Space4
113-115 Fonthill Road, London,
England, N4 3HH
Thursday 27 November 2025

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Dear Commissioner,

We, the undersigned civil society organisations, and individuals, write to formally raise concerns regarding serious breaches of the General Data Protection Regulation (GDPR) and accessibility issues within the Home Office's *Digital Status – View and Prove* system, also known as the eVisa scheme, which replaces physical proof of immigration status with a digital-only status. After reviewing the published Data Protection Impact Assessment (DPIA) and collecting evidence of lived experiences, we believe the system presents systemic risks to privacy, equality, and human rights that warrant formal investigation by the ICO.

The EU Settlement Scheme (EUSS) was the initial trial for digital-only status with several million EU citizens receiving an immigration status which could only be proved via an online process. From its rushed rollout in 2018, the scope of digital status has expanded to what is now known as an eVisa. People who once would receive physical proof, such as a Biometric Residence Permit (BRP) or Biometric Residence Card (BRC), now only have an eVisa to prove their right to work, live, study, access public services and travel in and out of the UK. Four million people who had BRPs had to go through a process in 2024 to create a UKVI account to gain access to their eVisa, the digital version of their visa. The eVisa system has caused significant distress and hardship to migrants due to ongoing technical failures, a lack of transparency, data integrity and quality issues, in addition to systemic barriers to accessing the immigration status.

The problems with the eVisa scheme remain unresolved. Now that it has been fully rolled out, the most affected groups are also the most vulnerable. As of June 2025, 36.6% of the problems that were received by a the3million/ILPA reporting tool were from refugees and people with Indefinite Leave to

Remain (who also had a BRP)[1]. At the end of 2024, we started to see cases of migrants being stranded abroad and being denied boarding due to a lack of communication between air carriers and the Home Office, or air carriers not recognising the digital-only status and the sharecode[2].

Our key concerns include:

1. Data inaccuracies and denial of rights.

1.1: Violation of the Accuracy Principle

- Errors in names, visa expiry dates, and photographs have left individuals unable to prove their lawful status.
- Current remediation mechanisms (Resolution Centre, error forms) lack guaranteed response times, leaving people vulnerable to exclusion from work, housing, benefits and education.
- No user journey is provided for rights actions (i.e, how someone can get an urgent change reflected for checks in progress).

Locking people out of their accounts risks exposing migrants and refugees to homelessness and destitution. Over the past year, the same technical problems have repeatedly occurred with eVisa accounts. According to the3milion report[3], the most commonly reported problem between April and June 2025 related to issues with viewing the eVisa (21.2%) and problems linking other ID documents to the eVisa (36.5%).

A frequent problem lies in discrepancies between the Machine Readable Zone (MRZ) on certain passports and the way UK systems store those details. Problems arise when names are shortened, misspelt, or altered following marriage or other legal changes. These are not isolated glitches; they reflect deeper flaws embedded in the eVisa infrastructure. Efforts to correct errors have at times made matters worse. In March 2025[4], for example, large numbers of users were locked out of the UKVI portal or encountered incorrect information associated with their eVisa accounts. The Home Office later confirmed this happened because a patch intended to resolve a bug elsewhere in the system unintentionally disrupted other functions. This illustrates how fragile the platform's design is; a single rushed repair can trigger a cascade of new technical problems.

Most of these problems could in theory be solved by reporting the error to the Home Office directly or to a charity organisation, who can support a person to report the error to the Home Office. However,

---

1 https://the3million.org.uk/sites/default/files/documents/t3m-report-evisa-problems-2025-Q2-01Aug2025.pdf

2 https://www.finnair.com/gb-en/travel-documents/travel-documents-to-the-usa--uk--canada-and-australia

3 https://the3million.org.uk/sites/default/files/documents/t3m-report-evisa-problems-2025-Q2-01Aug2025.pdf

4 https://the3million.org.uk/news/2025-03-06/widespread-identity-document-errors-digital-status-evisa-accounts

given the eVisa's role in time-critical checks to prove a person's right to work, rent, travel, enrol in education, or secure a loan, delays can have real-life consequences.

The Home Office's reporting tool, available through the Resolution Centre, is now fully automated, and people are finding it increasingly difficult to interact with a human. If they are unable to find their problem listed in the services menu, the phone call is dropped, and the line automatically disconnects.

