Disclosure and Barring Service
Countersignatory Privacy Policy

1. About us

1.1. The Disclosure and Barring Service (DBS) helps employers make safer recruitment decisions and prevent unsuitable people from working with vulnerable groups, including children.

1.2. A countersignatory is a person within a Registered Body. They are registered with the DBS to countersign applications, in accordance with Conditions of Registration and the DBS Code of Practice.

1.3. A lead countersignatory is a senior figure within a Registered Body. They are registered with the DBS to countersign applications and will also oversee the DBS process within their organisation.

All Registered Bodies must have a lead countersignatory.

1.4. The content of this Privacy Policy applies to both countersignatories and lead countersignatories, unless otherwise stated.

2. What is it I need to know?

2.1. This is our Countersignatory Privacy Policy. It tells you how we will use and protect any information we hold about you as part of your countersignatory application.

2.2. The Policy also explains what your rights are as countersignatory under the General Data Protection Regulation. It says why we need your personal data, what we will do with it and what you can expect from us. It also explains how to get a copy of any personal data we may hold about you. This is called a Subject Access Request.

2.3. We do have other Privacy Policies that cover our other statutory functions. They can be accessed here.

3. How will we use the personal information supplied to us?

3.1. We, at the DBS, collect your personal data in order to:

- verify your identity (this applies to lead countersignatories only – see section 3.2)
- assess whether you are suitable to be a countersignatory (see section 3.3)
- contact you regarding consideration or changes to your countersignatory application and/or registration status
- contact you in relation to further information that may be required on any applications you have countersigned (to either progress the application or as part of the compliance process)
- contact you regarding any changes you need to be aware of relating to DBS services and products

3.2. **Verify your identity (lead countersignatories only)**

The list of accepted documents to verify the identity of a signatory can be found here.

On receipt of a lead countersignatory application, the identity documents will be used to verify the identity of the applicant against the information provided on their application. This will be done on either the Registration Application Form or a 'Change of Lead Signatory' Form.

DBS recommends that identity documents should be sent by Special or recorded delivery as only original ID documentation can be accepted.

If any of the supporting documents of identification fail to meet the requirements for authentication, the application will be rejected and the documents will be returned to the applying lead signatory.

If however the documents fail any of the document checking procedures, they will be treated as a suspicious document and referred for further investigation.

Where documents have passed authentication they are scanned onto DBS computer files. The original documents are then placed in envelopes to return to the sender on the same day; they will be sent to either the address provided or to the address recorded on DBS computer files. This is done via recorded delivery unless specifically requested otherwise.

3.3. **Assessing countersignatory suitability**

Countersignatories will have access to personal and sensitive information - for this reason, those applying for countersignatory status are checked by the DBS to the level of an enhanced check with both barred lists. This allows the DBS to assess whether they are suitable to carry out this role.

The DBS Registration Team is responsible for determining if a countersignatory is suitable. Generally, the DBS considers that offences of dishonesty, extortion, serious sexual/violent offences and non-minor drug offences could in principle, have an impact on a person's suitability. This is dependent on the circumstances of the relevant offence and how long ago it occurred. Each case will be considered on its own merits. In considering each case, the following factors will be taken into account:

- the nature of the offences and their relevance to the functions
- the seriousness of the offences
- the number of offences
- the date that the offences occurred
- the circumstances surrounding the offending
- whether the offence was isolated or a pattern
- any other mitigating circumstances and/or factors that are considered relevant to suitability

However, where the applying countersignatory is on either of the children's or adults' barred lists, they would not be considered suitable to countersign applications for standard or enhanced level disclosures.

3.4. Your information may also be used for testing purposes. Testing is undertaken to ensure that our systems function as per specified requirements. If it is not practical to

disguise your data or use dummy data then we will test our system using your data. This testing will only take place in environments that are secured to the same level as our live system.

Please note we may use previous applications you have submitted to assist in the checking process.

4. Who is the data controller?

4.1. A data controller decides the purpose for which, and the manner in which, any personal data is processed.

4.2. The DBS is the data controller of information held by us for the purposes of GDPR. We are responsible for the safety and security of all the data we hold.

5. Who are the data processors?

5.1. A data processor is anyone (other than an employee of a data controller) who processes that data on behalf of the controller.

5.2. At the DBS we have a range of suppliers who process data on behalf of DBS as defined in section 9. We make sure that our data processors comply with all relevant requirements under data protection legislation. This is defined in our contractual arrangements with them.

6. Contacting the Data Protection Officer

1.1. The DBS Data Protection Officer Elaine Carlyle can be contacted via telephone on **0151 676 1154,** via email at **dbsdataprotection@dbs.gov.**uk, or in writing to:

Elaine Carlyle
DBS Data Protection Officer
Disclosure and Barring Service
PO Box 165
Liverpool
L69 3JD

7. What are the legal grounds for processing my information?

7.1. DBS was established under the Protection of Freedoms Act (PoFA) 2012 on 1 December 2012. Disclosure functions of DBS are contained within Part V of the Police Act (PA) 1997.

