

Written evidence from Amnesty International UK

Amnesty International UK is a national section of a global movement. Collectively, our vision is of a world in which every person enjoys all of the human rights enshrined in the Universal Declaration of Human Rights and other international human rights instruments. Our mission is to undertake research and action focused on preventing and ending grave abuses of these rights. We are independent of any government, political ideology, economic interest or religion.

Introduction:

1. By this submission, Amnesty International UK (AIUK) wishes to draw to the Committee's attention provisions in the Data Protection Bill – specifically, paragraph 4 of Schedule 2 – which have relevance to this inquiry.

General observations:

2. We have read and considered the written evidence submitted jointly by the National AIDS Trust (NAT) and Doctors of the World (DOTW), which succinctly sets out concerns regarding the deterrent effect of passing personal information given to healthcare providers for healthcare purposes to the Home Office for immigration purposes. As they highlight, that deterrence is likely to have significant detrimental impact upon individual and public health. They rightly highlight that deterrence is not only experienced by people in the UK in breach of immigration rules (still less only people entitled to be here, which includes people whose entitlement remains to be formally recognised).
3. The deterrence effect of passing personal information to the Home Office is particularly likely to affect directly anyone who fears intervention of immigration authorities. Given the many reported incidents of people being wrongly told they are not permitted to be in the UK, detained and otherwise threatened with or subjected to Home Office measures to remove them from the UK, it would be surprising if such fears were not held more widely.¹ It seems reasonably likely those most likely to be deterred are those who are most vulnerable and marginalised, particularly if their experience, or that of their family or someone else they know, includes being badly or wrongly treated in any matter related to immigration status or immigration functions.
4. We note that the harms caused by this deterrence extend beyond the individual and public health concerns highlighted by NAT and DOTW. For example, as has been specifically recognised by the government, healthcare staff are often particularly well-

¹ The Home Affairs Committee has drawn attention to this in its *Immigration policy: basis for building consensus*, Second Report of Session 2017-19, January 2018, HC 500, paragraphs 52-57: <https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/500/50002.htm>

placed to identify and support people caught in situations of exploitation and abuse, such as slavery and domestic violence.² While not all such persons are subject to immigration control, many are; and it is well-known that abusers use the threat of deportation and other immigration-related consequences as a means to control their victims.³ Accordingly, in addition to the concerns raised by NAT and DOTW, the practice of passing personal information to the Home Office significantly undermines government policy on modern slavery and domestic violence by deterring one means whereby the victims of these abuses may be identified or seek support.

Data Protection Bill:

5. The Data Protection Bill risks exacerbating these concerns significantly if the immigration exemption from basic safeguards set out in paragraph 4 of Schedule 2 to the Bill is retained.⁴ The Bill is to bring into UK domestic law the EU General Data Protection Regulation 2016/679 (GDPR), the key purpose of which is to strengthen and standardise across the EU the protection of personal information. However, paragraph 4 of Schedule 2 to the Bill would largely remove that protection by permitting exemption of the following basic matters in respect of data processing (taking, storing, sharing and using data) for the purpose of ‘effective immigration control’:
 - That processing of someone’s personal information must be lawful, fair and transparent.
 - That this data is processed accurately and kept up to date.
 - That this data is held securely.
 - That the person to whom the data relates is informed of the data being held, for how long it may be held and for what purpose it may be used.
 - That the person to whom the data relates may inspect the data and request its erasure or correction.