We Are Group[5], the private contractor to whom the Home Office has outsourced its role in supporting people to create their eVisa operates only in English and is unable to provide support for any technical errors. The accompanying chatbot, designed to assist people, merely repeats the same information available on the Home Office website and does not provide any additional support.

None of the tools mentioned above can help with technical issues. About 71% of submissions to the3milion reporting tool, between April and June 2025, reported attempting to reach the Home Office through the UKVI phone line, webchat, or email without any resolution[6]. Mitigation measures depend on an operational team, but no KPIs or surge capacity plans are documented[7].

2. Problems with the DPIA:

2.1: Digital only status not Digital by default:

- The Home Office states in their DPIA that, the Digital Status – View and Prove system is *"As part of the transformation of the UK immigration system to "digital by default"* .

This information is misleading and contradicts the fact that the eVisa scheme is now a digital-only and a live check status, as stated by the Home Office in one of their written communications with Open Rights Group (Appendix-1). The eVisa scheme removes all physical evidence of immigration status, with no fallback option available. Users cannot opt out of digital methods, which is contrary to the principle of digital by default as stated in the Government Digital Strategy [8].

This is not how a digital-by-default system would typically function: whereas a default option implies the existence of an alternative, non-default option, eVisa gives migrants no choice over how to prove their status. It is also ignoring the concerns voiced in the government report for the beta assessment of the Home Office's Prove your right to work service on 2 March 2018, which highlighted that:

"The services are easy for digital savvy users to get through, and the team have a good support model in place for helping low digital users through the service, although they are aware from user research

[5] https://www.wearegroup.com/

[6] https://the3million.org.uk/sites/default/files/documents/t3m-report-evisa-problems-2025-Q2-01Aug2025.pdf

[7] https://www.gov.uk/government/publications/digital-status-view-and-prove-data-protection-impact-assessment/digital-status-view-and-prove-data-protection-impact-assessment-accessible

[8] "By digital by default, we mean digital services that are so straightforward and convenient that all those who can use them will choose to do so whilst those who can't are not excluded." https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy

how unlikely it is that low digital users are to use the online service at all. This research raises concerns around BRP cards being retired in favour of digital only services, as the team has very strong evidence that this would cause low digital users a lot of issues. This is something that needs careful consideration with the drive to convert more services to digital and potentially remove their physical counterparts - that digital by default doesn't mean 100% digital."[9]

2.2: Biometric and special-category data risks

- Face images are stored and displayed without clear minimisation safeguards.
- No explicit prohibition on future facial recognition or automated use by third parties.
- The DPIA's screening out of profiling/ADM is fragile (no clear future-change controls), and it does not describe strict governance for biometric data minimisation or contextual limits on display/share.

The DPIA states that special category/biometric data (face images) are processed. It also states "no"to the presence of automated decision-making and profiling[10].

Biometric images are highly sensitive (uniquely identifying). The DPIA does not fully assess risks if face images are used for matching, automated checks, or shared with third parties that may combine them with other datasets.

There have been a high volume of instances where individuals discovered inaccurate personal details on their eVisas, including photographs, names, visa end dates, or even passport numbers. Not only is this a huge breach of sensitive data, but it may result in complete failure of the system, insofar as an individual is unable to prove their status, and unable to prove their rights, leading to serious harm. There is a well-documented case where entangled data occurred between two different individuals who visited the visa centre in different locations (Details in Appendix 2). The Home Office has not to offered any explanation as to what triggers such an error or entanglement. The Guardian[11] previously reported on this issue, asserting that malfunctions in the Home Office's system led to around 76,000 instances where individuals' immigration records became entangled with those belonging to other people.

Furthermore, the statement that "no" automated-decision making would be involved appears questionable. Border control and other operators will inevitably take decisions based on the information they are provided with when querying the eVisa system. Against this background, there is an obvious risk that officers and other decision-makers would take the information provided by the eVisa system at

---

9 https://www.gov.uk/service-standard-reports/prove-your-right-to-work-beta#to-pass-the-next-assessment-the-service-team-must

10 https://www.gov.uk/government/publications/digital-status-view-and-prove-data-protection-impact-assessment/digital-status-view-and-prove-data-protection-impact-assessment-accessible

11 https://www.theguardian.com/uk-news/2024/mar/14/home-office-immigration-database-errors-hit-more-than-76000-people

face value and act upon it without any meaningful oversight.

