

Privacy notice for processing personal data during National Security Vetting (NSV)

This privacy notice applies when the vetting provider is United Kingdom Security Vetting (UKSV). UKSV is part of the Ministry of Defence. If you are unsure as to the identity of your vetting provider, please ask your sponsor, which is normally the employer. This notice explains how we intend to store and handle your personal data and that of third parties in the course of conducting NSV. This notice may be updated from time to time – the latest version will be available on .gov.uk.

This notice applies in relation to all previous and current NSV applications processed by UKSV or its predecessors (Defence Business Services and FCO Services) and should be read in conjunction with the [NSV forms](#) and the document '[Personnel Security Controls](#)', also available on .gov.uk.

1. The identity of the NSV data controllers and contact details

UKSV is responsible for carrying out NSV and, for some of its customers, also makes the clearance decision. In these circumstances, with the exception of the Security Service, it is the sole data controller for the NSV process. As UKSV is part of the Ministry of Defence, the Data Protection Officer (DPO) responsible for NSV can be contacted via the MOD Chief Information Officer at CIO-DPA@mod.uk.

When UKSV carries out NSV, but the decision on whether to grant security clearance is taken by the sponsor (which is normally the public authority employer), the sponsor organisation is a joint data controller with UKSV. In these circumstances, if you wish to exercise your rights under data protection legislation, you can contact either UKSV's Data Protection Officer (DPO) or their counterpart in the sponsor organisation that decides whether you will be granted security clearance. It is the sponsor's responsibility to advise you of their DPO's contact details.

In addition to UKSV and the sponsor organisation, the Security Service is a data controller for NSV in respect of the check of Security Service records. The Security Service publishes advice on access to information at <https://www.mi5.gov.uk/access-to-information>. It can be contacted via:

The Enquiries Desk
PO Box 3255
London SW1P 1AE

Should you be granted clearance and subsequently move to another post requiring NSV at a different organisation, the relevant personnel security risk owner for the new organisation may review your clearance against the particular security risks that organisation faces. In such circumstances, the new organisation replaces the initial sponsor organisation as a joint data controller for NSV.

2. Why we will process your data

We will process your personal data and that of third parties for the purpose of carrying out NSV, including aftercare. NSV is necessary and proportionate to safeguard the UK's national security. We may also process your data for ancillary purposes, for example, to facilitate an appeal to the Security and Vetting Appeals Panel, to fulfil legal and regulatory requirements or, in an anonymised way for business monitoring and planning purposes.

3. The legal basis for the processing

UKSV and the sponsor organisation process your personal data and that of third parties in accordance with the General Data Protection Regulation, as applied by Chapter 3 of Part 2 of the Data Protection Act 2018 ('the Applied GDPR'). The Security Service will process your personal data in accordance with Part 4 of the Data Protection Act 2018 (intelligence services processing).

The processing of your personal data and that of third parties is necessary for the purpose of NSV, which is carried out for reasons of substantial public interest and in the exercise of official authority vested in the data controllers. Conducting NSV is a function of UKSV, which is part of the Ministry of Defence, a government department.

4. How your data will be processed

Your personal data and that of third parties will be processed as described in the 'Statement of HM Government Personnel Security and National Security Vetting Policy', which is included in the vetting forms and as an annex to

the document '[Personnel Security Controls](#)' available on .gov.uk. The categories of personal data which we process are described in those documents.

5. Who we share your data with

Personal data that we collect and process for NSV is very strictly controlled and protected by a high level of physical, cyber and personnel security measures. Your NSV personal data is kept separate from other personal data and access is only provided for the purpose of NSV and to those with a strict 'need to know', such as your UKSV vetting officer.

Conducting NSV

To conduct the various checks that form part of NSV, it may be necessary to share some of your personal data with the relevant check provider so that they may provide further personal data to us. We only share the minimum amount of personal data necessary to enable the provider to perform the check. In most cases this is limited to basic identifying information (such as your name or date of birth) to ensure that the provider performs the check on the correct individual.

