

## Privacy notice for processing personal data during National Security Vetting

### (NSV) 1. Definitions

- 1.1. **DPA 2018:** Data Protection Act 2018 (as amended).
- 1.2. **UK GDPR:** The UK General Data Protection Regulation (as amended).
- 1.3. **Sponsor Organisations:** government departments and agencies, the Armed Forces, Police forces and any other organisation that requires NSV Services either directly from UKSV or via the relevant Cluster Security Unit. For the purposes of this Privacy Notice, a Cluster Security Unit is considered a Sponsor Organisation when it is responsible for a government department's NSV.
- 1.4. **Sponsored Individual(s):** individual(s) for whom the Sponsor Organisation requires NSV.
- 1.5. **Third Party:** other than in paragraph 10, individual(s) connected to the Sponsored Individual such as: current or former spouse or partner, parent, parent-in-law, family member, cohabitant, character referee, supervisor or ex-supervisor.
- 1.6. **NSV Services:** security clearance and related services, including but not limited to: annual security appraisals; enquiries scheduled during security clearance to monitor identified risk factors; unscheduled enquiries necessitated during the life of a clearance by an unforeseen event such as a change of circumstances or a report of security concerns regarding a clearance holder (an "Aftercare Incident Report"); and other clearances or related authorisations.

### 2. Introduction

- 2.1. This Privacy Notice applies to the processing of personal data by UKSV when providing NSV Services. UKSV is part of the Cabinet Office. If unsure as to the identity of a vetting provider, please ask the Sponsor Organisation, which is normally the Sponsored Individual's employer.
- 2.2. NSV is designed to protect against threats from hostile intelligence services, terrorist groups, organised criminals and other threat actors. NSV allows decisions to be made as to whether an individual can be trusted with sensitive assets (personnel, physical, information).
- 2.3. This Privacy Notice does not cover personal data processed as part of Accreditation Checks, a level of NSV established for individuals employed in posts which require an Airport Identification Card or UK air carrier Crew Identification Card which provides unescorted access in the security restricted area of UK airports. For privacy information on these checks, individuals should look at the Privacy Notices of their (prospective) employee and on the Civil Aviation Authority's [website](#).

### 3. The identity of the NSV data controllers

- 3.1. UKSV is responsible for carrying out NSV Services in respect of Sponsored Individuals when requested by a Sponsor Organisation.
- 3.2. For some of its Sponsor Organisations, UKSV is given delegated authority to make the clearance decision.
- 3.3. Where UKSV undertakes NSV Services, UKSV and the Sponsor Organisation are joint data controllers of personal data which is processed by UKSV when providing NSV

Services. UKSV is a joint data controller of such personal data from the point it receives an application from a Sponsor Organisation for NSV services until the time UKSV deletes or destroys that data from its systems.

