

Response to the Government's Consultation on Digital ID

Consultation: [Making public services work for you with your digital identity](#)¹, closed 5 May 2026

the3million has raised the issues that eVisa holders face when trying to access, prove and keep their digital-only immigration status for the last eight years. We took the opportunity to respond to the UK government's consultation on digital-ID to continue to advocate for [Fix the Digital Status](#).

While our position on further rollout of digital ID remains focused on ensuring further protections for eVisa we encourage our members to continue to raise their personal concerns for digital ID programmes. Our focus is to remain in solidarity with migrants and other civil organisations in the call for the end of [Hostile Environment policies](#) that mandate right to work checks and immigration control in public life.

When the Labour Government announced in September 2025 that digital right to work checks would be mandatory for all UK and Irish citizens in the UK the reason for this programme was to stop 'illegal working.' the3million stands with other migrant organisations that vehemently oppose the rhetoric of scapegoating migrants for a rollout of a technical project. There has been no evidence from the nine years of operations of digital right to work checks for eVisa holders that the removal of physical documents stops employers that do not comply with immigration checks. Nor has there been any evidence that the digital format of immigration proof helps stop employment based abuse but in practice can make eVisa holders have a less secure means of proving their rights.

While it is up for public consultation on the future of a national ID programme for UK and Irish citizens to prove their rights, eVisa holders did not get to have a say in how their immigration proof would be accessed. We believe that the national digital ID consultation is an opportunity for the problems and impact of the eVisa system to be heard and fixed. The Home Affairs Select Committee agrees. The Committee's [recent report](#) on the findings from the inquiry on digital ID found recommended that the lessons of the eVisa programme be learned and ensure "opportunities to improve eVisas through the development of digital ID are not missed." the3million continue to collect evidence from people who are experiencing problems proving their rights or accessing their eVisa through our [Report-It Tool](#), co-hosted by ILPA.

In our consultation we focused on:

- Advocating that the existing problems with UK digital identification programme, eVisas, be resolved before any further rollout.
- Our remaining questions about what the national digital ID programme will mean for eVisa holders.
- Highlighting the current barriers non-UK citizens face when trying to access other digital identification programmes, like Government Gateway accounts or One-Login.
- Asking the consultation to clarify if eVisa holders would be able to benefit from the different options that the consultation and if the vulnerable groups identified in the consultation (elderly people, people with disabilities, digitally excluded, children and victims of domestic abuse).
- The lack of transparency over the amount of errors and impact the eVisa system had on users on their ability to access their rights.

¹ <https://www.gov.uk/government/consultations/making-public-services-work-for-you-with-your-digital-identity>

Part 1: Our Ambition

The Consultation asks:

1.0.Q1: *What do you think the main benefits will be, if any, for the government's new national digital ID system?*

1.0.Q2: *What do you think the main drawbacks will be, if any, for the government's new national digital ID system?*

1.0.Q3: *One of the government's aims for the new national digital ID system is to make it easier for people to prove who they are. To what extent do you agree or disagree that the proposed system could help achieve this aim, and why?*

1.0.Q4: *The government proposes to use the digital ID system to enable more modern, efficient and personalised public services. Which public services would you want the government to prioritise making faster or more efficient using the system?*

the3million responded:

Possible Benefits: *If the national ID system included an independent review and support for eVisa holders.*

A well-designed digital ID system could reduce duplication of effort across government departments and make it easier for people to access the services they are entitled to.

However, the government already operates a digital identity system for the [11 to 12 million](#) visa holders in the UK through eVisas, and that system has significant, well-documented failings. The main benefit of this consultation process should therefore be to learn from those failings before scaling up.

A key benefit of the new national digital ID scheme would be that the programmes named as its underlying infrastructure, principally the eVisa, are subject to an independent review of the data processing and implementation problems people have faced. For the digital ID system to deliver real benefits, it must correctly handle the full diversity of names on international identity documents and provide robust error correction and support options when digital systems fail.

It is encouraging that the consultation recognises excluded groups and acknowledges the possibility of people receiving in-person help or being issued with an alternative form of proof. A significant benefit of this programme would be for eVisa holders to gain access to this support and to a more accessible means of proving their rights in the UK. The standards and oversight mechanisms suggested in the consultation to be applied immediately to the eVisa system.

