



THE JOINT COUNCIL  
*for* THE WELFARE  
OF IMMIGRANTS



# HOW THE DATA PROTECTION AND DIGITAL INFORMATION (NO. 2) BILL HARMS MIGRANTS' DATA RIGHTS

Published by Open Rights Group - Open Rights is a non-profit company limited by Guarantee, registered in England and Wales no. 05581537. The Society of Authors, 24 Bedford Row, London, WC1R 4EH. (CC BY-SA 3.0)

Author Sara Alsherif

For Further information please contact Sara Alsherif on +447902 823 294  
sara@openrightsgroup.org

22 June 2023

The new Data Protection and Digital Information Bill (DPDI Bill) is going through parliament and is expected to be passed into law later this year. The changes in this Bill will exacerbate the existing power imbalances of migrants, refugees, and asylum seekers over their data leading to significant harm and negative consequences.

## DATA USES AND REUSES

The proposed changes will give the Home Office the power to repurpose

the use of personal data to ensure national security and public safety, which means that the data that refugees and asylum seekers handed over for a given reason could be used beyond what they consented to or expected, such as for immigration enforcement purposes or sharing data with their home country's authorities without the need for explicit consent or a thorough assessment of the risks involved.

For refugees and asylum seekers, collecting and processing personal data is crucial to processing their applications and ensuring a successful claim. Still, these changes would put them at risk of persecution or harm if their personal information is shared with their country, undermining their trust in the authorities and discouraging them from seeking help or accessing needed services, such as healthcare, legal aid, or social support programs. The exemption from the compatibility test also negatively impacts unintended consequences or discriminatory practices. For example, if any organisation or entities use their data to profile them based on their race, ethnicity, or religion, which could lead to unfair treatment or discrimination, leaving them as easy prey.

Likewise, the Bill would eliminate the need to carry out a "balancing test" to weigh the interests and impact of data processing on the individuals, which could lead to the disproportionate disclosure and transfer of migrants' data by private entities for various purposes, such as immigration enforcement or border security.

Clause 5, will make it legal for private entities to use personal data under 'legitimate interests'. While clause six will allow for public entities to share and reuse personal data that was collected for a different use.

That will put migrants, refugees, and asylum seekers' safety at risk. Government agencies or other organisations could use this to require employers, landlords, general practitioners, and any other private entity to hand over migrants' data for various purposes, such as immigration enforcement or border security. For example, employers and Identity

Service Providers could share the migrant workers' data with the Home Office without their knowledge or consent.

## DATA RIGHTS

If this weren't already bad enough, the Bill would make it easier for organisations to refuse to act upon a data rights request, which provides individuals with the right to request, access, and correct the personal information that the organisation (such as a government agency, company, or employer) are processing or hold about them.

This change will give companies, employers and organisations the power over peoples' data. These practices will cause a chilling effect on the migrants, Refugees and asylum seekers as vulnerable groups regarding exercising their right to request in such a hostile environment. Further, these changes seem to be a deliberate attempt to circumvent the recent Immigration Exemption judgment, where a Court found that the UK Data Protection Act arbitrarily and unreasonably restricts the right of access for immigration control purposes: in other words, the Government seem to be keen to legalise what has just been ruled illegal by a Court of Law

In addition, the Bill would remove the requirement to appoint a UK representative in overseas organisations. This means that if you are a migrant and want to exercise your data protection rights and complaint about how your data is being processed, you will not find any contact information for the foreign company, as they will not have a representative in the UK. Potentially will put migrants, refugees, and asylum seekers' digital rights at risk, as they would have less recourse if their data were mishandled or misused by a foreign company.

## RIGHT TO A HUMAN REVIEW, RIGHT TO ONLINE PRIVACY

The proposal will enable the government to exempt automated decisions using AI and algorithms from legal safeguards, providing individuals with

a right to know the reasoning behind these decisions or appeal them. This will make it even harder for migrant workers, refugees and asylum seekers to challenge life-changing decisions, such as refusing a visa or asylum application.

The proposal also will enable the government to weave the need for consent for cookies, exposing the personal data of migrant workers, refugees and asylum seekers to targeted advertising. That could lead to discriminatory practices that exclude them from specific jobs, services, and housing based on their legal status, race, sex, or ethnicity.

## INTERNATIONAL DATA TRANSFERS

These changes, combined with the other suggested changes about authorising the international transfer of personal data to countries without proper laws or safeguarding procedures for data protection rights, will have catastrophic consequences on refugees and asylum seekers.

Imagine workers who had fled their country out of fear of prosecution; their data and information may be highly sensitive and need to be protected. However, with the changes proposed in Schedule 5, there may not be a requirement to consider public security, defence, national security, and criminal law when assessing the equivalent level of data protection. It's even worse for people who sought refuge in the UK and applied for asylum. As part of the application process, they must provide personal data, including sensitive information about their work and personal life, to the UK government. Under these changes, the UK government could authorise transfers of their data to their home country or other countries without proper consideration of how this data could be weaponised against them.

