Disclosure & Barring Service

DBS Basic Check – Web Services Privacy Impact Assessment

Version:	1.0
Date	01/09/2017

Synopsis:	Privacy Impact Assessment (PIA) on the DBS Basic check applications submitted by Responsible Organisations via DBS web services.
Document Status:	Approved
Product Id:	DBS_STWR1_0322_DBS Basic Check – Web Services PIA

Abbreviations

Acronym	Detail
AO	Accountable Officer
CRM	Customer Relationship Management
DBS	Disclosure and Barring Service
DPA	Data Protection Act
GDPR	General Data Protection Regulation
HO	Home Office
IT	Information Technology
NACRO	Previously known as National Association for the Care and Resettlement of Offenders, now just Nacro.
NAW	National Assembly for Wales
NINO	National Insurance Number
NPCC	National Police Chiefs Council
OBIEE	Oracle Business Intelligence Enterprise Edition
PIA	Privacy Impact Assessment
PLX	Police Local Cross-reference
PNC	Police National Computer
R1	Release 1 (New DBS modernised computer system)
RBACs	Role Based Access Controls
RO	Responsible Organisation
ROA	Rehabilitation of Offenders Act
SMS	Short Message Service (is a text messaging service)
SPS	Swiss Post Solutions
SSL	Secure Socket Layer (security technology used by web service)
SVGA	Safeguarding Vulnerable Groups Act 2006
TCS	Tata Consultancy Services
TI	Technical infrastructure
TSQ	Telephone Security Questions

Table of Contents

1. INTRODUCTION

Basic criminal record checks submitted via Responsible Organisations - Privacy Impact Assessment (PIA)

1.1. The Disclosure and Barring Service (DBS)

The Disclosure and Barring Service (DBS) is a Non-Departmental Public Body (NDPB) and helps employers make safer recruitment decisions and prevent unsuitable people from working with vulnerable groups, including children.

We are responsible for:

- Processing requests for criminal records checks (DBS checks)
- Deciding whether it is appropriate for a person to be placed on or removed from a barred list
- Placing or removing people from the DBS Children's Barred List and Adults' Barred list for England, Wales and Northern Ireland.

The Disclosure function of the DBS provides information to help employers make informed recruitment and licensing decisions, especially for those posts that involve working with vulnerable groups, including children.

The DBS undertakes legislative functions included within Part V of the Police Act 1997, the Safeguarding Vulnerable Groups Act (SVGA) 2006 and the Safeguarding Vulnerable Groups (Northern Ireland) Order (SVGO) 2007.

The Disclosure function searches police records, Disclosure Scotland records and in relevant cases, information held by the DBS Barring function, and issues a DBS certificate to the applicant.

1.2. What is a Privacy Impact Assessment?

A Privacy Impact Assessment (PIA) is a process that assists organisations in identifying and minimising the privacy risks of new projects or policies.

When conducting a PIA it will involve working with people within DBS, with partner organisations and with people affected to identify and reduce privacy risks.

The PIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

Conducting a PIA should benefit DBS because it can help produce better policies and systems and improve the relationship between organisations and individuals.

The PIA is a process mandated by Cabinet Office and recommended by the Information Commissioner.

1.3. What does this PIA Report cover?

This report examines the impact it will have on data collection, data sharing and processing of a DBS Basic check.

1.4. Maintenance of the Privacy impact assessment

The DBS aims to fulfil its roles and functions efficiently and effectively, maintaining a high quality delivery of services and products. Protection of an individual's privacy and the security of their personal information are fundamental to all that we do.

Given the possibility of changes in Government Legislation, and any future releases of the IT platform, this privacy impact assessment will be regularly reviewed.

2. IDENTIFYING THE NEED FOR A PIA

2.1. DBS Basic Criminal Record Check – project

Basic criminal record checks are currently managed and processed by Disclosure Scotland. DBS are taking over responsibility for providing this service for people who live or work in England or Wales; Disclosure Scotland will continue to process basic criminal record checks for anyone living or working in Scotland (the responsibility for processing basic criminal records for people who live or work in England and Wales was temporarily delegated to Disclosure Scotland and will now be reverting back to DBS).

The project aims to provide a quick, accurate, secure and accessible DBS Basic application service that caters for all individuals and organisations.

A basic criminal record check shows unspent cautions and convictions.[1] Because there are no eligibility requirements, any person aged 16 or over can apply and use it for any purpose. However it is commonly used by many employers as part of their recruitment processes to determine the suitability of their candidates and to check the continuing suitability of their employees.