Potential Drawbacks: *The most serious drawback is the risk of replicating and scaling up the exclusion already caused by the eVisa system.*

The consultation names the eVisa programme as part of the fundamental infrastructure on which the new system would be built. However, it does not clarify whether visa holders would be expected to maintain both a UKVI account and a digital ID, or whether the two would be integrated. the3million already receives reports from people who find their UKVI account difficult to keep updated with current identity documents, either because of technical issues or because of the administrative burden of keeping an entire family's account accurate.

People have struggled when travelling, even when their eVisa is accurate and up to date, because carriers do not always engage with the share-code system. As the national digital ID programme would be a core part of how both UK and non-UK citizens prove their rights domestically, a significant drawback would be the impact on visa holders who need to prove their right to reside when returning to the UK. A further drawback is the absence of any physical backup document. When digital systems fail, eVisa holders are currently left unable to prove their immigration status, and a digital-only system with no physical fallback is inherently fragile.

Proving your rights with the eVisa and improving access to public services: *the current problems with digital programmes must be addressed before any further rollout.*

eVisa holders must rely on digital-only proof for all public services in the UK. eVisa holders also struggle to prove who they are when the underlying data, or the presentation of their information on their eVisa, is incorrect. For nearly nine years, the3million has heard from people whose immigration proof displays incorrect information.

- In our [Digital Status Crisis report](#), we share the account of a woman who logged into her UKVI account to find another woman's photograph on her eVisa, rendering her immigration proof invalid.
- In [August 2025](#), a confirmed bug affected thousands of users by changing their immigration status from settled to pre-settled, demonstrating the fragility of holding immigration status in a digital-only format. Immigration proof is not only a form of ID, used to prove who you are, but is what allows people to exercise their rights to live, rent, study, work, access public services, and travel in and out of the UK.

The Home Office justified the eVisa project as improving and [streamlining access to public services for users](#). However, as with any digital project, the automated sharing and checking of data is only as efficient and useful as the underlying information is correct. the3million regularly receives reports from individuals who cannot prove their identity to HMRC, DWP, the NHS, the DVLA, local authorities, and employers, either because they do not have access to their eVisa, there is a data error on the account or the third-party checker is not, or does not know how to, engage with the digital permission.

[HMRC, DWP DVLA services](#) must be the priority, as these are the services where the3million sees existing digital 'lock out'. People are currently unable to create Government Gateway accounts and are therefore locked out of managing their tax, benefits, and pension records. We also see impact on people's lives when there are problems with the DVLA, the NHS, system to system checks fail due to name mismatches due to how the identity application captures someone's name information from the Machine Readable Zone (MRZ) of their passport.

- the3million has documented cases of eVisa holders being wrongfully charged by the NHS because staff would not [accept their share code as valid proof of](#) immigration status. However, speed and efficiency must not come at the expense of accuracy and inclusion.

Faster processes that exclude the same people currently excluded by the eVisa system would simply make exclusion more efficient, and would risk locking out the very cohorts that digital programmes most often fail.

Part 2: How the Digital ID Will Work

The Consultation asks:

2.1.Q1: *Are there technical issuance standards, beyond those already used by the GOV.UK Wallet, that we should be building the national digital ID to?*

2.2.Q1: *Someone might wish to delete their own digital ID from their device. They will be able to do this at any time, and the process will be designed to be simple and quick. Are there any ethical factors government should consider that relate to an individual deleting their digital ID?*

2.2.Q3: *Do you think people should be able to choose to store their national digital ID directly in holder services (sometimes known as 'digital wallets') other than the GOV.UK Wallet?*

2.2.Q4: *To support secure use, there needs to be a robust way to check the national digital ID presented from the GOV.UK Wallet. This will help confirm it has not been faked, tampered with or revoked. The private sector has already developed free and paid-for checking services. In addition, we are considering creating a 'government checker' service. To what extent do you agree or disagree with the proposed government checker service being made available for use in the private and third sectors, at low or no cost?*

2.2.Q5: *Are there any specific limitations you think we should set for the government checker?*

the3million responded:

Improving the technical standards for eVisa: *International standards and the HM Passport office's policy for how names can be recorded in non-UK issued documents must be adopted.*

The system must comply with [ICAO standards for how names can be transliterated, shortened or only reflect someone's birth name, which clearly distinguish between the VIZ and the MRZ](#). The current government identity-checking apps (EU Exit: ID Document Check, UK Immigration: ID Check, and GOV.UK ID Check) all read from the MRZ and treat the result as the person's correct name. In practice, people whose names differ from the MRZ, because their name has been truncated, transliterated, or changed through marriage, are unable to access digital programmes.

