



Disclosure &
Barring Service

DBS AccessNI Privacy Impact Assessment

DBS_LEGC_0037_DBS Access NI PIA v1.0

Document History

Revision and Approval History

Author Name	Team	Role
Michelle Anderson	Corporate Services	Information Governance

Date	Document Version	Document Revision Description	Document Update By
26/03/2013	0.1	Draft document created	Michelle Anderson
18/04/2013	0.2	Reviewers list updated	Michelle Hamilton
15/05/2013	0.3	Updated following review	Michelle Anderson
16/05/2013	0.3	Document approved and baselined	Michelle Anderson

Reviewed Version	Name	Role
0.3	Adele Downey	DBS SIRO
0.2 & 0.3	Elaine Carlyle	DBS Security
0.2 & 0.3	Dawn Whitehead	DBS Legal
0.2 & 0.3	Stuart Baxter	Home Office Policy
0.2 & 0.3	Angela Duncan	Home Office DSU
	Helen Kilpatrick	Home Office SIRO
0.2 & 0.3	Scott Postlethwaite	DBS Policy
0.2 & 0.3	Graham Sadler	DBS Partnerships
0.2 & 0.3	Barbara Howard	DBS Transition
0.2 & 0.3	Andrea McDonnell	DBS Transition
0.2 & 0.3	Shaun McCann	ANI Head of Business Development

Approval Date	Approved Version	Approver	Approver Role
16/05/2013	v0.3	Adele Downey	DBS SIRO

Related Documents

Related Document	Version	Location
DBS Go-Live	v1.0	http://www.homeoffice.gov.uk/publications/agencies-public-bodies/dbs/about-dbs/dbs-privacy-impact
DBS Programme PIA	v1.0	http://www.homeoffice.gov.uk/publications/agencies-public-bodies/dbs/about-dbs/dbs-prog-impact-assess?view=Standard&pubID=1149281
DBS Privacy Policy		http://www.homeoffice.gov.uk/publications/agencies-public-bodies/dbs/about-dbs/privacy-policy?view=Standard&pubID=1092208
Data Protection Act		http://www.legislation.gov.uk/ukpga/1998/29/contents
Human Rights Act		http://www.legislation.gov.uk/ukpga/1998/42/contents
Police Act		http://www.legislation.gov.uk/ukpga/1997/50/contents
Safeguarding Vulnerable Groups Act		http://www.legislation.gov.uk/ukpga/2006/47/contents
Protection of Freedoms Act		http://www.legislation.gov.uk/ukpga/2012/9/enacted

Glossary of Terms

Reference	Definition
BPSS	Baseline Personnel Security Standard
CEO	Chief Executive Officer
CEOP	Child Exploitation Online Protection Centre
CRB	Criminal Records Bureau
DBS	Disclosure and Barring Service
EU	European Union
HMG	Her Majesty's Government
IAO	Information Asset Owner
DBS	Independent Safeguarding Authority
PIA	Privacy Impact Assessment

PNC	Police National Computer
POFA	Protection of Freedoms Act
POISE	Planned Office Information System Environment
RBAC	Role Based Access Control
SCRO	Scottish Criminal Records Office
SIRO	Senior Information Risk Owner
SOCA	Serious Organised Crime Agency

1 Introduction and Overview

1.1 The DBS was established under the Protection of Freedoms Act 2012 and provides information to help employers in England and Wales make informed safer recruitment decisions, especially those involving children or vulnerable adults. The DBS undertakes the functions previously undertaken by the Criminal Records Bureau (CRB) and the Independent Safeguarding Authority (DBS).

1.2 This Privacy Impact Assessment (PIA) is being undertaken due to the legislative change made to the SVGA, arising from the Protection of Freedoms Act 2012 (POFA). The barring powers of the DBS, in cases other than those meeting the criteria for automatic inclusion without the right to make representations, require the DBS to be satisfied that it has reason to believe that the person under consideration “...is or has been or might in future be engaged in regulated activity...”. This is internally referred to as the Test for Regulated Activity (TRA) The DBS may be so satisfied by carrying out checks including checks with Access Northern Ireland (AccessNI).

1.3 In order to undertake the Regulated Activity check, this involves the sharing of personal data:

- Surname;
- First Forename;
- Aliases;
- PNCID,
- Dates of Birth (DoB);
- DBS Reference Number;

originating from the DBS Discretionary referrals with AccessNI.