- 3.4. The Sponsor Organisation and not UKSV is an independent data controller from UKSV of any personal data:
  - 3.4.1. which is processed by the Sponsor Organisation prior to receipt of any application or request for the provision of NSV Services;
  - 3.4.2. which is processed by the Sponsor Organisation for any purpose other than in respect of NSV Services;
  - 3.4.3. which is extracted by the Sponsor Organisation from the National Security Vetting System (NSVS); and/or
  - 3.4.4. which is contained in paper format and provided to the Sponsor Organisation by UKSV, save that UKSV will also be a data controller in respect of its own copies of such records.
- 3.5. Where UKSV and the Sponsor Organisation are joint data controllers, you can exercise your rights by contacting either organisation. UKSV's contact details are set out at the end of this Privacy Notice. The Sponsor Organisation should provide you with their contact details.
- 3.6. In addition to UKSV and the Sponsor Organisation, the Security Service is an independent data controller for NSV in respect of checks of Security Service records undertaken as part of the NSV process. UKSV does not have access to the Security Service's data or systems, but the Security Service may provide data that it considers relevant. The Security Service publishes advice on access to information [here](#). It can be contacted via The Enquiries Desk, PO Box 3255, London, SW1P 1AE.
- 3.7. Where other clearances or authorisations are sought by a relevant government department, that department may access personal data processed by UKSV. In such circumstances, UKSV and the relevant government department are joint data controllers in respect of that data which is accessed by the government department unless otherwise agreed. The relevant government department is an independent data controller from UKSV in respect of any personal data:
  - 3.7.1. which is processed by the relevant government department prior to accessing any personal data held by UKSV;
  - 3.7.2. which is processed by the relevant government department for any purpose other than in respect of NSV Services;
  - 3.7.3. which is extracted by the government department from the NSVS; and/or
  - 3.7.4. which is contained in paper format and provided to the government department by UKSV, save that UKSV will also be a data controller in respect of its own copies of such records.
- 3.8. Should security clearance be granted, but the Sponsored Individual move to another post requiring NSV at a different organisation, the relevant personnel security risk owner for the new organisation may review the clearance against the particular security risks that organisation faces and personal data relating to the Sponsored Individual will be transferred to the new organisation. In such circumstances, the new organisation replaces the initial Sponsor Organisation as a joint data controller for NSV. In these

circumstances the new Sponsor Organisation may decide to undertake additional NSV enquiries or revoke security clearance based on their particular security risk considerations.

- 3.9. Where organisations opt to share the Sponsored Individual's security clearance, the existing Sponsor Organisation, the new Sponsor Organisation and UKSV are all joint data controllers for NSV for the period the clearance is shared.

#### **4. Why we process your data**

- 4.1. We process personal data of Sponsored Individuals and Third Parties in order to provide NSV Services.
- 4.2. Personal data acquired for the provision of NSV Services may also be processed to fulfil legal and/or regulatory requirements, or in an anonymised manner for business monitoring and planning purposes. The data may also be processed as part of the maintenance, monitoring and development of IT systems to ensure the secure and effective protection of the data at all times.

#### **5. The data we process**

- 5.1. The nature of the personal data we process and the extent of processing will depend on the type of NSV Services which UKSV provides. The processing may include special category or criminal offence data.
- 5.2. In order to conduct NSV checks, UKSV will collect the following data on a Sponsored Individual: your name, date of birth, sex or gender identity, nationality and place of birth, changes to nationality or citizenship, contact details, national insurance number, passport number, employment references, evidence of right to work in the UK, reasons for name changes, current and former relationship status, current and former addresses, details of your cohabitants, details about your current and former employment, unemployment or military service, details of education, qualifications or licences, details of time spent overseas, data about any spent or unspent criminal offences committed, information about your health including your GP or other health practitioner details, information about any substance or alcohol abuse, information about any financial difficulties, details of any previous clearances held and information obtained about you from the security services.
- 5.3. Depending on the level of clearance you are applying for, UKSV might need to collect additional personal data, this may include information about your political views, your religious views, your sexuality and sexual behaviour, your conduct during education and employment, information about your finances e.g. credit reference checks, your use of the internet and social media, and/or information about your foreign travel and connections and your associations.
- 5.4. We may also collect data on Third Parties and children connected to a Sponsored Individual. Further detail can be found in sections 6 and 7.
- 5.5. We may also approach Third Parties to ask for details on how well they know the Sponsored Individual, including how long they have known them and how often they are in contact with them. This information might include the personal data listed in paragraph 5.2.
- 5.6. We may collect your personal data if you contact the Help Desk depending on the nature of your enquiry, details on how long we keep the data can be seen in section 11.

## 6. Third Party Data

- 6.1. In the course of NSV, personal data belonging to Third Parties may be collected.
- 6.2. Third Party data is processed for the same purpose and on the same legal basis as the Sponsored Individual's personal data. If you are a Third Party that might be affected, you should review this privacy notice in its entirety to understand how and why your data is processed. You have the same rights as Sponsored Individuals. See section 16 for more detail on what these are and how to act on them.
- 6.3. Third Party personal data is collected via the Sponsored Individual or in the course of NSV. What is collected might depend on your connection to the Sponsored Individual. The table below provides more detail on the personal data UKSV might collect on a Third Party in the course of NSV.
- 6.4. As detailed in 3.6 above for the Sponsored Individual, the Security Service may provide data that it considers relevant in relation to Third Parties.

