Afghan Pro Bono Initiative

Hosted by **Refugee Legal Support** and **Safe Passage International**

Information Sheet: UK Government Afghan Data Breach

[Last updated: 2 September 2025]

This factsheet provides information about data breach incidents relating to the UK's Afghan Protection Schemes. It is intended as a resource to help Afghan nationals and their family members in their understanding of these events and does not constitute legal advice.

Please note that the information provided within is drawn from the limited information as provided by the UK Government. Wherever possible we strongly encourage you to seek legal advice in respect of your individual circumstances.

You can find template letters to support applicants under the UK's Afghan Relocations and Assistance Policy (ARAP) and its forerunner, the Ex-Gratia Scheme (EGS), who have been affected by the Afghan data breach here.

This factsheet has been updated as further details become available.

What are the data breaches?

There have been several different data breaches relating to applications made within the Afghan Relocation Schemes.

On 21 August 2025, the BBC reported that the Ministry of Defence has admitted that there have been 49 separate data breaches in the past four years in the team that has been handling the Afghan relocation applications.

There is limited information available about all of the leaks. Those which are known about so far are:

1. September 2021

The breach occurred when an email from the ARAP team was sent to applicants, including the addresses of 265 applicants in "copy". Individual recipients of the email were able to see the addresses (and in some cases location and photographs) of the full list of recipients to which it had been sent.

Information about this incident indicates that all of the recipients were individuals who had worked as interpreters.

The Information Commissioner's Office ("ICO"), the UK authority which regulates how personal information is stored and used, investigated the breach and fined the Ministry of Defence.

Those who have been affected have been contacted directly by the Ministry of Defence.

A compensation scheme has been established for those who were affected.

2. August 2025

On 15 August 2025 it was reported that a subcontractor to the Ministry of Defence, The Jet Centre, suffered a cyber-security incident that may have compromised the personal information for up to 3,700 applicants to the ARAP scheme. Those affected are understood to have arrived in the UK between January and March 2024.

Why do we only know about the breaches from 2022 onwards, now?

The breach that occurred in September 2021 was known about publicly at the time but those which have occurred thereafter have only recently been publicly reported.

This is because:

i. The UK government did not become aware of the February 2022 breach until August 2023;
ii. The UK government took legal steps to prevent the reporting of the February 2022 and August 2023 breaches; and
iii. The reporting of the February 2022 and August 2023 breaches were not permitted by the Courts until 15 July 2025.

Other than the information reported by the BBC regarding the number of breaches, we do not currently have any specific or further information about the other breaches that have occurred.

What did the UK government do about the February 2022 breach?

Reports indicate that the UK government took steps to:

- Prevent further dissemination and publication of the spreadsheet;
- Prevent the reporting of the spreadsheet's existence; and
- Assist individuals it considered to be most at risk of harm if the spreadsheet were to be obtained by the Taliban.

When the Ministry of Defence was contacted by journalists who were aware of the leak in August 2023, the Ministry of Defence firstly asked the journalists not to publish anything because of the seriousness of the risks that it posed to individuals on the list.

Then, the Secretary of State for Defence applied to the High Court for an injunction to prevent the publication of information about this leak.

As a result of the application for an injunction, on 1 September 2023, the High Court issued a strict court order – known as a super-injunction which prevented anyone from sharing information about the breach, or even about the court order itself. This was the first time that a court order of this kind had been made and it was reviewed again by the High Court in November 2023, February 2024, May 2024, July 2024 and July 2025. The super-injunction was eventually lifted by the High Court on 15 July 2025. You can read the judgments relating to the injunction being made and lifted here.

In April 2024, the UK government opened a specific relocation programme, the Afghanistan Response Route (ARR), to bring individuals and their family members who were at risk to the UK. The existence and eligibility criteria for ARR were not publicly disclosed and it was by invitation only. We now understand that for an individual to be eligible for assistance under ARR, they must have been:

i. affected by the breach (i.e. their information had been included in the spreadsheet)
ii. considered to be at the highest risk of targeting by the Taliban;
iii. located in a high risk country; and

iv. previously not received a grant of assistance under any of the existing routes (ARAP, ACRS, etc.)

The UK government confirmed that on 4 July 2025 the ARR closed.

How do I know if I am affected by the data breaches?

Those impacted by the September 2021 breach will have been contacted directly by the Ministry of Defence some time ago.

For the February 2022 breach you can use the Data Incident Self-Checker to find out whether you (and any family or dependants cited in your application) are affected.

