Disclosure & Barring Service

DBS Police National Database privacy impact assessment

Version: 1.0

Date: May 2014

References/related products

No.	Document / Material
01	IAS6 - Protecting Personal Data and Managing Information Risk
02	Privacy Impact Assessment Guidance
03	CESG Good Practice Guide No. 3 - Securing Bulk Data Transfers
04	ICO Data Sharing Code of Practice
05	ICO Data Sharing checklists
06	Data Transfer Policy
07	Human Rights Act 1998 - Article 8
08	The Freedom of Information Act 2000
09	Data Protection Act 1998
10	The Common Law Duty of Confidence
11	Safeguarding Vulnerable Groups 2006
12	Protection of Freedoms Act 2012
13	Computer Misuse Act 1990

Abbreviations

ACPO	Association of Chief Police Officers
CEO	Chief Executive Officer
CSD	Home Office Corporate Security Directorate
DBS	Disclosure and Barring Service
DPA	Data Protection Act
NDPB	Non-Departmental Public Body
PIA	Privacy Impact Assessment
PND	Police National Database
POFA	Protection of Freedoms Act
SIRO	Senior Information Risk Owner
SVGA	Safeguarding Vulnerable Groups Act

Contents

THE UPDATE SERVICE – PRIVACY IMPACT ASSESSMENT (PIA)

1 INTRODUCTION AND OVERVIEW

1.1 The Disclosure and Barring Service (DBS) was established on 1 December 2012 under Chapter 3 of the Protection of Freedoms Act 2012 (POFA) as a Home Office Safeguarding and Public Protection Unit sponsored Non-Departmental Public Body (NDPB).

1.2 This Privacy Impact Assessment (PIA) is being undertaken due to the legislative change made to the SVGA, arising from POFA to share the DBS Barred Lists with the Police.

1.3 This PIA also incorporates the sharing of DBS information with the Police under Section 50A of the Safeguarding Vulnerable Groups Act 2006 (SVGA).

2 WHAT IS THIS DOCUMENT FOR?

2.1 What is a Privacy Impact Assessment?

2.1.1 Projects 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 as well as saving life and protecting people who are vulnerable.

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 the DBS Barred Lists to the Police and incorporated the existing sharing of DBS data with the Police.

2.2 What does this PIA Report cover?

2.2.1 This report sets out the arrangements under which the disclosure of the DBS Barred Lists under POFA Section 77 (3) & (4) and DBS information shared with the Police under Section 50A of SVGA operates, 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.

2.3.2 We believe that the arrangements that DBS have put in place for the disclosure of the DBS Barred Lists and sharing information with the Police under Section 50A of the SVGA 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 the Police in its entirety , and its potential to impact on the privacy rights of the individual, in particular that:

- although the project does involve the introduction of new legislation, it does not completely present a new policy area. Concepts and practices of disclosure of the DBS Barred Lists are based on existing disclosures under SVGA Section 50A and POFA;
- information will be used by the Police in specific circumstances i.e:
    - recruitment of staff under the control of the Chief Constable;
    - check whether an individual is barred;
    - prevention and detection of crime;
- the disclosure of the DBS Barred Lists to the Police is on a bulk data exchange with updates as and when applicable i.e. when an individual is added or removed to/from the DBS Barred Lists;
- The disclosure of DBS information to the Police under Section 50A of the SVGA is on a case by case basis;
- The PND is to be used solely for policing purposes. For the purposes of this code:
    a) protecting life and property;
    b) preserving order;
    c) preventing the commission of offences;
    d) bringing offenders to justice and any duty or responsibility of the police arising from common or statute law.;

    Please note 'policing purpose' doesn't mean police purpose but wider policing by UK law enforcement or engage in the above activities.

The search result on PND may include a DBS record but the disclosure of that record to the requestor is on a case by case basis.

2.4.2 On the basis of our assessment, we decided to follow a small scale PIA process for the disclosure of the DBS Barred Lists. This is because the DBS are under a duty to provide these lists to the Police and the project has 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 With regard to disclosure of DBS information to the Police under section 50A this is a 'Power' and is undertaken on a case by case basis where the Police have provided a legitimate business reason for the requirement of the information and therefore there are no inherent privacy risks.

2.4.4 The changes described in this PIA would usually constitute an amendment to the larger PIA concerning the overall DBS 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 The Protection of Freedoms Act 2012 S 77 (3) & (4) provides the legal vires that places a duty on the DBS to provide the DBS Barred Lists to Police and to provide DBS Barred List information to the police for recruitment purposes. This builds on the legal vires in the Safeguarding Vulnerable Groups 2006 (S. 50A) of disclosing information to the Police on a case by case basis.

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 i.e. prevention and detection of crime. 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

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, those nuggets are, 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 Access to the Barred Lists will be matched against the individuals' Police National Database (PND) record and a marker set. This data is read only and will not invoke any changes to:

- Existing DBS data collection policies or practices;
- data quality assurance processes and standards;
- new or changed data retention arrangements;
- 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. A person (a member of Police or civilian staff or otherwise) is required to keep information confidential if it has become available to them by virtue of their role in accessing the information.