Third Party	Categories of personal data held
Sponsored Individual's partner or former partner(s) up to three years	Name and/or initials; gender; reasons for any change of name - surname and forename; date, place and country of birth; occupation; date of adoption; nationality (current and previous); citizenships (current and previous); marital/divorce status; home address (including former addresses); history of criminal offence allegations, convictions or proceedings; links to terrorism, activism, subversion, espionage, organised crime.
Sponsored Individual's parents/siblings/wider family	Name and/or initials; gender; reasons for any change of name - surname and forename; date, place or country of birth; occupation; date of adoption; nationality (current and previous); citizenships (current and previous); marital/divorce status; home address (including former addresses); history of criminal offence, convictions or proceedings; links to terrorism, activism, subversion, espionage, organised crime.
Co-residents	Name and/or initials (including former names); age or date of birth; address; present nationality; occupation; links to terrorism, activism, subversion, espionage, organised crime.
Character referee	Name and/or initials; age or date of birth; home and work telephone number; home and work address; home and work email address.
Education referee	Name and/or initials; age or date of birth; home and work telephone number; home and work address; home and work email address.

Supervisor referee	Name and/or initials; age or date of birth; home and work telephone number; home and work address; home and work email address.
Sponsor	Name and/or initials; work telephone number and email address; role; work address.

## 7. Children's data

7.1. UKSV uses children's personal data to help support the Sponsored Individual's (the person undergoing security clearance) application for security clearance. UKSV collects the following information on children;

7.1.1. the child's full name and reasons for any change of name,

7.1.2. their age,

7.1.3. current school or training,

7.1.4. nationality (current and previous), citizenships (current and previous) and country of birth,

7.1.5. their home address,

7.1.6. where needed, information on if the child has been in trouble with the police or been to court,

7.1.7. UKSV also collects information on whether the child has or has previously had any links to terrorism, and crimes which cause harm.

7.2. Children have the same rights over their data as an adult and this is covered in section 16 of this document. Children's data is secured in the same way as an adult's data on our secure IT system. It is processed under the same legal basis and for the same purpose. The child's personal data is only shared with the organisation who makes a decision on the application (usually the Sponsor Organisation).

## 8. The legal basis for processing

8.1. UKSV and the Sponsor Organisation process all personal data in accordance with the UK GDPR and the DPA 2018.

8.2. The primary legal basis for processing personal data for the provision of NSV Services is that it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller (Article 6(1)(e) UK GDPR and section 8 of the DPA 2018). Personal data may also be processed in accordance with Article 6(1)(a) or (c) of the UK GDPR, where consent is obtained or it is necessary for compliance with a legal obligation to which the data controller is subject. Special category data and/or criminal offence data will also be processed in accordance with one or more of the following conditions:

8.2.1. paragraph 6 of Schedule 1 of the DPA 2018 (processing necessary for reasons of substantial public interest, in the exercise of a function of a government

department (UKSV is part of the Cabinet Office)); and/or

8.2.2. paragraph 11 of Schedule 1 of the DPA 2018 (processing is necessary for the exercise of a protective function and is necessary for reasons of substantial public interest).

8.3. In some instances, UKSV may request information on your medical records or relating to your gender identity history. If so, UKSV will seek your consent as required under the relevant legal regimes. Any personal data obtained as a result will be processed in accordance with the legal basis set out at 8.2.

8.4. Calls to the UKSV Help Desk will be recorded for training and quality purposes. Recording of calls is done under UK GDPR Article 6(f) legitimate interests, you can opt out of recording by notifying the Helpdesk agent as stated in the Interactive Voice Response message at the start of the call.