7.2. DBS relies on Section 120 of the PA to carry out suitability checks to determine if an individual can have countersignatory status. Section 120A of the PA makes clear which information we can consider in making that decision.

8. Why would DBS hold my personal data?

8.1. We will only hold your data if you have:

- previously applied to be a countersignatory

- previously used or are using the Disclosure Service
- been referred to the DBS for consideration under the Safeguarding Vulnerable Groups Act 2006 (SVGA)/Safeguarding Vulnerable Groups (Northern Ireland) Order 2007
- been cautioned or convicted for a relevant (automatic barring) offence that leads to the DBS considering you for inclusion on one or both lists.

8.2. If we ask you for personal information, we will:

- make sure you know why we need this information
- only ask for information that we need
- ensure only those appropriate have access to it
- store your information securely
- inform you if the information will be shared with a third party
- ask you to agree to us sharing your information where you have a choice
- only keep your information for as long as we need to – see our Retention Policy
- not make it available for commercial use (such as marketing) without your permission
- ensure you are provided with a copy of data we hold on you, on request – this is called a Subject Access Request
- ensure there are procedures in place for dealing promptly with any disputes or complaints

Please note: We will share information with 'relevant authorities' such as the police, government departments etc. under UK Data Protection Act Prevention and Detection of Crime (Sch2, Part 1 Paragraph 2).

We will also share information under UK Data Protection Act (Sch2 Part 2 Paragraph 5 (2)) where disclosures are required by law or made in connection with legal proceedings.

8.3. In return we ask you to:

- give us accurate information
- tell us as soon as possible if there are any changes to your details, such as a new address

8.4. This helps us to keep your information reliable, up to date and secure. It will apply if we hold your data on paper or in electronic form.

This is a requirement for Registered Bodies under the conditions of registrations in section 7(j) of the previously mentioned Police Act under point 7.2 and in the Code of Practice.

9. Organisations that are involved in the Countersignatory Application Process

9.1. Data will be passed to organisations and data sources involved with the DBS where it is legally permitted to do so. This includes:

- Tata Consultancy Services (TCS) including their third party suppliers – a partner and data processor in the DBS service
- Police forces in England, Wales, Scotland, Northern Ireland, the Isle of Man, and the Channel Islands – searches will be made on the PNC and data may be passed to local police forces. The data will be used to update any personal data the police currently hold about you
- ACRO Criminal Records Office - manages criminal record information and improves the exchange of criminal records and biometric information
- Other data sources such as British Transport Police, the Service Police and the Ministry of Defence Police - searches are made using an internal database. Where a match occurs the information will be shared to ensure that the record match is you
- Disclosure Scotland – if you have spent any time in Scotland, your details may be referred to Disclosure Scotland
- Garda - if information held by Police Service Northern Ireland (PSNI) indicates some information exists in the Republic of Ireland your details may be referred to Garda
- Access Northern Ireland – if you have spent any time in Northern Ireland your details may be referred to Access Northern Ireland
- Independent monitor (IM) - to undertake reviews on local intelligence (approved information) released by local police forces
- Independent Complaints Reviewer (ICR) - part of their role to investigate complaints that have gone through internal review process
- United Kingdom Central Authority - for exchange of criminal records with other EU countries
- The Child Exploitation Online Protection Centre (CEOP) who are National Crime Agency (NCA) Command
- Registered Bodies – the bodies registered with the DBS to submit Disclosure checks
- DXC Technology - our provider for cloud storage
- ATOS - for the collection of e-bulk application data
- National Identity Services (NIS) – assisting in the uploading of old criminal records from Micro Fiche to the Police National Computer (PNC)

10. Where is my data stored?

10.1. Your data is held in secure paper and computer files. These have restricted access. Where your data is held in paper format we have secure storage and processes for this. In some cases we may use secure offsite storage. We have approved measures in place to stop unlawful access and disclosure. All our IT systems are subject to formal accreditation in line with Her Majesty Government (HMG) policy. They also comply with the security required within Article 5 of GDPR in ensuring that personal data is processed in a manner that ensures that appropriate security of the data including protection against unauthorised or unlawful processing.

11. How long will DBS hold my information?

11.1 We operate a Data Retention Policy to ensure that data is not held for longer than necessary. However at present, there is a restriction on the destruction of information due to the ongoing Independent Inquiry into Child Sexual Abuse. DBS are currently reassessing the retention requirements in light of this.

11.1. Any data that we identity that could be called on by the inquiry will be retained until completion of the inquiry. At this point the information will be securely destroyed as soon as is practicable.