DBS will be providing two channels for applying for a basic criminal record check:

- Via an organisation registered with DBS, known as a Responsible Organisation, where applications are submitted via a web service;
- A self-service channel where the individual provides all their application data, verifies their identity and pays for their application online - this is the DBS Basic Digital service (where an individual cannot/ or does not wish to verify their identity online an alternative route via the Post Office has been provided).

This privacy impact assessment is looking solely at the basic criminal record checks submitted by Responsible Organisations.

[1] Under the Rehabilitation of Offenders Act 1974, after a certain length of time some criminal convictions can be treated as 'spent' – meaning they're not relevant to a basic criminal record check.

A separate PIA has been completed for the DBS Basic Digital service although there will be some overlap between the two PIAs because the processing of the basic check will be the same.

The scope of this PIA includes the:

- basic applicant whose application has been submitted via a Responsible Organisation;
- Responsible Organisation registration process and the impact on representatives of that organisation.

This new service will provide individuals with quick and easy access to a Basic criminal record check, which for many individuals may help secure employment, for employers it may speed up their recruitment processes and it allows registered organisations to submit multiple applications quickly and securely.

2.2. PIA Screening

To determine whether a PIA was to be undertaken DBS completed a PIA screening checklist. Out of the 8 screening questions DBS answered 'Yes' to 5 of the questions; the reasons behind each of the responses and the decision to conduct a PIA is provided below:

Question	Yes or No	Reason for Response
1. Will the project involve the collection of new information about individuals?	Yes	Personal information will be required to process an application for a DBS Basic check.
2. Will the project compel individuals to provide information about themselves?	No	It is the individual's choice whether or not to apply for a DBS Basic check, however if they wish or need to use this service they must provide all the personal information required to process their application.
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Yes	Information will be made available to a Responsible Organisation in the form of an eResult (this gives an indication to the recipient that either there is nothing to disclose on the certificate or that they should wait to see the certificate); an eResult is produced for all applications. The individual must give consent to process the application and consent for a Responsible Organisation to receive an eResult before the application can be processed. The Responsible Organisation and other 3rd parties (e.g. an employer) can also receive the paper copy of the certificate but only if the individual requests and consents to their basic certificate being

		delivered to these organisations or people. The individual can also choose to give consent for a Responsible Organisation and/or other third parties to view an electronic version of their basic certificate.
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	No	The personal information provided will be used solely to process an individual's application for a DBS Basic check.
5. Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	No	There is no new technology that can be perceived as intrusive.
6. Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	Yes	Decisions on PNC matching and identifying unspent convictions could indirectly have a significant impact on an individual, for example when the basic certificate is presented to a potential employer any information disclosed could impact on the individual's employment opportunities.
7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	Yes	Criminal records can be disclosed on a basic certificate.
8. Will the project require you to contact individuals in ways that they may find intrusive?	Yes	There may be a need for DBS to contact individuals to request information about their previous identity or gender (transgender applicants), which for some may be considered intrusive.

2.3. Decision to conduct a PIA

In deciding whether to conduct a PIA we considered carefully the nature and scope of the collection and disclosure of information to and from both internal and external stakeholders, and the potential to impact on the privacy rights of the individual, in particular that:

- information will be used by DBS to determine whether an individual has any unspent convictions, which could, as an example, impact on an individual's employment opportunities, education etc.

This service involves a new collection of data and it is necessary to evaluate whether the collection and processing of this data will have the potential to impact on the privacy rights of the individual.

Currently the anticipated changes to the processing of data previously collected by the DBS is the way in which it is transmitted, collected and stored, which will now be primarily electronic.

For the basic criminal record check application submitted by Responsible Organisations the data is collected by the Responsible Organisation, who is responsible for verifying the applicant's identity and ensuring the accuracy of the application data. Applications will be sent to DBS via a DBS Application Web service for processing. The web service mechanism is a new interface functionality adopted by DBS and is a change to how DBS have received data before.