## **9. How personal data is processed**

9.1. We use personal data to inform decision making in relation to the provision of NSV Services. This includes checking it against relevant personnel records held by the Sponsor Organisation, criminal records (both spent and unspent as defined by the Rehabilitation of Offenders Act 1974), credit worthiness records and information held by the Security Service. The process also takes into account financial circumstances generally, character references and any medical considerations that could give rise to security concerns. More detail can be found in Annex A, paragraphs 1-14 of the Statement of HM Government Personnel Security and National Security Vetting Policy available [here](#).

## **10. Who we share personal data with**

10.1. Personal data that we collect and process for NSV Services is strictly controlled and protected by proper and appropriate security measures. Personal data processed in connection with NSV Services is kept separate from other personal data. It is only shared with third parties where this is necessary and proportionate as follows:

10.1.1. To provide NSV Services, UKSV will need to share personal data with the relevant check providers so that they may provide further personal data to us. We only share the minimum amount of data necessary to enable the provider to perform the check. To provide NSV Services, UKSV may share your data with:

a) A Sponsor Organisation (e.g. to request access to relevant personnel records).

b) Public authorities which maintain criminal records databases.

c) The Security Service.

d) Credit reference agencies. UKSV currently uses Experian whose Privacy Policy is available [here](#) but may use other agencies.

e) Character, education and employment referees.

f) Personnel security risk owners (e.g. to enable them to make a decision on your suitability to hold security clearance, so that they can specify any risk mitigation measures conditional for your clearance, to notify them that clearance has been granted or refused, or where

an existing clearance has been withdrawn or revoked).

g) A government department carrying out any other clearances or related authorisations.

h) Our IT providers who provide our platforms that hold vetting data.

i) Secure email suppliers that provide a platform to share official information.

ii) Customer Relationship Management tool and telephony system provider

10.1.2. In exceptional circumstances where a security risk has been identified, UKSV or the Sponsor Organisation may consider that it is possible to mitigate that risk to an acceptable level by sharing relevant information with an appropriate person or appropriate managers for a Sponsored Individual. Should this be the case, personal data will not be shared without notifying the data subject in advance of such disclosure.

10.1.3. In exceptional circumstances, information containing personal data may be sufficiently serious that UKSV may consider it necessary to share relevant information with a third party, such as the police, without consent and for purposes which are not related to NSV. This might occur, for example, when information suggests that an individual may have committed a previously undetected criminal offence of a sufficiently serious nature, that an offence may be about to be committed, that individuals may be at risk of harm, and/or that action is required to safeguard national security.

10.1.4. If security clearance is refused or withdrawn and an appeal is brought against that decision, we will need to provide the relevant authority considering the appeal with relevant personal data to enable them to conduct the appeal.

## **11. How long we keep personal data**

11.1. Personal data which we collect when providing NSV Services will be retained for so long as is necessary for the purpose for which it was collected (i.e. safeguarding national security).

11.2. Notes from a security clearance interview will be transferred into a record of interview and transferred onto the Sponsored Individual's file on NSVS. Hard copy and electronic notes will normally be destroyed once transferred and within 30 days of the date of the interview. Where security concerns are noted, the interview notes will be retained by UKSV for at least two months from the date of the interview and will be destroyed once a decision on security clearance has been reached. Where security clearance is refused, UKSV retains the interview notes until the application has been completed.

11.3. All other personal data obtained by UKSV when providing NSV services will be retained by UKSV and the Sponsor Organisation for fifteen years from the date that security clearance is last used, refused, expires, is withdrawn or revoked. However, in exceptional circumstances it may be necessary to retain personal data beyond this period, such as in the interests of national security or to defend legal proceedings which are reasonably in prospect or which have already commenced.

