information Commissioner's Office). The proposed measures would be counterproductive to research but would also be dangerous. The vagueness of the terminology and scope of these changes puts people at risk.

We also understand that the plans would enable the reuse of data and allow data to be sold where there is 'substantial public interest'. This is particularly concerning given the digital developments expected with border control. There is a legacy of abusive data use where the Home Office shared confidential asylum seekers information with their country of origin[3], made unlawful copies of the Schengen Information System database[4], and where The Home Office was repurposing NHS medical data[5].

[1] When we refer to EU Citizens and their family members we mean all those EEA/Swiss Nationals and other nationals living in the UK relying on rights under the EU framework of freedom of movement, who now have rights under the terms agreed between the UK and various parties (the EU Withdrawal Agreement, EEA EFTA Separation Agreement and Swiss Citizens' Rights Agreement).

[2] https://www.gov.uk/government/publications/new-plan-for-immigration-legal-migration-and-border-control

[3] https://www.theguardian.com/politics/2018/jan/17/home-office-pays-out-15500-to-asylum-seeker-over-data-breach

[4] http://europeanmemoranda.cabinetoffice.gov.uk/files/2020/03/ST_6554_2020_INIT_EN.pdf

[5] https://www.theguardian.com/society/2018/nov/12/home-office-scraps-scheme-that-used-nhs-data-to-track-migrants

We understand the Government proposes to create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying 'the balancing test'.

The balancing test is the thin veil that divides responsible use from abuse. We note the legitimate interests of "reporting criminal acts or other safeguarding concerns" as well as "ensuring that records of individuals are accurate and up to date" could allow unprecedented freedom to collect personal data about migrants for reasons connected with immigration control.

A fundamental principle of the GDPR framework is an individual's empowerment over their information and its use. Knowledge of how your information is used and in particular within decision making is fundamental to natural justice and other basic civil rights. The DCMS proposal, instead, undermines our rights to know, choose and complain about how our data is used. The Government's proposal to scrap Article 22 of the UK GDPR is a clear example of this.

Scrapping Article 22 of the UK GDPR would shift the burden to actively scrutinise automated life-changing decisions from organisations to individuals, who have no control or access over these systems. Automated decisions tend to adversely impact those that are already discriminated against, by amplifying discrimination already present in society. This is particularly important in the context of migrants' rights and the Home Office's future intention to increase automated decision making.

We understand there are plans to impose fees on a subject access request ('SAR'). SARs are a fundamental means of establishing decision making and information sharing within government and fees would act as a deterrent from their use. We are aware of hundreds of cases where a SAR has been the essential difference in many a person's case against the Home Office where mistakes have been made in their decision making.

A key component of compliance is the requirement of Data Protection Impact Assessments ('DPIA'). We understand the Government is looking to reverse their use and introduce privacy management programmes which would give organisations the freedom to decide how to demonstrate compliance with data laws. This would deny individuals useful grounds to expose and challenge harmful or discriminatory practices. A DPIA is a key component of standardised accountability that can be used by organisations to understand where issues may arise with data policies.

The Home Office's failure to undertake a DPIA with a recent algorithm was key to holding it to account especially when it became apparent that the algorithm was racist[6]. To reverse the requirement for a DPIA would remove a vital point of regulating data use by departments such as the Home Office.

Without measures such as the DPIA, organisations would be able to claim that they implemented a "privacy management programme which includes the appropriate policies and processes for the

[6] https://www.foxglove.org.uk/2020/08/04/home-office-says-it-will-abandon-its-racist-visa-algorithm-after-we-sued-them/

protection of personal information", or that they relied on unsubstantiated "risk assessment tools for the identification, assessment and mitigation of privacy risks across the organisation". Rather than asking organisations to demonstrate they conducted "due diligence", the burden to prove that these token measures are not adequate would fall on the individuals being discriminated against.

Key to rights being implemented is accountability. The ICO is central to the accountability framework of GDPR and we understand the proposals would allow the Government to dictate the ICO's priorities and the salary of the commissioner without parliamentary approval. This would weaken the ICO's effectiveness and reduce its power to hold the Government to account.

In general we have concerns over how the measures envisioned by the Government are compliant with GDPR. We will be keen to speak with our colleagues and institutions in the European Union to establish their views on whether these proposals are compliant with GDPR. We urge the Government to have a dialogue with its European partners to ensure that data transfers are not compromised in the future by these policy changes.