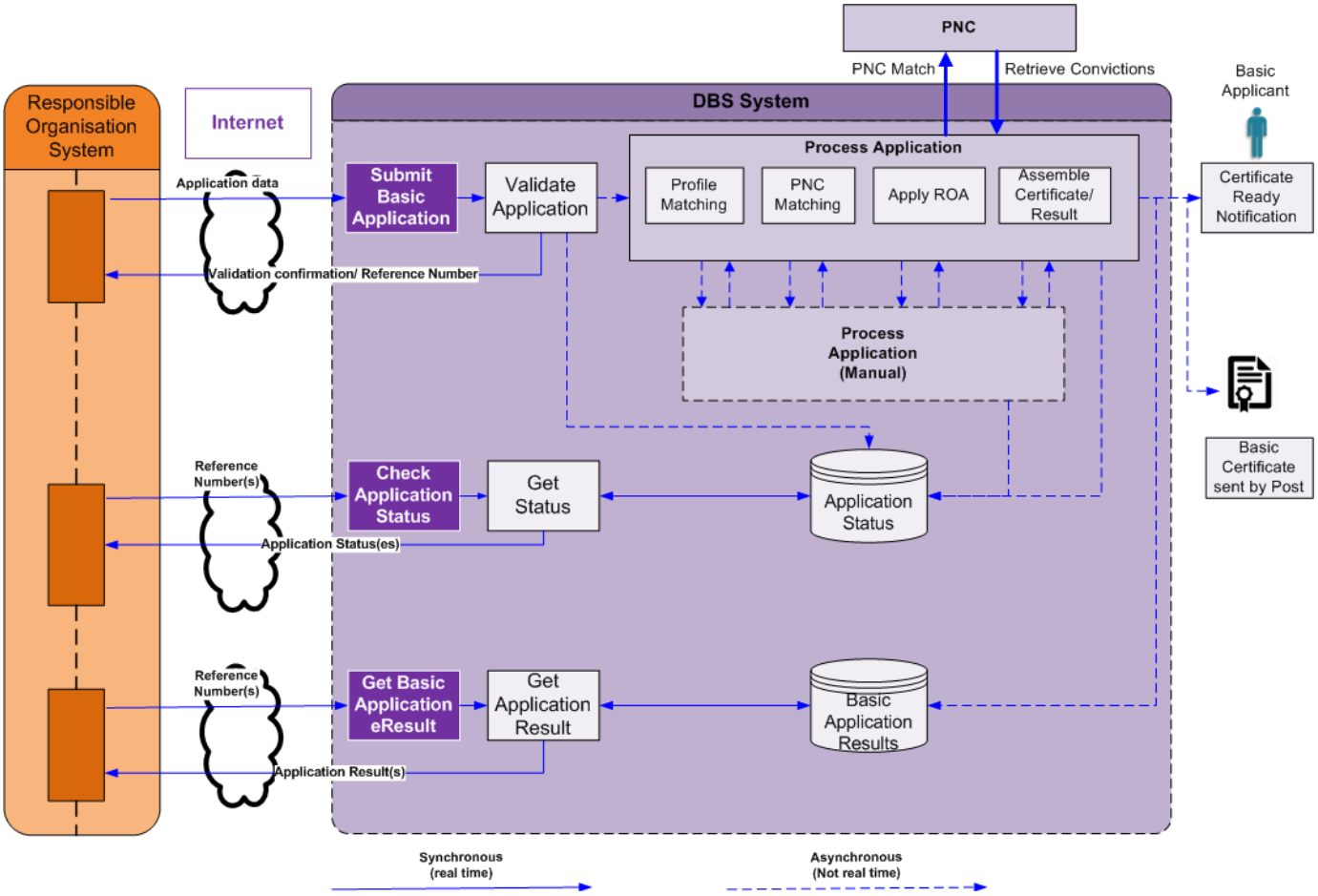
Whilst the basic criminal record check is a new DBS product, how it is processed after application data has been received is very similar to a DBS Standard check (a long-standing DBS product) - the main difference in processing the data is the introduction of new processes to correctly identify spent and unspent convictions in accordance with the Rehabilitation of Offenders Act 1974. Whilst DBS have a well established process for matching with conviction information held on the Police National Computer (PNC) system because this is sensitive information and because a new matching algorithm is to be implemented, if we fail to correctly identify spent convictions the individual's privacy could be severely impacted because we could disclose information that a third party is not entitled to see.

Because DBS require all of an individual's current and previous identity details to process a Basic application for some this could be considered intrusive, a particular example is an applicant who is transgender who does not wish to disclose their previous identity.

From the results of the screening there are areas where potential impacts on privacy could occur. With DBS expecting to receive approximately 1.7 million applications for DBS Basic checks in year 1 (it is expected that approximately 70% will be submitted via a Responsible Organisation and 30% via the DBS Basic Digital service) if any potential privacy risks are not identified and addressed the impact could be high. In light of these findings the decision was made to conduct a PIA.