To perform the component NSV checks and reach a security clearance decision, UKSV may share some of your data with:

- Your employing department or company (to request access to relevant personnel records)
- Public authorities which maintain criminal records databases
- The Security Service
- Credit reference agencies
- Referees (e.g. supervisors, character and academic referees)
- The personnel security risk owner (to enable them to make a decision on your suitability to hold security clearance or so that they can specify any risk mitigation measures conditional for your clearance).

Third party personal data may be processed as a result of these checks. For example, this might be provided to UKSV by a referee.

We may also notify your sponsor or employer whether your clearance has been granted, refused or withdrawn.

Risk mitigation

On rare occasions where a security risk has been identified, UKSV or the sponsor department may consider that it is possible to mitigate that risk to an acceptable level by sharing relevant information with someone within your line management chain. Should this apply to you, we will not share your personal data without discussing this with you first and obtaining your explicit consent. If we seek to do this we will give you further explanation of the reasons why and purpose and also explain your rights with regard to providing and withdrawing consent.

If you are worried about the confidentiality of the NSV process, please contact your sponsor for advice.

Public interest matters

Very exceptionally, data supplied by you or by a third party may be sufficiently serious that the NSV data controllers may consider it is necessary and in the public interest to share relevant information with an appropriate authority, such as the police. This might occur when information suggests that:

- you may have committed a previously undetected criminal offence, or that an offence may be about to be committed,
- you or others may be at risk of harm,
- action is required to safeguard national security.

Appeal

If your clearance is refused or withdrawn and you decide to appeal to the Security Vetting Appeals Panel, we will provide the Panel with relevant personal data to enable them to consider your appeal.

6. How long we will keep your personal data

Your personal data and that of third parties will be retained for so long as is necessary for the purpose for which it was collected (safeguarding national security). Personal data collected during the NSV process will normally be

retained by UKSV and the sponsor organisation for six years from the date that your security clearance expires, lapses or is withdrawn. However, it may be necessary to retain some personal data beyond this period in the interests of national security or to defend legal proceedings which have already commenced.

7. Your data rights

You have considerable say over what happens to your personal data. Your rights and how you may exercise them are fully detailed on the ICO website. In relation to your personal data held by UKSV or the sponsor organisation, unless an exemption applies, you have the right:

- a. to request a copy your personal data
- b. to require us to restrict the processing of your data in certain circumstances
- c. to request your data be deleted or corrected
- d. to object to the processing of your data
- e. to lodge a complaint with the independent Information Commissioner's Office (ICO) if you think we are not handling your data fairly or in accordance with the law. You can contact the ICO at <https://ico.org.uk/concerns>, or telephone 0303 123 1113.

8. International data transfers and international organisations

As described above, for important reasons of public interest and national security, it may be necessary for UKSV to seek information from referees some of whom may be from international organisations, EU member states, or located in countries where the EU Commission has not issued an adequacy decision to confirm that it considers the country provides an adequate level of data protection.

Where the sponsor organisation is an international organisation, for example NATO, or where your clearance is to work for a contractor overseas, we will inform the organisation or contractor whether your clearance is granted, refused or withdrawn.

9. Decisions based on automated processing

NSV decision are not based solely on automated processing, including profiling. The decision whether to grant or refuse security clearance is taken individually by the relevant personnel security risk owner.

10. Failure to provide data

You are required to provide the personal data requested as part of NSV in order to obtain the security clearance necessary for your role, which will be either a contractual requirement or necessary for your employment with the sponsor organisation. If you do not provide the requested data, we will be unable to grant you security clearance and this may impact on your employment.

11. Complaints

If you are not satisfied with the way in which your personal data is being processed by UKSV:

You can make a complaint to the Ministry of Defence Information Rights Team:

MOD Information Rights Team
Ground floor, zone D
Main Building
Whitehall
London SW1A 2HB
Email: cio-dpa@mod.uk

The team will acknowledge your complaint within 5 working days and endeavour to send you a full response within 20 working days. If the team is unable to respond fully in this time, the team will explain why and let you know when you should get a full response.

If you are not satisfied with the response, you have the right to take your complaint to the Information Commissioner's Office: <https://ico.org.uk/concerns/>; telephone: 0303 123 1113.