One technical solution would be for HM Passport Office's notes on naming conventions to be accepted by other UK government departments, ensuring this lockout does not occur.

- the3million have been supporting a woman whose UK driving licence was recently destroyed by the DVLA because her passport does not show her married name in the MRZ. Some countries do not allow the MRZ of a passport to be changed but will capture the married name in the VIZ. This woman is now caught in an endless loop trying to recover her driving licence, all because "the computer said no".

Even after nearly nine years of operation, the UKVI website remains in "beta". New technical features continue to corrupt data quality: when new software is deployed or a bug is fixed, it can cause problems elsewhere in the system.

- A recent example is the programme automating extensions for people moving from pre-settled to settled status, or extending their existing status, where delays in issuing the new grant have left people's eVisas displaying as "expired".

The consultation needs to take the severity of data quality issues seriously, because if a visa holder's eVisa is incorrect, they have no reliable back-up to prove their entitlements and rights in the UK.

eVisa holders must benefit from the support proposed with the national digital ID programme: *there are currently eVisa holders that would benefit from extra support and backup options for proving their rights.*

Any digital ID programme that integrates eVisa holders must take into account the different stakes and use cases between UK citizens and visa holders. For UK citizens, the digital ID would largely be a transformation of existing identity documents such as passports and driving licences. These are relatively static forms of identity, with only possible changes for things like name, address, or gender. For eVisa holders, by contrast, permissions, rights, and entitlements can change frequently because of differing visa conditions and the time-limited nature of immigration status. The deletion of an account therefore carries significantly greater consequences for visa holders, and the ethical considerations around deletion must ensure that users can still prove their rights in the UK.

The eVisa experience demonstrates the dangers of a digital-only identity system with no physical backup. If someone deletes their digital ID, or loses access to the device storing it, they must still be able to prove their identity and access public services. Beyond the data problems eVisa holders have faced, there is also widespread concern that proof of immigration status can be changed overnight or erased entirely.

Any digital ID cannot be deleted without considering safeguards for immigration status:

For eVisa holders, any disruption to their digital status has immediate real-world consequences, including the inability to work, rent, access healthcare, or travel. The government must ensure that revocation does not leave individuals unable to prove their identity or access essential services, even temporarily.

There should be a mandatory physical backup document that remains valid during any revocation process, and individuals must be given clear notice and the opportunity to challenge a revocation before it takes effect. Any revocation of a digital ID must also follow the same standards of proportionality and procedural safeguards that apply when the Home Office curtails or cancels a visa holder's leave.

Giving eVisa more autonomy: *There was no public consultation for eVisa holders the national digital ID must prioritise fixing the existing digital proof of rights.*

eVisa holders were not given any choice on how their immigration status is stored, accessed or displayed to third parties. The national ID programme should give the current 11 to 12 million people who rely on an eVisa to prove their right to work, rent, study, access public services and travel in and out of the UK to decide the format of their immigration proof. [the3million continues](#) to raise that the rollout of digital- only immigration status used the EU Settlement Scheme (EUSS) as a 'guinea -pig' pilot to rollout the eVisa project. The eVisa programme has not benefited from the oversight and user input that the national digital ID consultation suggests as people subject to immigration control are at the discretion of the Secretary of State on how immigration proof is issued. the3million proposes the eVisa should be stored in a QR format (like a COVID-pass) giving the user the ability to store the eVisa on their phone or print out their immigration proof. Currently, eVisa holders must rely on the internet and the UKVI website to work to prove their rights in the UK. the3million urges the consultation to provide and support equal autonomy to eVisa holders on the storage options for their immigration status.

However, allowing multiple storage options does not address the fundamental problem: if the underlying identity data is wrong, whether due to a Home Office error or a technical fault, it will be wrong regardless of where it is stored. Data accuracy must be resolved at the point of creation, not delegated to storage providers.