3. INFORMATION FLOWS

3.1. Basic criminal record check – via web service



The Basic check application service allows Responsible Organisations (ROs) to submit individual basic applications electronically via the DBS Submit Basic Application web service (one application is submitted per transaction, many transactions can be made each day).

The RO could be submitting applications on behalf of a client (e.g. an employer) or on behalf of individuals who have chosen to use this service. How application data is captured by the RO is between them and their customers/ clients however under the terms of conditions the RO must keep the personal data secure and as Data Controllers are required to comply with the Data Protection Act 1998 and the forthcoming General Data Protection Regulation (GDPR).

ROs will be able to apply to use 3 web services; Submit Basic Application, Check Application Status and Get Basic Application eResult.

It is estimated that over 1 million Basic applications will be submitted via the web service each year.

The diagram above provides a view of these web services and where they fit within the end-to-end processes.

Details of the information flows relating to each of these web services are given below.

3.1.1. Submit Basic Application Web Service

To submit a basic criminal record check the RO must:

- Capture all the application data;
- Have the consent of the individual to process the basic application and have the consent of the individual to allow the RO to receive an eResult (see section 3.1.3 for details);
- Verify the identity of the individual as per DBS ID checking guidelines (the RO completes a declaration confirming that the applicant's true identity has been established and verified, and must provide the name of the person who checked the applicant's identity).

Personal application data to be captured includes:
(O) – Optional, (M) - Mandatory

- Title (O);
- Current names: surname(M), forename (M), middle names (O);
- Current address (M);
- Previous addresses within last 5 years (M);
- Dates from and to (for addresses) (M);
- Date of Birth (M);
- Gender (M);
- NINO (National Insurance number) – if available (M);
- DBS Profile ID – if available (O);
- Email address (M);
- Any previous names/ aliases (M);
- Town of birth (M);
- Country of birth (M);
- Mobile number (to be entered if applicant chooses to receive text messages about the status of their application (SMS (Short Message Service)) (O);
- Contact number (can be mobile number or landline) (O);
- Purpose of check (M);
- Passport number and Country of issue - (M) if applicant has a current passport;
- Driving licence number – (M) if applicant has a current UK driving licence;
- Option to have a paper certificate or not (M)
- Address to send paper basic certificate as an alternative to home address (O).

There is also an applicant declaration that requires consent from the applicant to process their application and consent for the RO to receive an eResult (See section 5.1 for more details about consent).

The applicant can also choose to give consent to the RO's Accountable Officer to view an electronic version of their Basic certificate (e-Certificate) when it has been issued. The Accountable Officer would view the online DBS certificate via their DBS online account. The question on the online form reads:

- Do you wish to provide consent to lead contact of RO to view your online DBS certificate when it has been issued? Answer Yes or No.

The applicant can also choose to give consent to a third party who is a DBS online account holder to view their online DBS certificate; to do this the applicant must enter the email address used by that third party to create their DBS online account (this must match an email address used to create a DBS online account to be a valid entry). The recipient of consent would view the online DBS certificate via their own DBS online account. The question on the online form reads:

- Enter the third party email address to provide consent to view your DBS certificate once it is issued.
  This should match the email address registered for the recipients DBS online account (this is an optional question).

There are application data specifications that the RO must comply to (details are within the Submit Disclosure Application Web Service Specification document). If any application data is invalid the application will be rejected by DBS. The validation rules should contribute to a high level of application data accuracy.

An RO must also provide a unique reference number for each application they submit, which will be included in any DBS web service responses and will enable the RO to identify and track the application in their own system.

On receipt of an application from an RO via the web service:

- DBS validates the data format and applies application level validations.
- DBS provides a web service response to ROs informing them of the application acceptance status (either accepting application for further processing or rejecting application due to validation failure).
  - If the application is accepted, DBS sends a web service response containing a unique application reference number to the RO.
  - If the application is rejected DBS sends a web service response containing the reason for rejection.

The only personal data included within the web service responses is the RO unique reference number and the DBS application reference number, which are used to associate the message to the right person in the respective RO and DBS Systems.