Meaningful human involvement and oversight would require human operators to:

- Have access to the relevant information needed to understand and evaluate the information given by the eVisa system.
- Have the agency and the means to intervene and, when necessary, override a decision taken on the basis of the information provided by the eVisa system.
- Actively strive and mandate for decisions taken on the basis of the information provided by the eVisa system to be fair, unbiased and to respect individual rights.

The DPIA does not give any indication as to whether technical and organisational measures to meet these standards have been implemented.

2.3: Risks to individuals without phones:

- The DPIA has not assessed or mitigated the risks faced by people without smartphones or digital access. This omission represents a significant failure in equality and human rights, as it overlooks a foreseeable and well-documented form of exclusion and risk.
- There is no equality impact assessment of how individuals who are digitally excluded (due to poverty, disability, age, or other barriers) can access or prove their immigration status.
- Risks from reliance on friends or family for access to personal eVisas such as partner coercion are both foreseeable and require mitigation.

Nowhere in the DPIA is there a detailed risk analysis of people without smartphones, internet access, or digital literacy. People without smartphones or consistent internet access cannot easily retrieve or present their eVisa status, especially when proof is needed urgently. There is also no mention of alternative channels for those unable to use the digital platform. The government justifies such measures by claiming to provide small funds for charity organisations to help people who lack access to smartphones or digital literacy. This approach forces reliance on third parties or intermediaries, thereby undermining autonomy and privacy. Furthermore, the funding is only provided on a once-and-done principle, providing funding to help individuals set up their initial UKVI account, but not to help individuals who struggle on an ongoing basis to use their UKVI account to provide proof of their eVisa to others. In line with this once-and-done approach, the funding has reduced dramatically (£400,000 for the six months to 31 March 2026, reduced from previous funding of £4 million for the year to 31 August 2025). It is not known whether there will be any further funding from April 2026.

2.4: Large-scale data processing:

- The processing involves special categories and is on a large scale; it includes data of children (aged 13 or younger).

- No detailed extra safeguards for children or vulnerable groups, nor impact analysis for equality harms (e.g., migrants with precarious statuses, such as those with temporary leave to remain in the country and those with refugee status).
- It acknowledges nationality/race appears in datasets and that sensitive categories are processed, but there is no granular equality analysis.
- No disaggregated risk assessment (how harms differ by nationality, asylum status, gender, age).

Migration status and nationality intersect with protected characteristics (race, nationality, religion) and vulnerability. Inequalities can be exacerbated by data errors.

2.5: DPIA is reactive / retrospective and does not commit to continuous review against harms

- The DPIA has been updated retrospectively to reflect the rollout; ODPO referrals exist, but many edits are redacted.
- The DPIA treats future technological changes as “No” for profiling/ADM/monitoring without hard controls to prevent future drift.
- Some answers (access control, security measures) are redacted. It claims logging capability for law enforcement processing, but provides inconsistent "Yes. No." answers in places.
- Inconsistent or redacted statements about logging, access control and security weaken assurances. Transparency regarding who can access data, what is logged, and who audits the logs is essential for detecting misuse and upholding rights.
- Redactions reduce external scrutiny and make it harder to trust safeguards.

The Home Office has approached the DPIA as a one-off compliance exercise rather than a living process for identifying and mitigating risks. The DPIA has been conducted retrospectively and updated reactively, with no commitment to continuous review as new harms emerge. This approach treats the DPIA as a procedural “tick-box” document rather than a tool for accountability and improvement. It fails to evaluate or address the well-documented problems that have arisen since the eVisa system’s rollout, such as data inaccuracies, system outages, and barriers to correction.

3. GDPR violations

3.1: Lack of Transparency

- Migrants are not adequately informed about how their data is processed, stored, or shared.
- There is a lack of clear information on how errors can be corrected or how to challenge system decisions. This contradicts transparency obligations under the UK GDPR and the DPA 2018, which require providing individuals with information that allows them to exercise their data

protection rights effectively.

- Information about personal data is not provided in a manner that allows data subjects to understand it.
- English-only systems exclude non-English-speaking migrants, making the process inaccessible.
- The DPIA doesn't show comprehension, nor tailored notices for vulnerable groups or children.

3.2: Inability to Access Data

- Users experiencing technical errors cannot view or prove their immigration status.
- Some migrants are locked out of their accounts, violating their right to access their personal data.
- Migrants with disabilities may be denied access to their personal data due to the system's lack of accessibility.
- Migrants have the right to access their data, but their ability to exercise this right is limited if they cannot understand the workings of the platform.