6. The exemption from these safeguards would apply to the Home Office, other government departments and bodies, and private individuals and bodies. Significant to the Committee’s inquiry, this would include healthcare providers, NHS Digital and the Home Office, permitting exemption for immigration purposes of basic legal safeguards at the core of what will be the UK’s primary legislative source of protection of personal information. The memorandum of understanding and practice

² The government has, for example, published guidance specifically for healthcare staff in relation to victims of modern slavery: <https://www.gov.uk/government/publications/identifying-and-supporting-victims-of-human-trafficking-guidance-for-health-staff>

³ For example, this is expressly acknowledged in the UN Global Report on Trafficking in Persons 2016, pp59-61 (*What factors can influence the vulnerability of certain migration flows to trafficking in persons*):

https://www.unodc.org/documents/data-and-analysis/glotip/2016_Global_Report_on_Trafficking_in_Persons.pdf

It has also been acknowledged in parliamentary committees, including the Home Affairs Committee, *The Trade in Human Beings: Human Trafficking in the UK*, Sixth Report of 2008-09, May 2009, HC 23 (paragraph 60); and the Joint Committee on Human Rights, *Human Trafficking*, Twenty-Sixth Report of 2005-06, October 2006, HL Paper 245, HC 1127 (paragraph 140).

⁴ Further detail regarding the provisions of the Bill, their operation and effect is available from the submission of AIUK to the Joint Committee on Human Rights legislative scrutiny inquiry on the Data Protection Bill, see: <https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/500/50002.htm>

under it, or any future or related arrangement and practice, could thereby be relieved of these basic legal constraints – allowing those formulating and implementing policy and practice to ignore these safeguards and depriving those subjected to (and those regulating, including courts) such policy and practice of the opportunity to rely upon and apply these safeguards.

7. As the Home Affairs Committee have recently concluded on the wider immigration policy – originally styled by the Prime Minister as a ‘hostile environment’ – of which this data sharing forms part:⁵

“While the hostile environment is currently aimed at non-EU nationals without valid leave to be in the UK, there are regular reports of people with a lawful right to be here (including UK and EU nationals and non-EU nationals with valid leave) being caught up in the system, often via errors in an application process and problems with data retained by the Home Office.”

8. This is before the passing and commencement of the Bill. By expressly allowing exemption from basic safeguards, the Bill could be expected to seriously exacerbate these concerns by permitting, arguably encouraging, an even more lax attitude to individuals’ rights in the sharing and use of their personal data. In turn, that can be expected to exacerbate the concerns NAT and DOTW express, and which we share, regarding the deterrence effect summarised above.
9. Moreover, witnesses before the Committee have emphasised how the memorandum of understanding significantly undermines ethical standards expressed in GMC guidance and the NHS code permitting disclosure of personal information in relation to serious harm and/or offending.⁶ The immigration exemption in the Bill risks compounding these concerns – particularly having regard to evidence of the chief executive of NHS Digital before the Committee⁷ - because the Bill would undermine the broader legal framework currently operating in the UK by generally extending exemptions to that framework (which is distinct from the specific ethical healthcare considerations raised by witnesses) from crime prevention and prosecution purposes to immigration control purposes.⁸
10. Our purpose in drawing this matter to the attention of the Committee is not to detract from or lessen the prior concerns set out by NAT and DOTW in their joint submission. While the immigration exemption in the Data Protection Bill risks making a situation significantly worse and that exemption ought not to be retained in

⁵ See Home Affairs Committee, *Immigration policy: basis for building consensus*, *op cit*.

⁶ This was particularly raised in the first of the two sessions on 18 January 2018:

<http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/health-committee/memorandum-of-understanding-on-datasharing-between-nhs-digital-and-the-home-office/oral/77354.html>

⁷ See second of the two sessions on 18 January 2018 *op cit*, particularly Qs 57, 58 & 62, where the chief executive effectively emphasised the underlying legislative framework as the basis for NHS Digital data-sharing rather than the more specific and higher ethical considerations and positions to which previous witnesses referred.

⁸ Section 29, Data Protection Act 1998 currently includes a crime prevention and prosecution exemption. Such an exemption is also included in the Data Protection Bill (paragraph 2 of Schedule 4), reflecting the inclusion of a crime prevention and prosecution exemption (unlike the immigration exemption) in the General Data Protection Regulation 2016/679 at article 2(d).

the Bill, removing it from the Bill would not remedy substantial harm done to individual and public health, and other policy aims such as relating to modern slavery and domestic violence, resulting from the deterrent effect of current data sharing.