After an application has been validated and accepted by DBS, processing by the DBS system will commence:

- If the applicant has an existing DBS online account linked to their DBS Profile a notification will be sent their online account informing them that their application has been received (an email is also sent to inform the applicant that a notification has been sent to their DBS online account);

- If the applicant provided their mobile telephone number and agreed to receive SMS messages, an SMS message will be sent informing them that their

application has been received; the message includes an application reference number (the applicant does not require a DBS online account to receive an SMS message);

- Matching and linking application data to the applicant's DBS Profile; if no DBS Profile exists one is created (a DBS Profile is an individual's unique record that holds personal data and a record of any transactions, services used, previous applications etc. relating to any interactions with DBS, past or present, subject to DBS data retention rules). Matching to a DBS Profile may require manual intervention;

- Matching application data to a PNC (Police National Computer) record; PNC matching may require manual intervention.

- If a match to a PNC record is confirmed, conviction details will be retrieved from PNC; DBS may need to increase the number of DBS staff with access to live PNC by approximately 30 staff to process Basic applications.

- DBS must identify and remove any spent convictions because only unspent convictions can be disclosed on the basic certificate; the process that strips out 'spent' convictions may involve automation and/or some manual intervention;

- Where manual intervention is required access is only given to specific DBS users, who will have access to only the functionality, records and data they need to perform their tasks.

- In exceptions, where it has not been possible to confirm or reject a match to a PNC record, the applicant will be asked to provide fingerprints at a local Police station (the DBS fingerprint process is an existing process). If the applicant refuses to give consent to provide fingerprints or fails to provide fingerprints after giving consent, then their Basic application will be withdrawn;

- The basic certificate will then be assembled and sent to SPS (Swiss Post Solutions) for printing (the certificate can contain unspent convictions or no information).

- If an individual applicant has provided their mobile phone number and agreed to receive SMS messages, an SMS message will be sent to the applicant informing them that their certificate has been despatched.

- If the applicant had an existing DBS online account linked to their DBS profile, a notification will be sent to their online account informing them that their certificate has been despatched.

- After successfully processing the application a paper basic certificate, if requested, will be sent out by post either to the applicant's current address or to another address (for example an employer's address); there is an option on the basic application form to have the basic certificate sent to an alternative delivery address. Only one paper certificate is issued.

- In all cases an online DBS certificate is created (an e-Certificate), which the applicant can view via their own DBS online account, if they have one or choose to create one after their application is processed.

- If the applicant granted consent on their basic application form for an Accountable Officer and/or a third party to view their e-Certificate a notification will be issued to their DBS online account informing them they have consent to view the applicant's e-Certificate however if there are any convictions/ cautions to disclose on the certificate consent will be automatically revoked before the certificate can be viewed.

- Throughout processing the status of the application (where it is in the process) will be recorded to allow the RO to use a web service to check the application status.

- The applicant can also track the progress of their application via DBS online services if they have their application reference or if they have an existing DBS online account linked to their DBS Profile.

After processing, the DBS System will generate an eResult, which can be retrieved by the RO via a web service should they wish to do so (See section 3.1.3. below).

A basic applicant can raise a dispute if they believe incorrect information has been disclosed on their basic certificate. DBS have a well established disputes process. If a dispute is upheld an amended certificate can be issued with any incorrect information removed or amended.

There are potential privacy risks relating to the information disclosed on a paper basic certificate, which are addressed in section 5.

3.1.2. Check Application Status Web Service

The RO will be able to use the Check Application Status web service to find out at which point in the application process each application they have submitted is at e.g. PNC Matching.

Any request must include the Organisation ID (this is a unique organisation identifier generated by DBS when the RO registered with DBS). The RO can request multiple application status checks in a single batch (to ensure requests are manageable a maximum number of requests per batch will be set – initially this will be 50).

The RO must provide the application reference number, the applicant's current surname and their date of birth within their request.

The DBS response will include the Organisation ID, application reference number, the applicant's current surname, date of birth and the status of the application. The status for a basic application can include:

- Received date;
- PNC search date;

- Assemble certificate date;
- Certificate despatched date.

DBS will not give any more personal data to the RO than that provided on the basic application.

3.1.3. Get Basic Application eResult Web Service

An RO can also use a web service to request an electronic result (an eResult) of basic applications they've submitted.

After an application has been processed the DBS system generates an eResult, which will be made available for the RO to retrieve.

DBS provides the facility for an RO to retrieve multiple eResult(s) in a single transaction (up to a maximum of 50 per transaction) via this web service. The RO must provide their unique Organisation ID and the DBS application reference number for each eResult they wish to retrieve or they can specify they want to retrieve eResults generated within a certain period, for example within the last 7 days. An RO can only receive eResults of applications that they submitted.

In response to any requests for an eResult the RO will receive a web service response that will indicate whether an eResult is available or not for retrieval.