Give eVisa more control over their digital identity: *eVisa holders do not benefit from the same data minimisation control as suggested by the consultation.*

eVisa holders should be given greater certainty that the underlying data of their account will allow them to use their digital credential. The digital ID checks should return only the minimum information

necessary for the specific verification, in line with the principle of data minimisation. It must not expose full biographic data where a simple yes/no confirmation would suffice. There is a problem that with the Government Checker service people who are using the service may not fully understand the information presented and the rights of this person.

As UK public bodies are obligated to check immigration status in most cases, there must also be ethical safeguards and training for staff on how to interpret the different permissions that visa holders hold in the UK.

- The eVisa programme has shown that significant barriers to accessing critical public bodies and support arise when members of staff do not have the necessary training to interpret an eVisa correctly. [the3million is aware of problems eVisa holders face when the "title"](#) on their account is misinterpreted by public bodies as meaning the person is not eligible for public funds or support.
- For example, people granted permission as a dependant of a refugee, or under other family routes, may have entitlements to public funds even though their eVisa title shows "Dependant". Because the person seeking support has no autonomy over what data is shared or minimised, there have been implementation issues when information is not shared when it would be helpful for the individual.

An eVisa title states what type of permission the person holds, while a separate section of the check sets out what they can and cannot do in the UK. If the national digital ID programme is rolled out with the design principles that there is no 'one-size fits all' but can reliably adjust and support individual needs, there could be more trust and buy-in from individuals. There must be more user control on how the information shared is displayed and shared that is not dictated by standardised data minimising practices.

Currently, eVisa holders have reported problems to the3million when travelling, even when their account is up to date with their most recent travel document. There is no way for an eVisa user to easily confirm, before they travel, that their account will return the correct information to carriers through the backend system the Home Office uses.

People visiting the UK are provided with a service to check that their [Electronic Travel Authorisation \(ETA\)](#) is in date and working. A similar service for eVisa users would help them feel more secure when travelling, by assuring them that what they see on their eVisa account aligns with the backend system used by carriers.

Part 3: Wider Uses of the Digital ID

The consultation asks:

3.1.Q1: *What further information, if any, should the digital ID also include?*

3.1.Q2: *The government is not planning to initially include address information on the national digital ID, but we may review this position in the future. If your organisation were to rely on this information, what would help you trust an address on the digital ID?*

3.1.Q3: *Businesses and organisations accepting the national digital ID need to trust that the information on it is up to date and accurate. We are exploring whether people with a digital ID should be legally required to inform the government within an appropriate timeframe of certain changes (such as a name change) or errors to their personal information, so that their digital ID can be updated. To what extent do you agree or disagree with a legal requirement to inform the government of changes or errors within an appropriate timeframe?*

3.2.Q1: *Are there examples of any barriers or inefficiencies that prevent you (or people you support) from interacting with public services, that you think the digital ID system could help with?*

3.2.Q2: *Have you ever faced issues with knowing which public services are available to you, or have you faced similar issues when supporting others?*

3.2.Q3: *Have you ever been unable to or had difficulty accessing a public service because you were unable to prove your identity, or have you faced similar issues when supporting others?*

3.2.Q4: *To what extent do you agree or disagree with the adoption of an approach to securely identify and match people across different public services*

3.2.Q5: *What ethical issues, if any, can you think of when designing a way to identify and match people across services?*

3.3.Q1 *To what extent do you agree or disagree that the private sector and third parties should be able to use the digital ID alongside other options?*

3.4.Q1: *Are there any additional challenges not captured in the consultation that businesses would face in carrying out fully digital right to work checks for all new workers?*

3.4.Q2: *Would any additional support not captured in the consultation be required for business to comply with fully digital right to work checks?*

the3million responded:

Data minimisation principles: *eVisa data minimisation principles are currently a 'one-size fits most'*

The consultation states that a person's nationality will be displayed on their account. Data minimisation principles should mean that eVisa holders are not required to display this information when it is not relevant to the check being carried out. For example, if the national digital ID is used to prove a person's age, eVisa holders may not wish to display their nationality in that setting, whether out of personal preference or fear of discrimination. The programme must include options that allow individuals to control which information is displayed for different types of checks.

Individuals may be incentivised to keep their information up to date, provided they are given sufficient support to manage the digital system, if the digital ID is useful for them to easily prove their entitlements. However, a legal requirement to report errors becomes problematic when, as is the case for eVisa holders, the error in the data may have originated in the government's own systems.