12. What are my rights? How will DBS protect them?

12.1. We are committed to protecting your rights under the GDPR**.**

12.1.1. Your right to be informed

This document provides you with information in relation to how your data is processed as a DBS applicant. This ensures that we are transparent with you as an applicant with regards to what we will do with the information you supply to us on your countersignatory application.

12.1.2. Your right to access to your personal data held by DBS - known as a Subject Access Request

You have the right to request a copy of the information we hold about you.

On receipt of a valid application we will tell you whether we hold any data about you and provide you with a copy. Further information on how to apply can be found here.

12.1.3. Your right to request information held is accurate. Can I update it?

If you think that the information held by us at the DBS is incorrect, you have the right to request it is corrected. If you challenge the accuracy of data that was provided to us by a third party we will send your request for correction to that party for their consideration.

If you believe you have submitted an error when your registration is still in progress you will need to contact us immediately on 03000 200 190.

You will receive a letter advising you if your application to become a countersignatory has been accepted or rejected by the DBS. If we reject your application you can appeal this. Details regarding how to do this will be included in the letter you receive.

If your contact details change you are required to provide these to us. These should be provided in writing to the customer services address found in the Contact DBS section of our GOV.UK page.

12.1.4. Your right to request erasure of your personal data

In certain circumstances you have a right to have personal data held about you erased. At the DBS we will only do this if certain criteria are met. There are some circumstances where this cannot be done therefore we advise you to seek independent advice before submitting an application to us.

Any requests for information to be destroyed will be considered on a case-by-case basis.

There are some specific circumstances where the right to erasure does not apply and we may refuse your request.

12.1.5. Your right to prevent DBS from processing information which is likely to cause you damage or distress

You have the right to request restriction of processing where it has been established that one of the following applies:

- the accuracy of personal data is contested during the period of rectification
- processing is unlawful
- where an individual has requested it is retained to enable them to establish, exercise or defend legal claims
- pending verification of the outcome of the right to object
- where processing has been restricted

DBS customers can request restriction of processing for any of the above reasons until these are resolved. Should you wish to restrict processing you will need to call the DBS helpline on **03000 200 190**. Any requests to stop processing will be considered on a case-by-case basis.

12.1.6. Right to receive an electronic copy of any information you have consented to be supplied to us - known as data portability

You have the right, where it is technically feasible to receive electronically any personal data you have provided to DBS to process, on a consent basis.

Please note that basic, standard and enhanced certificates are processed under Part V of the Police Act 1997 and barring information is processed under the Safeguarding and Vulnerable Groups Act 2006. Therefore this information falls outside of the right to Data Portability.

All requests for portability will be considered on a case-by-case basis.

12.1.7. You have the right to object to processing of your information

Should you wish DBS to stop processing your application you will need to withdraw the application.

You will need to telephone the DBS to request withdrawal, followed with a request in writing

within 14 days. It should be noted that this will need to be done as soon as possible as the countersignatory application process can be completed quite quickly.

The DBS will inform the lead countersignatory, as the person who countersigned the application, that we are not processing the application as you have exercised your right.

You do not have to provide a reason for the withdrawal of the application and we will not provide the reasons you may have given in your request to the lead countersignatory.

12.1.8. **You have rights relating to automated decisions being made about you**

The DBS Registration Team make each suitability decision on a case-by-case basis, based on the content of the enhanced disclosure check. This suitability decision is not automated.

Our disclosure process is generally an automated process, however if the system identifies that 'potentially' there is police information held about you this is then sent to the relevant police force for consideration, regarding information which may be disclosed on your certificate. This is not an automated process and involves the judgment of the Chief Officer.

You have the right to object to any automated decision-making**,** it should be noted that you would need to inform us of this on submission of your application by contacting us on 03000 200 190.

DBS do not currently undertake any profiling activities.

12.1.9. **You have the right to make a complaint to the DBS and the ICO**

If you wish to make a complaint to the DBS regarding the way in which we have processed your personal data you can make a complaint to the Data Protection officer via the contact details in Section 6.1. If you then remain dissatisfied with the response received, you have the right to lodge a complaint to the ICO at the following address:

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

https://ico.org.uk/

13. Transfer outside the European Economic Area

13.1. If you have spent time in the Channel Islands or the Isle of Man, it is likely that your data will be passed to police forces in that area. If any of your data has to be transferred outside of the UK DBS will ensure that an adequate level of protection is put in place.

14. Our staff and systems

14.1. All our staff, suppliers and contractors are security vetted by the Home Office security unit prior to taking up employment. All staff are data protection trained and are aware of their data protection responsibilities and this is refreshed on an annual basis. We conduct regular compliance checks on all DBS departments and systems. All checks

are to the standard set out by the Information Commissioners Office. In addition continual security checks on our IT systems are undertaken.

15. Notification of changes

15.1. If we decide to change our privacy policy, we will add a new version to our website.