The eResult gives an indication of the information that will appear on the certificate:

- A blank response (indicates that no unspent convictions have been disclosed on the basic certificate) or;
- RO is advised to wait to view the paper basic certificate (this could infer that something is disclosed on the paper basic certificate but no details of convictions are disclosed within the eResult).

Because there is an option on the application for an alternative delivery address for the basic certificate how and when the RO views the certificate is dependent on where and to whom it is delivered - it could be received by the applicant or a third party such as an employer or the RO itself. The RO may have no requirement to view the certificate, they may only be interested to know that the application has been processed and the certificate has been despatched.

The eResult will also include the following details:

- RO Organisation ID
- Certificate number;
- Date eResult and certificate were issued;
- Applicant's forename;
- Applicant's surname
- Applicant's other names;
- Date of birth;
- Address;

- Birth town;
- Birth country;
- Gender

Whilst no specific sensitive information (convictions/ cautions) are are actually disclosed within an eResult it is accepted that if the RO is advised to wait to see the certificate this is a clear indication that there is something disclosed on the certificate; this is a privacy risk (see section 5).

DBS will not give any more personal data to the RO than that provided on the basic application.

3.2. Responsible Organisation Registration - Accountable Officer

A Responsible Organisation (RO) is an organisation registered with DBS to enable them to submit applications for Basic DBS checks via a new DBS web service.

An application to become an RO can only be submitted online and must be completed by an Accountable Officer (this should be a person of authority within the organisation).

To enable an Accountable Officer to submit an application to register as an RO they must first create a DBS organisation online account. To create a DBS online account the Accountable Officer will need to provide some personal details (DBS online accounts will be covered in detail in a separate Release 1(R1) DBS Standard and Enhanced checks Privacy Impact Assessment that will cover all aspects and features of the DBS online accounts, which will include creating a DBS online account, hence the impact on privacy of DBS online accounts are out of scope of this PIA).

The Accountable Officer will initially complete an online RO application form (ROAF) via their DBS online account. This provides details of the organisation, expected usage of the Basic application service and some financial details of the organisation. The Accountable Officer also provides some personal data about themselves that will be stored within the DBS organisation profile relating to the Responsible Organisation; personal data collected:

- Title
- Forename(s)
- Surname
- Date of Birth
- Gender
- Contact telephone number (likely to be an organisation number)
- Role in the organisation

The Accountable Officer will also be asked to provide their work address details

On receipt of the RO application form DBS will review the details and make a decision on whether or not the organisation is eligible to become a Responsible

Organisation. To be eligible the organisation must have stated that they will submit at least 1000 Basic applications per year and satisfy a DBS financial credit check; the organisation must also sign up to all agreements, for example Terms and Conditions.

If the organisation is considered eligible DBS now have to determine the suitability of the Accountable Officer. The Accountable Officer will be asked to apply for a DBS Basic check (they will be able to apply via the DBS Basic Digital service from January 2018 or via another Responsible Organisation). On receipt of their paper basic certificate the Accountable Officer will be required to send the certificate to the DBS Registration Team (the Accountable Officer can choose to have their basic certificate sent direct to DBS or send it themselves after they've received and viewed their certificate). If the Accountable Officer refuses to apply for a DBS Basic check the RO registration process will be cancelled. The organisation can reapply to register as an RO but the new application would need to be completed by an Accountable Officer who is willing to apply for a DBS Basic check.

A decision on the suitability of the Accountable Officer will be made by DBS based on the information disclosed on the basic certificate (the Accountable Officer Responsible Organisation Privacy Policy sets out the criteria for determining suitability of an Accountable Officer).

If the Accountable Officer is found to be unsuitable they can appeal against the decision.

If the Accountable Officer is found suitable and the organisation is considered eligible, the organisation will be registered as an RO. The Accountable Officer's personal details will be held on the new DBS system.

An Accountable Officer can also nominate other individuals from the RO to fill particular roles (these roles aren't mandatory; an Accountable Officer may choose to take responsibility to perform the activities associated with some or all of these roles):

- Primary contact – a named contact who can deal with the day to day notifications between DBS and the RO;
- Finance contact – who will manage invoices, payments etc. related to the number of basic applications submitted by the RO.
- Technical contact – who will be involved in technical tasks such as setting up and maintaining the web services.