1.4 AccessNI will return where available:

- Match found,
- ANI case number,
- Adult, Children or both sectors,
- Position applied for,
- Registered Body name,
- Application in progress / Completed / Withdrawn,
- Application received date,
- Middle Name(s),
- Alternative Surname,
- Alternative Forename(s),
- NINO,
- PNCID,
- Place of Birth,
- Current Address,
- Previous Address(es),
- Passport Number, and
- DVLA No.

1.5 The DBS will use this information to verify that a match has been made against the correct individual to determine whether the Test for Regulated Activity (TRA) has been met and to consider the requirement to progress the referral made to the DBS.

1.6 The legislation POFA which has been commenced, took effect from 10th September 2012.

2 What is this document for?

2.1 What is a Privacy Impact Assessment?

- 2.1.1 Processes that involve exchanging or disclosing personal information inevitably give rise to privacy concerns. Indeed, the cumulative effect of many such initiatives during recent decades has resulted in harm to public trust and to the reputations of corporations and Government agencies alike.
- 2.1.2 PIA is a process which helps organisations to anticipate and address the likely privacy impacts of projects, in order that we can foresee problems, develop solutions, and ensure that concerns are addressed appropriately. For this reason we have followed a PIA process for the implementation of the disclosure of PNC and DBS data by the DBS to the AccessNI to undertake a check for a match against an application for a Barred List check, the results of which will be returned AccessNI to the DBS.
- 2.1.3 This PIA covers only the disclosure of DBS information with regard to Discretionary Referrals made to the DBS.
- 2.1.4 For those cases that are received through the 'AutoBar' route, a separate direct data share will be put in place direct between Police National Computer Services (PNCS) and Access NI. This route will also undertake an initial check on approx 55,000 cases followed by a monthly check. This route will be subject to a separate agreement and PNCS between PNCS and AccessNI.

2.2 What does this PIA Report cover?

- 2.2.1 This report sets out the arrangements under which the disclosure of PNC data will operate, and how its operation can be expected to relate to the privacy of the individuals involved.

2.3 How have we conducted the PIA?

- 2.3.1 We have sought to examine the arrangements both objectively and from the point of view of the individual, to ensure that we meet the legitimate expectations of those concerned. We believe that the arrangements that we have put in place for the disclosure of DBS data to AccessNI reflect good practice in data sharing and protection, striking a fair balance between protecting the privacy rights of the individual and the protection of the public from harm.

2.4 What type of PIA have we conducted?

- 2.4.1 In deciding whether to conduct a PIA, and what type of PIA to conduct, we considered carefully the nature and scope of the disclosure to AccessNI, and its potential to impact on the privacy rights of the individual, in particular that:
- the project involved the introduction of new legislation i.e. POFA which was enacted from 10 September 2012;
 - information will be used by AccessNI to match against disclosure histories where a barred list check has been requested since October 2009; The document has several references to BARRED LIST CHECK. This PIA is about the transfer of information to

determine the Test for Regulated Activity so these references need changing. It may get confused with the new product on the RouteMap known as Barred List check.

- the disclosure to the AccessNI is on a bulk data exchange with updates as and when applicable i.e. when new data is received from PNC.

2.4.2 On the basis of our assessment, we decided to follow a small scale PIA process for the disclosure of the PNC data to ACCESSNI. This is because the project had privacy issues associated with it, but not the large inherent risks that would warrant a full scale PIA, for example those typically associated with new policy areas, major new databases, or using data collected in connection with one purpose for very different purposes.

2.4.3 The changes described in this PIA would usually constitute an amendment to the larger PIA concerning the overall DBS Programme PIA.

2.5 *Is this report the end of the PIA process*

2.5.1 No. We, in consultation with partners will closely monitor and review the scheme's operation, including ongoing review of the privacy impacts, and monitoring compliance with the specific privacy and security arrangements. This will help us ensure that the scheme continues to support the protection of the public from harm and provides benefits both to the DBS and the Police.

3 What is the legal basis for disclosure?

3.1 Schedule 1 Safeguarding Vulnerable Groups (Northern Ireland) Order 2007 (SVGO) provides the legal vires to enable AccessNI and DBS to share information upon request.

4 Data Sharing

4.1 People are naturally concerned to ensure that there is an appropriate balance between the individual's right to privacy and the state's need to share data in order to carry out its functions effectively. People often have very different perspectives on where this balance should lie.

4.2 Whilst the great majority of people agree that Government should share relevant data to an extent that is necessary and proportionate for their purposes – which is also the basic essence of UK data protection law – what this extent actually is in practical terms is often hotly debated. In many ways this is because of the effect of what we might call the 'data sharing conundrum'.