If you submitted multiple applications, you may have been given more than one reference number. The Government guidance explains that you will need to check every reference number you have been given.

If you have never applied for ARAP or EGS (for example, you applied only for ACRS or another scheme) your data also cannot be subject to this breach because it will not have been on the spreadsheet.

Additionally, you may have received a letter from the MOD which looks like this or this.

For the other data breach incidents, it is unclear how you can confirm if you have been impacted. It is likely that you will need to write a letter to request confirmation.

I have lost my documents/I don't know my reference numbers – what can I do?

If you don't know your ARAP, EGS, or ATAE reference (or not all of them) you can use this contact form to ask the Ministry of Defence to tell you. You should ensure that you give all of your names (especially if you can spell your name in multiple ways) and you may be asked to give more information if they cannot immediately locate your records.

You can also make a "Subject Access Request" (SAR). This is where you ask a government department to give you a copy of all the records that it holds about you. If you worked with the Ministry of Defence in Afghanistan, you can find the form to make a SAR here. Other government agencies may have a different process for SAR; if you have worked with other Government Departments (for example the Foreign, Commonwealth & Development Office ('FCDO')) we recommend you search in the

individual webpages of the government agency you worked with for the specific SAR process.

I know I am impacted by the data breach, what can I do?

The UK government has published a guide in English, Dari and Pashto for people who have been affected by the February 2022 incident.

If your data was breached, we would suggest that you:

i. carefully consider and follow security advice on remaining safe;
ii. keep records and evidence that you think is shows that you have been affected by your data having been included in the leak; and
iii. consider the information below about what options you may have in relation to your ARAP application.

Security advice

The following is a summary of advice included by the UK government in its information page. Much of the advice is common sense and is worthwhile following even if you have not been directly affected by a data breach:

- consider changing your contact details – make sure you maintain access to the address given in your application form in case the DARR team need to contact you.
- be especially careful of taking phone calls or responding to messages or emails from unknown contacts;
- limit who can see your social media profiles and consider shutting them down if you need to;
- be careful of accepting friend/follow requests from individuals you do not know and trust;
- monitor your online accounts to check for any unauthorised access or change in settings;
- where possible use a Virtual Private Network (VPN) to access the internet;

- be wary of telling anyone that your personal data may be vulnerable because you may draw attention to the fact that your information could be exploited; and
- be particularly careful if travelling or crossing an international border.

Scam emails and SMS

There have been reports of people receiving emails and text messages that suggest that they are eligible for compensation as a result of the data incident. It is highly likely that these are not official and are scams which should be reported and deleted.

If you receive any emails or text messages which claim to be from the Ministry of Defence, DO NOT reply or click on links or attachments. Be careful to check who has sent a message – anything from the Ministry of Defence will be sent from an email address ending in '@MOD.GOV.UK'.

Additionally, the Afghan Relocation Programme does not have any application or acceptance fees: you do not have to pay for an ARAP, EGS, or ACRS application. If you are contacted about an offer for relocation under the Afghan Relocation Programme and asked to pay money, DO NOT do so.

For further advice on spotting and reporting scams, read the National Cyber Security Centre's phishing guidance.

Evidence: making sure you keep evidence if you believe it is connected to the data breach.

If you believe that you have been targeted or suffered consequences as a result of your data being included in the leak, try to keep evidence and records of what has happened.

For example:

- Take screenshots or photographs of unsolicited electronic communications;
- Take screenshots or print copies of webpages where your information or data has been made available;
- Download copies of any WhatsApp, messaging, or social media accounts before deleting them;
- Take photographs of any letters or notices you receive; and
- If you receive any telephone calls, write down the time and date, any telephone number, and what was said, as soon as possible afterwards.

If it is unsafe for you to keep these records yourself, consider if you have a trusted person in a safe location who you can send them to for safe-keeping before deleting your local copy.

I was relocated to the UK under ARAP/EGS or ARR and my data was in a leak.

If you were found eligible for relocation and have arrived in the UK, a data breach will not affect your status in the UK. However, you may be eligible to make a claim for compensation. There are a number of law firms who may be able to advise you on whether you have a compensation claim.

- Wilsons Solicitors LLP: public@wilsonllp.co.uk
- Leigh Day: ARAPdatabreach@leighday.co.uk
- DPG: newcaseenquiries@dpglaw.co.uk

You should still follow the security advice if you are in the UK. If you receive correspondence which claims to be from the Ministry of Defence, please see below for information about scam emails and texts.