Each of these roles will require an organisation DBS online account (this will be covered in the R1 DBS Standard and Enhanced checks Privacy Impact Assessment), which will require each individual to provide a limited set of personal data (this will be used purely to identify them when they make contact with DBS). Apart from checking the format of the data provided to create an online DBS account, DBS will not be carrying out any other checks, such as identity checks, on any of the individuals filling these roles nor will an individual DBS Profile be created; the onus will be on the Accountable Officer to nominate suitable people.

4. CONSULTATION

DBS are currently going through a major modernisation programme (R1) of which changes to how DBS Standard and Enhanced checks will be processed will be the major changes. The DBS Basic check is dependent on much of the functionality developed for Standard and Enhanced checks but because the new Basic check is due to go-live ahead of Standard and Enhanced, which was not the original plan, some of the privacy risks already identified for Standard and Enhanced will now be addressed from the perspective of the Basic check.

Whilst DBS are introducing new services, systems and processes much of the new design is based on the current processes. And because DBS have a good working knowledge of the current processes we had already identified a number of existing privacy risks (no PIA has been carried out on the existing service because it was implemented prior to the introduction of PIAs), which has influenced the design of the new system. This has enabled DBS to look more closely at changes that are particular to the DBS Basic check service.

4.1. Internal consultation

Many business representatives have been involved in the design of the new Basic application service from the outset and have an extensive knowledge of the end-to-end process, decisions made, reasoning and considerations of privacy risks.

The relevant business subject matter experts have been consulted throughout to confirm and clarify processes to help determine if there are any potential privacy risks and what, if anything is being done to address them (includes our operational staff, security, finance, legal and policy people).

Regular consultation with our Data Protection and Information Governance & Security people has taken place and continues as services are further developed.

DBS in parallel are developing an individual online self-service DBS Basic check application service, known as the DBS Basic Digital service, where personal application data is provided by the individual direct to DBS. The DBS project team involved in developing this channel have built the service using agile, iterative and user-centred development methods in accordance with Government Digital Standards. They have consulted with DBS business representatives, and potential users throughout and agreed and identified the minimum set of personal data required to process an application, in line with the principle: only data that is actually needed is collected and processed; some of these decisions have influenced the design of the Basic application service where applications are submitted via a Responsible Organisation (for example a decision was made to remove a question about unspent convictions, which has been removed from both services). Ongoing consultation between the teams developing the different Basic application channels continues.

4.2. External consultation

DBS are taking over responsibility for providing the Basic application service in England and Wales from Disclosure Scotland. DBS have consulted throughout with Disclosure Scotland, which has helped DBS identify potential privacy risks and has influenced the design of the DBS Basic service (for example identity checking methodology).

Approximately 70 organisations that are registered to submit Basic applications via Disclosure Scotland will be registering with DBS to become Responsible Organisations. DBS have engaged with these organisations since the decision to transition was made and continue to do so. These organisations are fully aware of their responsibilities and the new web services they'll be using to submit basic applications. Each organisation will need to sign up to all relevant agreements with DBS.

The DBS Registration Management (RM) team have a working relationship with all registered organisations (Responsible Organisations and Registered Bodies) and will be the conduit for any consultation with Responsible Organisations.

The DBS Registration Management (RM) team will also be responsible for carrying out compliance checks to ensure that each Responsible Organisation is meeting all agreements.

User research has also been conducted by the DBS project team developing the DBS Basic Digital service, some of their findings have influenced the design of this service and helped to eliminate a privacy risk; this is a continuous and iterative process and hence consultation will continue throughout product development.

DBS will also involve the Information Commissioner's Office (ICO) in the PIA review process.

DBS have also approached the top 4 Registered Bodies who will become Responsible Organisations, NACRO, Liberty and Unlock to see if they wish to be involved in the review process.

5. DATA PROTECTION PRINCIPLES

5.1. Data protection Act Principle 1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless: a) At least one of the conditions in Schedule 2 is met, and b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.	
Why is the personal data being collected used, disseminated, or maintained?	**Basic Applicant** • Personal data will initially be used to check if DBS have an existing record of the individual; a DBS Profile (this could have been created by the individual when they had applied for a DBS check previously or used another DBS service). An individual should have only one DBS Profile; if an existing profile is found the application will be linked, if no profile is found one will be created. • Personal data is collected primarily to be used to match against PNC records (convictions and cautions). • DBS provides facilities that allow an individual to notify DBS of any changes to their personal data, which will be added to their DBS Profile. • The DBS Data Retention Policy (DRP) specifies how long data is retained (subject to current Home Office embargo on deleting data). **Accountable Officer** • Personal details captured on the RO registration application form will be used to contact the Accountable Officer about matters relating to the Responsible Organisation and provide a means to confirm their identity. • The Accountable Officer must inform DBS of any changes to their personal details and any organisation details. • Personal details captured as part of a DBS Basic check – see section on Basic Applicant