11.4. Where personal data has been captured in the course of correspondence with the Help Desk, it will be kept as follows:

11.4.1. Telephone calls that are recorded will be retained for a period of 130 days, then deleted.

11.4.2. Correspondence in our Customer Relationship Management tool will be deleted when there has been no corresponding activity on the enquiry/case for 3 months.

## **12. Failure to provide data**

12.1. Sponsored Individuals are required to provide personal data requested as part of NSV in order to obtain the requisite clearance for a role, which may be either a contractual requirement or mandatory for employment with the relevant organisation. If the requested personal data is not provided, UKSV and the Sponsor Organisation may be unable to assess and grant security clearance, which may impact on the Sponsored Individual's employment.

## **13. Where you did not provide your personal data**

13.1. Where personal data was not provided by you, it is provided by an employer, a Sponsored Individual, medical professionals (with your consent), or by a Third Party described above in sections 6 or 10.

## **14. Decision based on automated processing**

14.1. NSV decisions are never based solely on automated processing.

## **15. International data transfers and international organisations**

15.1. It may be necessary for UKSV to seek information from referees. As part of that process, it may be necessary for UKSV to share information with those referees in order to obtain the required information. Some of those referees may be from international organisations, EU member states, or located in countries where the UK has not issued an adequacy decision to confirm that it considers the country provides an adequate level of data protection. Where no other appropriate safeguards are in place, the basis for transferring the data is that it is for important reasons of public interest and national security (Article 49(1)(d) of the UK GDPR).

15.2. 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 or refused, or has been withdrawn or revoked. In the event that there is an information sharing agreement with the party in question, this will be communicated to you as part of your clearance process.

15.3. As your personal data is stored on our IT infrastructure, and shared with our data processors, in limited circumstances it may be transferred and stored securely outside the UK. Where that is the case, it will be subject to equivalent legal protection through an adequacy decision or appropriate safeguards.

## **16. Your data rights and complaints**

16.1. If we process your personal data, you have rights in respect of that data which you may choose to exercise. Your rights and how you may exercise them are fully detailed on the independent [Information Commissioner's Office website](#).

16.2. These rights include:



- 16.2.1. the right to request a copy of your personal data;
  - 16.2.2. the right to require us to restrict the processing of your data in certain circumstances;
  - 16.2.3. the right to request your data be deleted or corrected;
  - 16.2.4. the right to object to the processing of your data; and
  - 16.2.5. the right to lodge a complaint with the independent Information Commissioner's Office (ICO) if you think we are not handling your personal data in accordance with the law.
- 16.3. The exercise of these rights may be subject to certain limitations or exemptions, including (but not limited to) where an exemption is required for national security or where processing is necessary for the prevention and/or detection of crime.
- 16.4. If you have provided UKSV with your consent for it to obtain your medical data from a medical professional, you have the right to withdraw consent to the processing of that data. This may affect the ability for UKSV to grant or renew your security clearance.
- 16.5. If you wish to exercise any of these rights, or complain about how we are processing your personal data, please write to UKSV Data Protection Team, Imphal Barracks, York YO10 4AS or email [UKSV-data.protection@cabinetoffice.gov.uk](mailto:UKSV-data.protection@cabinetoffice.gov.uk). We will acknowledge your complaint within 5 working days and provide you with a substantive response within one month of receipt of the request, except where a longer period may be necessary. If a longer period is necessary, we will write to you within one month of your request informing you of when you can expect a substantive response and the reasons for the delay.
- 16.6. UKSV's Data Protection Officer is Steve Jones. They can be contacted at [dpo@cabinetoffice.gov.uk](mailto:dpo@cabinetoffice.gov.uk). The Data Protection Officer provides independent advice and monitoring of UKSV's use of personal information.
- 16.7. If you are not satisfied with the response, you have the right to lodge a complaint with the Information Commissioner's Office if you think we are not handling your data or your request in accordance with the law. You can contact the ICO by calling 0303 123 1113 or by using their online form available at <https://ico.org.uk/make-a-complaint/your-personal-information-concerns/>.

**July 2023**