4.3 Data sharing initiatives can therefore involve sharing a relatively substantial amount of data in order to find relevant information within. Whether the data sharing is seen as justifiable is likely to depend on how many, and how valuable the relevant information is, in comparison with the totality of the data sharing. The broader the data sharing, the more intrusive people will find it to be and the more value they will expect it to provide before they consider it to be justified.

4.4 It is therefore important for Government to ensure they target their activities to derive the maximum benefit for the public from the minimum data sharing, as a matter of public trust as well as legality.

5 Data Handling

5.1 There is additional data handling of customer data in the processing of the discretionary referral data by AccessNI to enable a match against individuals' requests to AccessNI for a Barred List check. This will not invoke any changes to:

- data collection policies or practices;
- data quality assurance processes and standards;
- new or changed data retention arrangements.

5.2 The handling of data under this arrangement will also be subject to additional statutory protections under the Data Protection Act 1998 and the Computer Misuse Act 1990.

5.3 Further disclosure is only permitted where it is:

- authorised by an Act of Parliament;
- in pursuance of a order or direction of a court or tribunal;
- in pursuance of a Community obligation.

6 Exemptions and Exceptions

6.1 There are no exemptions or exceptions to this data processing which is in any way exempt from the DPA or other legislative privacy protections.

7 Privacy Law and Data Protection Act Compliance Checks

7.1 There are multiple layers of supervision in place to supervise the access process conducted by the AccessNI:

- The system can only be used by AccessNI staff and suppliers who have Baseline Personnel Security Standard security clearance.
- The AccessNI system has audit logs of individual user activity, which can be accessed by auditors.
- A Memorandum of Understanding has been agreed and signed by the DBS and AccessNI PNC for provision of data to undertake a Barred List Check.
- AccessNI is accredited to handle IL4 'Confidential' information.

8 Consultation and analysis phase

8.1 There have been a number of consultation events along with the passage of POFA through the Houses of Parliament and Lords that have informed that a Test for Regulated Activity (TRA) will be undertaken prior to the DBS proceeding with a referral unless it is an 'autobar' offence that does not require the TRA.

8.2 The public consultations processes prior to the introduction of the Safeguarding Vulnerable Groups (Northern Ireland) Order 2007 outlined that the DBS must provide the Secretary of State with prescribed information relating to a person if it is considering whether to include them in a barred list;

8.3 The public consultation processes prior to the introduction of the Protection of Freedoms Bill into Parliament in 2012 outlined plans for restriction on Regulated Activity.

9 Name of Project/Programme, Process or Policy etc.

9.1 Disclosure and Barring Service (DBS) provision of data to AccessNI.

10 INTRODUCTION

10.1 The disclosure of data to AccessNI to undertake a match as to whether an individual has ever applied for a Barred List Check check.

11 What is its purpose, and how does it relate to Home Office business?

11.1 The principal aim of this data share is to provide the DBS and AccessNI with information that will enable them to better safeguard children and vulnerable adults. It is intended to increase public protection, ensure proportionality with the introduction of the Test for Regulated Activity, and reduce the risk of crime and as such is central to Home Office core business.

11.2 This PIA relates to the DBS sharing of personal information between the DBS and AccessNI. This will enable AccessNI to undertake a check to verify whether an individual has applied for an Barred List check which is only undertaken where an individual has applied or is applying for work in Regulated Activity.

11.3 A positive response will indicate to DBS that the individual may have met the Test for Regulated Activity i.e. an individual is, or has been, or might in the future be engaged in Regulated Activity.

12 Details of personnel involved in undertaking the PIA

12.1 The stakeholders involved in this initiative are:

- DBS CEO;
- DBS SIRO;
- DBS Asset Owner;
- DBS Policy;
- DBS Legal;
- DBS Security;
- DBS Information Governance;
- DBS Project;
- Head of PNC Services;
- Home Office Policy;
- Home Office DSU;
- Home Office SSPU;
- AccessNI;
- Citizens are referred under SVGA.

13 **Awareness:** Does supporting documentation demonstrate awareness of privacy issues? Outline evidence and give details of any appended documentation.

13.1 The DBS and AccessNI operate established processes and systems for the management of sensitive personal information i.e. personal data.

