Science, Innovation and Technology Committee
House of Commons
London
SW1 0AA

8 July 2026

DATA SECURITY INQUIRY AND eVISA

Dear Dame Chi Onwurah MP,

We are a coalition of 20 civil society groups and experts, active in the fields of immigration policy, data protection, and human rights. We wish to thank the Science, Innovation and Technology Select Committee for raising the issue of eVisa problems during a hearing on data security in government, held on 10 February, 2026.

Due to ongoing instability in the Home Office digital programme, eVisa holders face challenges accessing and proving their immigration status. In a letter sent on 27 November, 2025, we asked the Information Commissioner's Office to intervene against the numerous infringements of UK data protection law that underpin the eVisa scheme.

Thus, we urge the Select Committee for Science Innovation and Technology to support the previous letter received by your Committee, and urge you to open an inquiry into the ICO oversight failures.

Since its rollout, the eVisa scheme has been affected by glitches and data security issues.

UK residents trying to prove their status with eVisas have been facing data entanglement issues- when personal data of an eVisa holder and another, unrelated third party end up being mixed up - as well as denial in accessing the service, generating proof of immigration status, or rectifying or updating incorrect or outdated personal data. As you have correctly pointed out in your intervention during the February 10 hearing, eVisa issues include data breaches, the integrity, availability and confidentiality of personal data. We also commend that the “operational and security problems relating to the eVisa system” were recognised in your Committee’s recent report on Digital ID.

As a study by the3million has found, these issues are systemic and rooted in design and architectural choices. Further, data collected by the Report.it! platform shows

that eVisa holders have been encountering these issues consistently over the past six years.

However, the Home Office has refused to disclose how many of such incidents they recorded, or how many people have complained or sought assistance. We acknowledge that the Home Office has recognised that mistakes are being made and have indicated their intention to resolve them. Nevertheless, it is essential to understand the timescales involved, what transparency they intend to offer on systemic issues and in what forums, and whether they plan to publish a roadmap against which the Select Committee could hold them to account.

We identified and listed numerous failures to comply with UK data protection law by the Home Office. These include failures to adhere to baseline data protection principles, or to conduct and publish Data Protection Impact Assessments (DIPAs) before rollout and throughout the eVisa lifecycle. In light of the above, we also urged the Information Commissioner to open an investigation.

Indeed, we were not the first to raise such issues with the ICO. The press reported that, following a complaint made by a member of the public, the ICO had already determined in June 2025 that the Home Office breached UK data protection law. That complaint was not an isolated case: as disclosed in response to a Freedom of Information request, the ICO received 851 complaints against the Home Office only within the last two years. The volume of complaints against the Home Office is so significant that the ICO would exceed the cost threshold of the FOIA regime if they were to review and identify which complaints relate specifically to eVisa failures. Against this background, the Information Commissioner's Office is yet to take any action to remedy eVisa data protection infringements.

Unfortunately, this follows a pattern that emerged within the evidence discussed in your inquiry into data security in government. As your committee has heard during the February 10 hearing, the government is still working on implementing the recommendations from the Information Security Review, which should have been implemented in full by the end of 2024. Despite these delays, and the very consequential incidents that followed, the ICO has yet to take action, and have so far only sent a letter to "urge" the government to move faster.

While the ICO delays action to remedy these issues, it is eVisa holders who pay the price.

As the "Exclusion by design" report shows, eVisa failures prevent individuals from proving their status when they need it to enter the country, from applying for jobs or getting a pay rise, from o enrollingin education, from claiming benefits. The human

price of non-compliance is high and unjustifiable: UK data protection law already provides for rules that ought to prevent these harms from occurring. It also gives the ICO the role to remedy such infringements and hold public authorities like the Home Office to account.

In fact, the Administrative Court found, in their recent judgement, that the Home Office is able to fix eVisa failures when sufficient pressure is applied. The ICO is the authority with the statutory powers and the Parliamentary mandate to apply such pressure. Further, Parliament has also given individuals the power to raise complaints to the ICO for free, and to seek remedial action without the costs and procedural burdens associated with Judicial Reviews.

There is a risk of reduced scrutiny towards public bodies and diminished responsiveness to public complaints by the ICO.

The ICO has recently signed a memorandum of understanding with the government which was described, by government officials, as a shift away from a relationship of opposition to a relationship of partnership. Likewise, the ICO adopted a new complaints policy, according to which individual complaints would be routinely disregarded unless they reach an unspecified numeric threshold.

As the Home Affairs Select Committee have pointed out in their recent report about digital identity, restoring public trust and ensuring strong safeguards are necessary to deliver digital identity schemes. As the issues surrounding the eVisa scheme demonstrate, these important recommendations risk remaining unmet insofar as the ICO refrains from holding the government to account, to intervene when they get it wrong, and to protect the public from harm.

In light of the above, we urge the Select Committee for Science, Innovation and Technology to:

- Open a comprehensive inquiry into the Information Commissioner's Office and their failure to carry out their oversight duties under the law.
- Investigate what institutional changes are needed to strengthen the ICO ability to oversee the government and other public bodies, also to support the implementation of the recommendations of the Home Affairs Committee's Report on digital identity.
- Further investigate eVisa data practices, governance and failures, to inform the broader inquiry into data security in government.
- Ask the Home Office to disclose the data they hold concerning the amount of data security incidents, complaints and requests for support they received

from the public in relation to the eVisa scheme. We note that on 1 July, the Home Office published error correction volumes from the online webform, but this does not show the volume of *requests* for support.

Signatures:

BARAC UK
ILPA
Imkaan
Liverpool Advocates For Windrush (LAW)
Medact
Middle Eastern Women and Society Organisation (MEW)
Migrant Democracy Project
Migrant Voice
Migrants' Rights Network
No Borders in Climate Justice
Open Rights Group
POMOC
Reunite Families UK
Reset Communities for Refugees
Sherrards Solicitors LLP
South East and East Asian Women's Association
Status Now 4 All
Steve Newman
the3million
The William Gomes Podcast