If you have family who you are concerned about, please see below for further information on what you can do.

I have a pending ARAP/EGS application and my data was breached, how will this affect me?

If you or family members are outside of the UK and you are waiting for a decision on an application, you are likely to be feeling anxious about what the breach may mean for you and your family.

The UK government has said that:

- It believes that the risk to people whose personal data was included in the spreadsheet is no longer high.
- It does not believe that the Taliban will use the information to target anyone and that this is why the ARR closed.

But you may have reasons to believe that you or your family are likely to be targeted and you may wish to write to the Ministry of Defence.

To assess this risk you could ask them to confirm what personal data was included on the spreadsheet relating to you and your family. Where relevant you may also wish to explain the impact of the data breach on you and your application, with an explanation for why you are particularly at risk.

RLS has prepared a template letter for people in this situation to ask the MOD to urgently make a decision.
Download the Follow-Up Letter template here.
Alongside the template, we have produced a Letter Guide, which explains how to use the templates effectively. You are strongly advised to read the guides before using the letters.
Download the Follow-Up Letter guide in English.
Download the Follow-Up Letter guide in Dari.
Download the Follow-Up Letter guide in Pashto.

My ARAP/EGS application or ARAP/EGS review has been refused, what can I do?

If your data was breached and you were found ineligible for both your application and following a Review, usually this would mean that your application is finished.

However, you should be entitled to request a further review if you have compelling new evidence that was not available at either the initial application, or when the review was undertaken. We would suggest that where your data being breached puts you at risk (or at higher risk) this should be considered compelling new evidence and you may want to submit a new Review request.

You could include a statement to explain the risks the data breach has created, including detailed information about any new threats that you or your family members have received, any house searches, arrests or other harassment experienced. You can use the APBI ARAP self-help guide which includes a section on witness statements; (see page 32; Appendix 2).

Please note, we cannot guarantee that your request for a further review will be accepted or if your application will be granted. This is because applications are always assessed on a case-by-case basis.

You will need to complete the Review request form here or email: ARAP-Casework@mod.gov.uk.

RLS has prepared a template letter which you can use to request an urgent review if you are in this situation and you know that your data was part of the breach.
Download the Fresh Review Letter template here.

Alongside the template, we have produced a Letter Guide, which explains how to use the templates effectively. You are strongly advised to read the guides before using the letters.

Download the Fresh Review Letter guide in English.
Download the Fresh Review Letter guide in Dari.
Download the Fresh Review Letter guide in Pashto.

I was relocated under the ARAP/ARR scheme and have an Indefinite Leave to Remain (ILR)/ALES settlement. Some of my additional family members were found ineligible (elderly mother/father, adult brother/sister and their families); how can they apply to join me in the UK?

If you included your family members on your original ARAP/EGS application and received a negative eligibility decision, you may be able to submit a review of the decision. Usually the review request must be submitted within 90 days but you may be able to argue that this requirement should be waived if you think that the risks they are facing have are because of or heightened as a result of the breach.

If you did not include your family members in your original application, their details would not normally have been included in the data breach. However, if you are concerned that they are now at risk because of the data breach, you may wish to contact ARAP-Casework@mod.gov.uk and request a form for additional family members. You should set out in detail why your family members are now at risk, and why they were not included in your original application.

If neither of the above situations apply to you or your family members, there is no specific scheme to help your family join you in the UK. They may be eligible to make an immigration application directly to the Home Office to join you. Further details can be found here.

One of my family member's data was breached and now I think I am at risk. Can I still apply for ARAP?

The UK government closed the ARAP scheme for new applications on 1 July 2025. It is no longer possible to submit an ARAP application and there is no access to the online form.

Please note, the closure of the ARAP scheme does not apply to people with *existing* applications. All existing applications and review requests will still be considered.

Also, if you did not previously apply for ARAP but your relative did and you were included as a family member, it may be possible to request an out-of-time review of any decision that you are not eligible for assistance under the scheme.

Are there any pathways left for Afghans to come to the UK?

On 1 July 2025 the ARAP scheme closed for new applicants and the ACRS schemes closed for new referrals. There are now no specific schemes available for Afghans to come to the UK.

I feel very stressed about my family members in Afghanistan, what can I do?

The news about the data breach is very distressing. It is understandable to feel upset, confused, worried or stressed. Please seek mental health support if it would assist. You may find helpful support here (for those in the UK) or here (for those in Afghanistan or the region).