- 13.2 There is a change to handling of sensitive personal data in that a XML file containing PNC Name(s), Aliases, DoB, PNCID, DBS Reference Number etc will be sent via email over GSI from DBS to AccessNI with a response XML file being returned over GSI.
- 13.3 All emails are checked by 2 separate individuals to check email address and file attachment before being sent. Delivery and read receipts are requested. Minesweeper has been configured to only allow the file to be issued to a specified email address. In the event that Delivery and Read receipts are not received a manual process will be invoked to contact AccessNI.
- 13.4 Awareness of the privacy implications are demonstrated by the fact of the awareness of:
- the legal vires that have been put in place to enable this data sharing;
 - the controls that are in place for access to this data via DBS and AccessNI.
- 14 **Scoping:** Please provide evidence that all privacy issues have been fully considered through privacy scoping at an early stage, including details of consultation with all relevant partners?
- 14.1 Access to the AccessNI system is controlled by Role Based Access Controls (RBAC). These processes ensure only those DBS and AccessNI staff / suppliers with a legitimate business interest will have access to the data.
- 15 **Impacts:** With regards to privacy issues, what could go wrong, how serious could it be, and what could be done about it?
- 15.1 Disclosure could be given to someone who then goes on to further disclose the information to another for either good intent or malicious intent. This could result in either information being unnecessarily disclosed, information being passed to other individuals for a genuine reason i.e.: safeguarding and in the extreme case, information being disclosed that then leads to acts of vigilantism i.e.: harassment.
- 15.2 There are a number of measures that have been put in place in order to reduce the likelihood of such situations and also minimise their impact. These are:
- AccessNI is not open to anyone – it is made to specific staff with a legitimate business interest who are best placed to use the information to protect the children and vulnerable adults from harm;
 - Staff are also informed that any breach of the confidentiality agreement constitutes a breach of the Data Protection Act and may result in legal proceedings being brought against them;
 - All staff users who have access to the data are subject to a minimum of Baseline Personnel Security Standard (BPSS) security clearance;
 - All staff undertake data protection training on an annual basis;
 - All staff access is managed by RBAC so as to enforce need to know principles;
 - The data exchange between interested parties will take place over a secure accredited network to defend against interception during file transfer.
- 15.3 There is no additional impact to the individual in that the checks will be made against the data already held by the AccessNI, and there will be no additional collection of data from the individual with regards to the AccessNI application.
- 15.4 As part of the coalition agreement, the government committed to reviewing and reforming the vetting and barring scheme and criminal records regime, scaling them back to common sense levels. The TRA ensures there is a continued service to help safeguard

vulnerable groups including children from those people who work or volunteer with them who pose a risk of harm, while operating in a way that reduces the burden on employers and better respects the civil liberties of the individual.

16 SUMMARY OF PRIVACY RISKS AND MITIGATION

16.1 Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?

16.1.1 Data interception during file transfer which is mitigated by the use of a secure network email exchange from and to specific email addresses.

16.1.2 User Browsing of data which is mitigated with RBAC and Access Assurance Checks (Audit), user awareness training and minimum BPSS security clearance.

16.1.3 Security controls are in place as per HMG standards to protect against attack i.e. hacking and is being transferred system to system over a RESTRICTED accredited network.

16.2 16.2 Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?

16.2.1 As described in the Section 16.1 and limited to the DBS and AccessNI.

16.3 What are the risks associated with how long data is retained and how they might be mitigated?

16.3.1 The DBS file containing data will be received by AccessNI and processed. This file will be overwritten each month, reducing access to the data. An audit file will be retained for 4 years, this will be secured along with all other audit files to the standards in place and as defined within the AccessNI Data Retention Policy.

16.4 What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

16.4.1 As described in Section 16.1.1. No further risks have been identified.

16.5 16.5 Given the external sharing, what are the privacy risks and how might they be mitigated?

16.5.1 As described in Section 16.1.1. No further risks have been identified.

16.6 16.6 How could risks associated with individuals being unaware of the collection be mitigated?

16.6.1 There is no new collection of data from individuals however AccessNI will be sharing information as to whether an individual has applied for an Barred List Check since October 2009 with the DBS.

16.7 What are the privacy risks associated with redress and how might they be mitigated?

16.7.1 Any redress would be against inclusion in the DBS Barred Lists for which there is in place an Appeal Procedure, Review Procedure and Complaints Procedure and/or disputes with AccessNI regarding whether an Barred List Check has been applied for at any time.

16.7.2 In the event of data loss this would be subject to the Information Commissioners' investigation and findings.

16.8 Given access and security controls, what privacy risks were identified and how might they be mitigated?

16.8.1 The existing Access and Security controls within DBS and AccessNI are sufficient for access to the PNC data and no further risks have been identified.

17 OVERVIEW

17.1 What changes have been made or recommended as a result of the PIA process? At which key milestones in the project's lifecycle will the PIA be revisited? Please give details of appended Risk Register.

17.1.1 No changes are required for this data share with the current Access and Security Controls that are already in place within the DBS and AccessNI Systems.