Disclosure and Barring Disclosure Service

Online Services and Enquiry Matrix Privacy Policy

1 Introduction

1.1 This is the Privacy Policy for the Disclosure and Barring Service’s (DBS) Online Services and the Enquiry Matrix. It tells you how we will use and protect any information we are required to collect about you where a response will be required.

1.2 This Policy explains your rights as a user of the DBS’ online services and the DBS’ enquiry matrix. There are other DBS Privacy Policies which cover other statutory functions undertaken by DBS. So if you are:

- applying for, responding to or requesting information regarding a basic disclosure certificate using DBS’ online services please read the Basic Disclosure Check Privacy Policy
- responding to or requesting information regarding a standard or enhanced disclosure certificate please read the Standard and Enhanced Disclosure Check Privacy Policy
- responding to or requesting information regarding a referral made to the DBS barring service please read the Barring Privacy Policy

This Policy will cover any other queries submitted using either DBS’ online services or the DBS enquiry matrix. If your query is in regards to cookies, please see the GOV.UK Cookies Policy.

1.3 This Policy tells you why the DBS collects and processes your data in compliance with the General Data Protection Regulation (GDPR).

2 Why DBS collects and uses information

2.1 The DBS collects information from DBS’ online services and/or the enquiry matrix in order for us to answer your query.

2.2 Should your query be relevant to a current or previous disclosure certificate, disclosure application or barring referral, it will be passed to the relevant team(s) for a response and the relevant Privacy Policy from those listed above will apply.

3 Who is the data controller?

3.1 The DBS is the data controller of information held by DBS for the purposes of GDPR. A data controller determines the purposes for which, and the manner in which, any personal data is to be processed (either alone or jointly or in common with others).

3.2 We have the responsibility for the safety and security of all the data we hold.

4 Who are the data processors?

4.1 Any supplier that works on behalf of the DBS is one of our data processors. A data processor is any organisation that processes data on behalf of the DBS. We make sure that our data processors comply with all relevant requirements under data protection legislation. This is defined in the contractual arrangements.

5 Contacting the Data Protection Officer
5.1 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

6 Legal Processing

6.1 By making your enquiry you are consenting to your details, including your name, email address and any supplementary details you have provided, being processed and stored securely on our systems in order for us to provide you with a response.

7 What personal data do we hold?

7.1 The most common reasons that we hold your information, are if you:

- have previously used or are using a Disclosure service to obtain a DBS certificate
- have been referred to DBS for consideration under the Safeguarding Vulnerable Groups Act 2006 (SVGA) / Safeguarding Vulnerable Groups (Northern Ireland) Order 2007
- have been included as a named victim or witness in a barring referral (you will need to tell us the name of the individual referred)
- have been cautioned or convicted for a relevant automatic barring offence that leads to DBS considering you for inclusion in one or both lists
- have previously applied or are in the process of applying to be a lead countersignatory or counter signatory of an organisation registered with the DBS to process standard and enhanced applications
- have previously applied or are in the process of applying to be an accountable officer within a Responsible Organisation set up to submit basic applications
- have been or are an employee of DBS, CRB or ISA
- have been involved in carrying out finance related functions for organisations who use our service
- have been involved in delivering services via a contract

This is not a limited set of circumstances and we will search all our systems and records if required in order to respond to your enquiry.

7.2 In return, we ask you to:

- give us accurate information
- inform us as soon as possible if there are any changes to your details, such as a new address
7.3 This helps us to keep your information reliable, up to date and secure. This will apply whether we hold your data on paper or in electronic form.

8 What you can expect from us
8.1 We aim to respond to your enquiry within 10 working days.
8.2 If you are unhappy with our response to your enquiry you can raise this with our complaints team.

9 Who we will share data with
9.1 As a rule we will not onward share your enquiry unless it concerns a previous or current disclosure application, certificate or barring referral.

For details on who we may share data with for:

- a disclosure application please refer to the Basic Disclosure Check Privacy Policy or the Standard and Enhanced Disclosure Check Privacy Policy
- a barring referral please refer to the Barring Privacy Policy

10 Organisations that are involved in the DBS service
10.1 Data may also be passed to organisations involved with the DBS where it is legally permitted to do so. These are:

- Tata Consultancy Services - including their approved third party suppliers. These are data processors of the DBS service
- DXC technology - our provider for cloud storage
- Police forces in England, Scotland, Wales and Northern Ireland, the Isle of Man and the Channel Islands. Searches will be made on the PNC and data may be passed to relevant local police forces. The data will be used to update the information 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 on an internal database. Where a match occurs the information will be shared to ensure the record match is you
- Disclosure Scotland - if you have spent any time in Scotland, your details may be referred to Disclosure Scotland
- Access Northern Ireland - if you have spent any time living in Northern Ireland your details may be referred to them and DBS consider barring information under SVGO
- 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
United Kingdom Central Authority - for exchange of criminal records with other EU countries. This is under the decision made by the council of The European Union

The Child Exploitation Online Protection Centre (CEOP) who are National Crime Agency (NCA) Command

Independent Monitor (IM) - to undertakes reviews on local intelligence (approved information) released by local police forces on a Disclosure Certificate

Independent Reviewer (IR) - part of their role to investigate complaints that have been through internal review process

10 Other organisations we may share information with

10.1 We will share information with ‘relevant authorities’ such as the police, government departments, etc under GDPR Sch 2 Prt 1 para 2 Crime and taxation. We will also share information under GDPR Sch 2 Prt 2 Para 5 (2) of GDPR where disclosures are required by law or made in connection with legal proceedings.