As the eVisa programme demonstrates, people may not need to prove their immigration status or identity frequently, and may only access their account when prompted by a trigger event such as a hospital visit, imminent travel, or an application for support from public services. When someone has not checked their account for some time and is suddenly confronted with an error, the immediate impact is on their ability to prove their rights.

A legal mandate to report errors risks placing the administrative burden on users and could create a situation where people feel compelled to check their digital ID constantly, in a way they would never need to with a physical document. Passports and driving licences do not change overnight, but a digital credential can be correct one day and wrong the next. The burden of identifying these errors should not fall on users. Imposing a legal duty on individuals to report errors that the government's own systems have created, while providing no effective mechanism to correct them, would be unjust.

If such a requirement is introduced, it must be accompanied by: a simple, reliable process for individuals to request corrections; a guaranteed response time; and no penalties where the error originates from the government's own data capture processes.

Public service access: *Not everyone has a eVisa who might need one*

For visa holders to access public services, in most cases, they must have access to their eVisa. There are an estimated 200,000 people as of January 2026 that need to set up their accounts with the Home Office; this cohort should benefit from the in-person support that the consultation mentions for people enrolling in the digital ID programme. There needs to be support for people who English is not their first language or have difficulty independently accessing technologies.

Matching Services technical and ethical questions: *There must be safeguards for data errors not cascading throughout government*

Cross-service matching would make matters worse if it relies on the same flawed name data. Before adopting this approach, the government must resolve the underlying data quality problems, store both MRZ and VIZ names, and develop matching logic that accounts for the known, well-documented variations between MRZ and VIZ names. There would be a problem for someone who has not had their name accepted by HMRC to then face issues in other public departments in a cascading effect. The most pressing ethical issue is that errors in one system could cascade across all systems, compounding harm

There are also significant equality concerns. Non-UK citizens, primarily women (who more often have married name discrepancies), and people from countries with naming conventions that do not fit the MRZ format. There must be protections for people who had an administrative error or problem with their eVisa not to face problems with all UK public bodies at once. As eVisa status can update more regularly than a person might change their name or upload a new passport there would have to be safeguards that one error of status (expiry date, type of visa, name, lists of entitlements) do not instantly cut that person off from much needed support.

The consultation process should address the current data matching errors that the Home Office experiences when people have similar [biographical data](#) or a human administrative error on the person's most current leave in the UK. As the eVisa system operates within a database that contains 220m identity

records in the immigration database even a small percentage of errors can impact thousands of people's records. The eVisa programme must demonstrate to its users that the digital only proof of immigration can be reliable and error mitigations trusted before there is any further rollout of data matching services.

Voluntary ID must not turn into mandatory: *Cohorts that are exempt from having an eVisa to prove their right to travel have faced barriers.*

Physical documents must remain a valid alternative, and the data on the digital ID must be accurate.

The private sector already encounters these problems. Employers conducting right-to-work checks using the Home Office online service face name mismatches, and landlords conducting right-to-rent checks face the same. Extending a flawed digital ID into the wider economy without first fixing the underlying data quality would compound the exclusion that already exists.

Physical documents must also remain a legally valid alternative for all purposes where the digital ID is accepted. There is still a cohort of visa holders who use legacy documents, such as a wet stamp or vignette showing Indefinite Leave to Remain, to prove their right to travel in and out of the UK. However, as [digital permissions for visa holders and visitors have become more widespread](#), holders of these physical documents have experienced implementation problems when carriers are not familiar with them. The difficulties this cohort faces serve as a warning that, even where people are

formally exempt from digital identification programmes, their ability to prove their rights risks becoming digital-by-default in practice, as third-party checkers insist on an electronic version of proof.

Right to work checks: *The existing digital only right to work checks have failed people*

There must be an independent review on the problems reported by eVisa users who have struggled to prove their right to work using the digital service. Additionally, there must be a wider campaign and training for employers on how to check immigration status using the eVisa system.

the3million has documented cases of digital right-to-work checks failing because of data quality issues or because employers struggle to operate the online checking service. Reports from eVisa holders show that these implementation problems can hinder a person's ability to prove their right to work, and add the further burden of having to advocate for their future employer to use alternative sources of verification, such as the Employer Checking Service. There is a concern that employers may simply choose not to hire someone, or may decline to engage with the additional steps required.