5.2 Access to DBS Information shared under SVGA Section 50A is on a case by case basis. This data is read only and does not invoke any changes to:

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

5.3 Further disclosure is only permitted where:

- It is authorised by an Act of Parliament;
- It is in pursuance of a order or direction of a court or tribunal;
- It is in pursuance of a Community obligation;
- It is in order to facilitate the prevention,detection and investigation of crime and /or the apprehension and prosecution of offenders;
- The Chief Officer of Police reasonably believes the disclosure to be relevant to an enhanced disclosure application.

6 EXEMPTIONS AND EXCEPTIONS

6.1 Whilst the processing of data is subject to the protections afforded by the Data Protection and Human Rights Acts and other relevant legislation, some of the processing may, on a case by case basis, be exempt from some aspects of the legislative privacy protections under Section 29 of the Data Protection Act (which covers the use of personal data for crime and taxation purposes).

7 PRIVACY LAW AND DATA PROTECTION ACT COMPLIANCE CHECKS

7.1 There are multiple layers of supervision in place to supervise the access process to the Police National Database (PND) and the Police National Computer (PNC):

- The system can only be used by Police or Civilian staff who have met the appropriate level of security clearance and completed the Police vetting process and have access level DARC 5.
- The PND and PNC systems have audit logs of individual user activity, which can be accessed by auditors.
- A Memorandum of Understanding has been agreed and signed by both the DBS and ACPO for provision, security and service management of PND access to DBS Barred List markers.
- Information under Section 50A of the SVGA can be disclosed to the Police. This information will be put through the Police National Intelligence Assessment prior to uploading to the Police systems.
- A Memorandum of Understanding has been agreed and signed by both the DBS and ACPO for disclosure of information under Section 50A

8 CONSULTATION AND ANALYSIS PHASE

8.1 There have been a number of consultations that have highlighted that information would be provided from the DBS to the Police for the purposes of verifying whether an individual is barred from working with children, vulnerable adults or both.

- The public consultation processes prior to the introduction of the Protection of Freedoms Bill into Parliament in 2012 outlined plans for this data sharing to take place.
- During the passage of the Bill, the intention to share the DBS Barred Lists, and the further disclosure of information under Section 50A to the Police was outlined.

9 NAME OF PROJECT/PROGRAMME, PROCESS OR POLICY ETC.

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

10 INTRODUCTION

10.1 The disclosure of the DBS Barred Lists to the Police to be stored on the Police National Database system

11 WHAT IS ITS PURPOSE, AND HOW DOES IT RELATE TO HOME OFFICE BUSINESS?

11.1 The principal aim of this scheme is to provide the Police with information that will enable them to better safeguard children and vulnerable adults. It is intended to increase public protection and reduce the risk of crime and as such is central to Home Office core business.

11.2 This PIA relates to the sharing of personal and corporate information and includes the sharing of data between the DBS and other parts of the Home Office family i.e. The Police and the Police National Database system (PND).

12 DETAILS OF PERSONNEL INVOLVED IN UNDERTAKING THE PIA (NAME/SECTION/ROLE/CONTACT DETAILS)

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;
- Chief Constable ACPO Intelligence
- ACC ACPO lead Disclosure;
- Police National Database SIRO;
- Home Office Policy;
- Home Office CSD;
- Citizens who have been barred 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 operates established processes and systems for the management of sensitive personal information i.e. personal data (Name, Date Of Birth, Address, etc), Barred Decisions / Reasons / Lists incorporating data from the Police National Computer i.e. cautions, convictions, Local Police Forces intelligence and other sources i.e. referrals and subsequent allegations.

13.2 There is a change to handling of sensitive personal data and handling of the DBS Barred Lists in that under POFA the DBS will provide this data to the Police National Database. This information will be uploaded by DBS into a dedicated access point to PND within DBS Stephenson House by nominated DBS staff.

13.3 Awareness of the privacy implications are demonstrated by the fact of the awareness of the legal vires that enable this data sharing and the controls that are in place for access to this data via PND..

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 The PND is accredited to the same level as the DBS casework system. Access to this system is controlled by Role Based Access Controls and requests for information from the PND system are authorised by a Supervisor. All access to the PND is fully audited. These processes will ensure only those Police and civilian staff with a legitimate business interest will have access to the barred markers.

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 occurrence of such consequences and also minimise their impact. These are:

- Disclosure 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.

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 PND Users will have access to the markers set on the PND Database to inform the Police of the individuals 'Barred Status'. This is mitigated with the Role Based Access Controls to PND, all requests for PND information are authorised by a Supervisor and all PND access is audited.

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 16.1.1

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

16.3.1 The markers set on PND will remain in place as long as the individual is on a DBS Barred List (The bar is for life, subject to appeal or review). If an individual is removed from an DBS Barred List(s) the PND Marker will be removed accordingly.

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.

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..

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 involved in this data share.

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. In the event of these procedure(s) resulting in removal from the Barred list(s) the PND Marker will be updated accordingly.

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 PND are sufficient for access to the DBS Barred Markers.

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 PND System.