10.2 We may also share information where you provide your consent for DBS to do so.

11 Storage of data

11.1 Your data, once received, is held in secure paper and computer files with restricted access. We have approved measures in place to stop unlawful access and disclosure. All of our IT systems are subject to formal accreditation inline with HMG policy. They also align with the security required within GDPR to protect against unauthorised or unlawful processing.

12 Retention of data

12.1 We operate a Data Retention Policy to ensure that information is not held for longer than is necessary. For general enquiries where we do not have a disclosure application or barring referral your information will be retained for three months. However if your enquiry is relevant to a disclosure application, certificate or barring referral it will be held on the original system or clerical files for the time determined in our Data Retention Policy, relevant to disclosure applications and barring referrals.

12.2 The Home Office has placed a restriction on the destruction of information due to the ongoing Independent Inquiry into Child Sexual Abuse (IICSA). To comply with DBS’ Data Retention Policy and the restriction, DBS have agreed with the Information Commissioner’s Office (ICO) to mark relevant information i.e. information identified as not relevant for ongoing DBS purposes, for secure destruction and place this information outside of operational control. It will only be supplied to IICSA following a legal request.

12.3 At the conclusion of IICSA and/or lifting of the restriction by Home Office this information will be securely destroyed as soon as is practicable.

13 Your rights and how we protect them

13.1 We are committed to protecting your rights under GDPR and the right to be informed how your data is processed
13.2 Your right to access your personal data held by DBS

13.2.1 You have the right to request a copy of the information DBS hold about you this is known as Subject Access Request. Further information on this process and how to apply can be found here.

13.3 Your right to request information held is accurate and how to update it

13.3.1 If you think that the information held by us is incorrect, you have the right to request it is corrected.

13.3.2 Where the information was provided to DBS by another party this request will be forwarded to the relevant party and you should contact them directly. They will be asked to consider the request to correct the information e.g. if your request relates to an employer statement, strategy minutes or the PNC, the request will be sent to the originating organisation.

13.3.3 A copy of your request for correction will be held on the DBS file.

13.4 Your right to request erasing your personal data – also known as the right to be forgotten

13.4.1 In certain circumstances you have the right to have personal data held about you erased. We will only do this if certain criteria are met and there are some circumstances where this can not be undertaken. You should seek independent advice in this regard.

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

13.5 Your right to prevent processing likely to cause you damage/distress

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

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

13.5.2 Should you wish to invoke this right we would suggest you seek independent advice before submitting your enquiry.

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-
13.6 **Your right regarding rectification or erasure of personal data or restriction of processing**

13.6.1 Any requests regarding rectification, (correction), erasure (right to be forgotten) or restriction of processing will be considered on a case-by-case basis.

13.6.2 The DBS will tell any organisation we have shared data with, the correction / destruction / restriction of processing of your personal information where we have upheld your request.

13.7 **Your right to receive an electronic copy of any information you have consented to be supplied to us - known as data portability**

13.7.1 You have the right, where it is technically feasible to receive electronically any personal data you have provided to DBS if you wish. This will enable you to give this to another organisation.

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

13.8 **Your rights relating to automated decisions being made about you**

13.8.1 You have the right to object to automated processing of your information. With regard to submitting an enquiry either through the enquiry matrix or DBS’ online services, there is no automated decision making in our responses.

13.8.2 You have the right to object to any automated decision making including profiling.

Currently DBS does not undertake any profiling activities.

13.9 **You have the right to make a complaint to the DBS and Information Commissioner (ICO)**

13.9.1 If you wish to make a complaint to us 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 set out in Section 5. If you remain dissatisfied with the response received, you have the right to lodge a complaint to the Supervisory Authority. The Supervisory Authority for the UK is:

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

[https://ico.org.uk/](https://ico.org.uk/)

13.10 **Your right to effective judicial remedy against a controller or processor (GDPR Article 79)**

13.10.1 You have the right to an effective judicial remedy in certain circumstances against us as data controller or our data processor(s). You should seek your own independent legal advice with regard to this right.

13.11 **Your right to appoint representation**

13.11.1 You have the right to appoint a not-for-profit body, organisation or association to act on your behalf where you believe the following rights have not been adhered to:
• the right to lodge a complaint with a Supervisory Authority i.e. ICO
• the right to effective judicial remedy against a Supervisory Authority i.e. ICO
• the right to an effective judicial remedy against a controller or processor

13.11.2 You should seek your own independent legal advice with regard to these rights.

13.12 Compensation for failure to comply (DPA Para 13) / Right to compensation and liability (GDPR Article 82)

13.12.1 You have the right to seek compensation where it is proven we or our data processors have not complied with GDPR unless it is proven that we or our data processors are not in any way responsible for the damage.

13.12.2 You should seek your own independent legal advice with regard to this right.

14 Restrictions

14.1 There are restrictions to the rights of individuals and these are:
• National Security (DPA para 28) / (GDPR Article 23 (1)(a)
• Defence (GDPR Article 23 (1) (b))
• Public security (GDPR Article 23 (1) (c))
• Crime & Taxation (DPA para 29) / (GDPR Article 23 (1) (d))

These restrictions are covered in more detail in the forthcoming Data Protection Bill 2018.

15 Transfer of data outside the European Economic Area

15.1 As a rule your data will not be transferred outside of the EU. If your data needs to be transferred outside of the UK DBS will ensure that an adequate level of protection is in place.

16 Our staff and systems

16.1 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 responsibilities and this is refreshed on an annual basis.

16.2 We conduct regular compliance checks on all DBS departments and systems. In addition continual security checks on our IT systems are undertaken.

17 Notification of changes

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