There is currently no audit mechanism through which eVisa holders can raise concerns about how employers handle their checks or about the implementation problems they have experienced. To ensure that digital programmes work for end users, there must be a way for people to report not only formal errors, but also broader problems with using the service.

The existing eVisa system has already created a two-tier labour market in which UK citizens face no such barriers, while non-UK citizens must navigate a flawed digital system. There is no concrete evidence that the current digital-only right-to-work checks for eVisa holders have increased compliance with immigration checks among employers who do not conduct checks regularly. Nor does the proposed digital ID scheme address how to safeguard people from exploitative work conditions, which can be a significant risk where workers feel their right to remain in employment is precarious or contingent on their employer's cooperation.

Part 4: Inclusion and Accessibility

The Consultation asks:

4.1.Q1: *All British and Irish citizens, and foreign nationals with permission to be in the UK, who are above an agreed minimum age will be eligible for the national digital ID. Are there any other groups that should be included?*

4.1.Q2: *Which of the following ages do you think is most suitable to access the digital ID system from?*

4.2.Q1: *Some people may face barriers to creating or using the national digital ID. This may be due to difficulty accessing traditional proofs of identity (like passports) or due to a lack of digital access, skills or confidence. Are you aware of any other barriers not captured in the consultation?*

4.2.Q2: *Is there any particular support not captured in the consultation that would help you or other people to use the national digital ID?*

4.2.Q3: *Are there any groups not included in the list that you believe could also be at risk of ID or digital exclusion?*

4.3.Q2: *We are considering dedicated accessible support for those who are digitally excluded, delivered locally, in-person and by trusted organisations. Are there any other ways you think the government should consider supporting those who are digitally excluded?*

4.4.Q1: *The government intends to engage with a range of people and organisations outside of government to help ensure the design and delivery of the national digital ID system is accessible. Can you suggest any specific organisations or types of organisations which the government should engage with?*

4.5.Q1: *We are exploring alternative ways to access the national digital ID for those who cannot use a device. What do you think are the most important barriers for government to address when designing alternative access routes for the national digital ID*

the3million responded:

How do non-UK citizens fit into the national digital ID: *There needs to be a greater degree of clarity on what the digital national ID programme means for eVisa holders.*

The consultation states that foreign nationals with permission to be in the UK will be eligible. It is critical that this includes all eVisa holders, and those whose status is pending or subject to administrative review. It should also include those with outstanding applications who have a right to remain while their application is processed. Children of non-UK citizens are themselves often eVisa holders the question the Consultation must address is how to ethically safeguard the existing children using eVisas.

The government must ensure that the digital ID system does not create additional barriers for people whose immigration status is already complex to prove digitally.

Getting support with digital ID, support beyond enrollment: *From the experience of digitally excluded eVisa holders getting support to create an account does not ensure they will be able to access their rights.*

The consultation also does not address language or literacy barriers. Non-UK citizens may struggle to navigate English-language digital systems, particularly those who are still working to have their status recognised by the Home Office. There remain people whose immigration status has not yet been recognised and who need support to submit an application and gain access to their eVisa.

The Home Office has withdrawn funding from organisations that were supporting people to set up their eVisas, and from organisations that were supporting people eligible for status under EUSS. As more public services are administered through digital programmes, there is a risk that those already excluded from eVisa support will struggle to prove their rights.

The government should fund specialist support through trusted community organisations who understand the specific challenges faced by migrant communities. There must be in person help for both UK and non-UK citizens to not only enroll in the National ID programme but to maintain their accounts or report a problem. The administrative burden on visa holders applying for or renewing their status is already high, and requiring people to maintain two separate accounts may lead to errors, mismatches, or lapses on either or both. If the underlying problems with the eVisa programme are not addressed, the groups already excluded from independently accessing their immigration accounts will face compounded difficulties when trying to access support through any new digital ID system

Groups that are at risk of digital exclusion: *Some eVisa holders belong to the identified vulnerable groups this cohort should benefit from the same accessibility measures and safeguards.*

All eVisa holders should be given the same benefit of a backup document that does not rely on having internet, a smartphone or computer and digital literacy. The government must issue a secure backup (like a QR code linking to the digital record) to all digital ID holders, but especially eVisa holders who face immediate consequences if their account data is not correct.

Additionally, the government should fund trusted community organisations to provide in-person support for digital ID registration and problem resolution, particularly for non-English speakers and those with complex identity document situations. The government should engage with organisations

representing migrant communities, including organisations that have assisted in vulnerable people setting up their eVisa to understand that support for users cannot stop at account set up.