## ACCESS TO REMEDIES AGAINST INFRINGEMENTS

The Bill will weaken the role of the Information Commissioner's Office

(ICO) and prevent them from acting to benefit people's interests, especially for a marginalised group such as migrant workers, refugees and asylum seekers. It will hinder their ability to complain to the ICO and expose them to their offenders, biased employers who could discredit their motive leading to the ICO refusing their complaint. This change in power mechanism will expose marginalised groups to abuse, exploitation, and revenge acts. It will also have its chilling effect to avoid getting in trouble by reporting faults or misusing information. It also will strip the ICO its independence and undermine its ability to protect the data rights of migrants, refugees, and asylum seekers. By giving the Secretary of State more power to set the strategic priorities for data protection, the ICO may become subject to political influence and pressure, which could compromise its ability to act independently and enforce data protection laws effectively.

If the Secretary of State's strategic priorities do not align with the best interests of migrants, refugees, and asylum seekers, this could result in weaker protections for their data. For example, the Secretary of State may prioritise data sharing between government agencies over vulnerable populations' privacy and data protection rights. Additionally, the requirement for the Commissioner to have regard to the statement of strategic priorities could limit their ability to act autonomously and impartially when making decisions that affect data protection rights.

#### LESS ACCOUNTABILITY AND DUE DILIGENCE

The Bill also will replace the requirement to nominate a data protection officer (DPO) with an appointed "senior responsible individual" (SRI), which would affect the creditability, independency, and neutrality of the officer. In contrast, under the current GDPR, the DPO must provide independent advice and in-house supervision and operate without conflict of interest. The SRI tasks will range from managerial interests to decision-making, removing the confidentiality and secrecy between them and the employees. In addition to positioning the SRI in a conflict of interest, this situation creates a hostile environment for vulnerable groups around their

digital and privacy rights and protecting their data for fear of intimidation or losing their jobs.

The proposed Bill would weaken the risk mitigation and risk assessment process regarding sharing and using people's data, putting the safety of people who flee their country out of fear at risk. These changes will remove any requirements to consult with people affected by high-risk data processing, exposing them to harm and danger without proper risk mitigation assessment or safeguarding procedures, in addition to weakening the ICO's role to hold the public entities, organisations or private sectors to accountability in case of for any data breaches or violations. This, for example, will restrict the ICO's ability to hold the Home Office accountable for any data breaches or violations of the refugee's data rights. This could put the refugee at risk of having their personal information exposed or used against them, potentially jeopardising their safety and the success of their asylum application. It could also leave them with limited legal recourse or means of seeking redress in case of a data breach or misuse.

## CONCLUSION

It is crucial to ensure that appropriate safeguards are in place to protect individuals' data rights and privacy, especially in vulnerable situations, to prevent harmful online practices from infringing on their rights and perpetuating existing power imbalances.

The changes proposed by the current government could lead to a situation where vulnerable migrants and refugees have less control over their data and are more vulnerable to data protection violations. And could leave vulnerable migrants at risk of having their data and information shared with countries with inadequate data protection laws and limited legal recourse. This could expose them to potential harm and persecution and undermine their digital rights.

It is crucial to ensure that data protection laws are upheld and strengthened to protect the rights of all individuals, regardless of their immigration status or country of origin.

Overall, these changes could have severe implications for the data rights and safety of migrants in the UK, including refugees and asylum seekers, and may limit their ability to seek justice or hold those responsible for data breaches accountable. This could seriously affect migrants' data rights, including refugees and asylum seekers, who may be particularly vulnerable to data breaches and abuses. Parliamentarians should oppose the UK Data Protection and Digital Information Bill by voting against it, emphasising the need for more robust safeguards, and proposing amendments that protect migrant data rights.

**The undersigned:**

Open Rights Group

Joint Council for the Welfare of Immigrants (JCWI)

Privacy International

Migrants' Rights Network

State Watch

Thousand For Thousand (T4K)

Detention Action

Racial Justice Network

Stop the Scan Campaign

Community Action for Refugees and Asylum Seekers (CARAS)

African Rainbow Family

Positive Action in Housing

Haringey Welcome

Refugee and Migrants Forum of Essex and London (RAMFEL)

West London Welcome

Lorraine Masiya Mponela, Author

Claudia Aradau, Professor at King's College London

Siana Bangura - Writer

Roseanna Dias - Inclusion Producer

Nish Doshi - Tech for Good Organiser

William Nicholas Gomes, Human rights activist and freelance journalist

Ellie Hale - Tech for Good Organiser and Producer