3.3: Accountability

- The Home Office must demonstrate compliance with GDPR, including ensuring accessibility. Compliance cannot be demonstrated if the Home Office fails to comply with basic data protection principles as outlined above.

3.4: Legal Obligations Under UK Law

- The Home Office has a duty, under Article 35 of the UK GDPR, to conduct an assessment that identifies and contains measures to mitigate potential risks for individuals (such as lack of access to immigration statutes, misrepresentation of one's status, etc) before deploying a system such as eVisas.
- The Home Office acknowledges frequent third-party checks (approx. 100k/month)[12] and public access via links. The scale of checks invites potential scraping, aggregated profiling, and misuse, particularly by private actors or foreign entities, which can lead to breach of privacy and chilling effects.
- Under the UK Equality Act 2010, public bodies (such as the Home Office) have a legal duty to make reasonable adjustments for individuals with disabilities.

3.5: Failure to Recognise Travel Documents and Names on Passports (Data Security and Data Accuracy)

- Refugees with UK-issued travel documents are unable to link them due to a the current shortfalls of the eVisa scheme. At present, and prior to its full roll-out, the system was not

[12] https://www.gov.uk/government/publications/digital-status-view-and-prove-data-protection-impact-assessment/digital-status-view-and-prove-data-protection-impact-assessment-accessible

designed to accommodate all legal statuses, resulting in exclusion.

3.6: Discriminatory Data Processing (Principle of Fairness and Duties under the Equality Act)

- The system disproportionately affects vulnerable groups, including refugees, migrants without biometric passports, and people with limited digital literacy.
- Barriers such as inaccessible design, lack of language support, and insufficient assistance for disabled users lead to unfair and potentially discriminatory outcomes.
- When users cannot understand how their data is processed—due to language barriers or inaccessible information—they are unable to make informed decisions about their immigration status.
- These shortcomings may amount to indirect discrimination under the Equality Act and breach GDPR's principles of fairness, transparency, and accessibility.
- Disability support and inclusive design should be integral to the system from the outset, not added as an afterthought.

We urge the ICO to:

1. Conduct a formal investigation into data protection, GDPR compliance, and equality implications of eVisa scheme.
2. Ensure that migrants can easily access their data through alternative means if they are unable to use the digital system (Offline alternatives).
3. Mandate that the Home Office provide multilingual guidance, free support services, and an available and effective appeals process for system errors.
4. Hold the Home Office accountable for failures to ensure data accuracy, accessibility, and non-discriminatory processing.
5. Create and communicate fast and effective remedies for inaccurate data, ensuring people are not forced out of work, education or benefits or housing, or suffer from their inability to travel, arising from eVisa failings.
6. Require the Home Office to accept full liability for losses arising from the use of UKVI accounts, removing the exclusion of liability clause from its "UKVI account: term and conditions"[13].
7. Require the Home Office to publish its unredacted Data Protection Impact Assessment (DPIA), equality impact assessment for the eVisa scheme, and implement ongoing DPIA updates with each system change.

[13] https://www.gov.uk/government/publications/ukvi-account-terms-and-conditions/ukvi-account-terms-and-conditions#exclusion-of-liability

Signed by:

1. Jim Killock, Executive Director, Open Rights Group
2. the3million
3. Nazek Ramadan, Director, Migrant Voice
4. Dr Derya Ozku, Assistant Professor in Sociology, University of Warwick
5. Dr Marie Godin, Lecturer in Human Geography at the University of Leicester
6. Susan Cueva, Trustee, Southeast and East Asian Women's Association (SEEAWA)
7. Julia Tinsley-Kent, Head of Policy and Communications, Migrants' Rights Network
8. Mariam Yusuf, Chairperson, Status Now 4 All
9. Minnie Rahman, CEO, Praxis
10. William Gomes, Director , The William Gomes Podcast
11. Rose Bernstein, Interim Executive Director, Joint Council for the Welfare of Immigrants (JCWI)
12. Hannah Billington, CEO, Kalayaan
13. Caroline Coombs, Executive Director, Reunite Families UK
14. Louise Calvey, Executive Director, Asylum Matters
15. Moses Seitler, CEO, Screen Share
16. Sasha Haddad, No Borders In Climate Justice
17. Anjona Roy, CEO, Northamptonshire Rights and Equality Council
18. Amina Khanom, Director, Reset Communities for Refugees
19. Rosalyn Akar Grams, Managing Director of Legal Practice and Human Rights, Coram Children’s Legal Centre