- [A caseworker who was part of a grant funded organisation](#) that helped vulnerable people to create an eVisa makes clear that helping setting up a digital account does not mean that a person will be able to independently keep the account up-to-date or prove their status.

Critically, the government should engage with the Independent Monitoring Authority for the Citizens' Rights Agreements (IMA), which has oversight of the rights of EU citizens under the Withdrawal Agreement and has been made aware of the digital status problems documented in this response. The government should engage with organisations representing migrant communities, including organisations that have assisted in vulnerable people setting up their eVisa to understand that support for users cannot stop at account set up.

Part 5: Trust and Oversight

The Consultation asks:

5.1.Q2 *How should the government ensure transparency around how national digital ID data is used?*

5.2.Q1: *Are there any additional security safeguards that should be considered in relation to the national digital ID system?*

5.4.Q1: *What additional oversight mechanisms, if any, should be put in place for the national digital ID system?*

5.4.Q2: *What measures can you suggest that could be put in place to make sure people can resolve issues with their national digital ID?*

the3million responded:

Improve the transparency standards for the eVisa programme: *The standards of accountability and oversight have not been applied to the eVisa programme in practice.*

The government must commission an independent review of the existing eVisa system before launching the national digital ID, to identify lessons learned and ensure they are applied. The experience of eVisa holders should be central to the new programme as this cohort has already experienced a form of mandatory digital identification.

Transparency is essential because the current eVisa system operates with very little. At the time of writing there have been no public accounts on the amount of errors that have been reported by eVisa holders or robust oversight on the impact of the project. The consultation offers encouraging steps for oversight but these must be applied immediately to the eVisa project before there is a further rollout of digital ID.

The Home Office in their [exclusion liability states](#): "The Home Office is not liable for any loss or damage that arises from use of the UKVI account. This includes: any direct, indirect, or consequential loss, any inability to use the UKVI account, any disruption to access to the UKVI account, any information that is lost or corrupted while data is being transmitted, processed or downloaded from the UKVI account." Because of these terms and conditions eVisa holders do not have a straight forward path to redress if there are issues that occur and directly impact their lives. These terms and conditions for digital status holders must be examined under the consultation to ensure that visa holders can benefit from the same protections as UK citizens if a technical issue results in harmful impact on their lives.

Enabling visa holders to integrate into the digital system would require additional funding and support for immigration advisers. Because eVisa holders are required to maintain an online account in order

to prove their rights, comprehensive support must be available for those struggling to regularise their status.

The government should introduce a guaranteed maximum response time for identity data correction requests, with triage based on urgency, for example where a person needs to prove their rights that day or in the near future in order to travel, work, rent, or study in the UK. Where complaints are not resolved at the first stage, there should be a clear escalation route to an independent body. There should also be greater transparency with end users about updates, system changes, and problems affecting their accounts, so that people are not left to discover errors only at the moment they need to prove their rights.

The eVisa programme must be resolved and used as an example of potential pitfalls for the national digital ID programme. The current silos with how different UK public bodies technology capture and store individuals' names is currently excluding non-UK citizens from programmes with no clear route to resolving the problem. An oversight body would need to focus not only on registration of national ID but the entire lifecycle of the project - with an emphasis on the harms that occur when an error on an account prevents people from proving their rights.

Part 6: Wider Summary of Impacts

The Consultation asks:

6.1.Q5: *Do you believe there are any other wider impacts from introducing the national digital ID system that have not been considered in this consultation?*

the3million responded:

The consultation does not adequately address the risk that a national digital ID system could deepen existing inequalities between UK citizens and non-UK residents. The eVisa system has already created a situation in which non-UK citizens face barriers to everyday life that UK citizens do not. If the national digital ID is built on the same technical foundations, these inequalities will be extended and entrenched.

If the infrastructure of the eVisa system is not resolved before the national digital ID programme is rolled out, there is a serious risk of repeated failures that will continue to hinder people's ability to prove their rights in the UK. There must be a standardisation of accountability across the eVisa programme and the national digital ID, to ensure that further exclusion of visa holders is not perpetuated.

The consultation does not address the systemic failures that eVisa users have faced; there must be clarity and technical solutions to fix the current mandatory digital programme.