	above.
Where is the information collected from, how, and by whom?	**Basic Applicant** • The Basic applicant's personal data is provided by a Responsible Organisation (RO) and is submitted to DBS via a DBS web service. • How this data is collected from the Basic applicant may vary for each RO; an RO may collect the application data direct from the individual or via a client, for example an individual's employer. **Accountable Officer** • The Accountable Officer will provide their own personal data; some personal details will be provided on the online RO registration application form and other personal data will be provided with their application for a DBS Basic check (this could be provided via the DBS Basic Digital service or via another Responsible Organisation). • In some circumstances the Accountable Officer will be required to send DBS a set of specific identity documents, which are used by DBS to confirm their identity (see section 5.4 for more details).
If collected by an organisation on behalf of DBS, what is the relationship and authority/control DBS has over the organisation? Who is the Data Controller and Data Processor? Is a formal agreement in place to regulate this relationship?	**Basic Applicant** • An organisation (RO) must have successfully registered with DBS before they are permitted to submit Basic applications; this will involve confirming whether the organisation is eligible and whether their responsible person, known as an Accountable Officer, is suitable. • The organisation must sign up to DBS's Terms and Conditions, an Interchange Agreement, and commercial Data Processing Terms and Conditions agreements. • DBS will carry out regular checks on ROs to ensure the organisation remains compliant to all agreements. If any irregularities are identified an RO's registration may be cancelled, which will prevent the RO from submitting basic applications. • The RO will be the Data Controller for the information until it is received by DBS.

How will you tell individuals about the use of their personal data? Do you need to amend your privacy notices?	**Basic Applicant** • It is the Responsible Organisation's responsibility to confirm with individuals that they know about the use of their personal data; how they do this is between the RO and the individual, for example they may include it on the application form they use to capture the application data from the individual. • After confirming with the individual that the application data that they have collected is complete and true, and that they have read the DBS's related fair processing notice (privacy notice) the RO are required to complete the declaration on the electronic application form, which is to be submitted via the DBS web service, confirming that the applicant has read and understood the DBS's statement of fair processing (privacy notice). If no such assurance is received the application fails validation and will not proceed to processing. • DBS have created a new DBS Basic Check Privacy Policy For Applicants submitting applications via an RO due to the introduction of this DBS Basic check application service. • DBS will also make the relevant privacy notices available on the GOV.UK website to allow individuals to check how their personal data will be used. • **Accountable Officer** • DBS have amended their Privacy Policy to inform the Accountable Officer how their personal data will be used. **Note:** DBS will be reviewing all Privacy notices to ensure they comply with GDPR but they may not be at the standard required when this service goes live.
Have you established which conditions for processing apply?	**Basic Applicant** • Yes, consent. **Accountable Officer** • Yes, consent
If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or	**Basic Applicant** • The Responsible Organisation cannot submit applications unless they have the individual's informed and explicit consent (European Data Protection Directive (to which the Data Protection Act gives effect) defines an individual's consent as: any freely given specific and

withdrawn?	informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed).The nature of consent to satisfy the condition for processing sensitive personal data (in this case criminal records) must be "explicit". • The Responsible Organisation must obtain the individual's informed and explicit consent. • The Responsible Organisation must indicate on the application that the individual's informed and explicit consent has been received. • When giving consent the individual must agree to their application being processed and to the Responsible Organisation receiving an electronic notification (an eResult) once the application has been processed (see section 3.1.3 for details of eResult). • If the individual does not wish to give the Responsible Organisation consent to receive an eResult the individual will not be able to use this service and should be advised to use the Basic Disclosure service provided by Disclosure Scotland (service available until 31/12/2017 for people who live or work in England and Wales) and from 01/01/2018 the DBS Basic Digital Service if they still require a DBS Basic check. • The Responsible Organisation is required to keep a record of informed and explicit consent received from each individual. • If consent is withheld the application will not be processed. • An individual can also choose to give explicit consent on their basic application to the Accountable Officer and/or another third party (who must must have a DBS online account) to view an electronic version of their Basic certificate; this is optional. After their certificate has been issued the individual can remove consent if they so wish • DBS will carry out regular compliance checks that will include checking with individuals that they did give consent; full details of the compliance checks are to be determined. • An individual can withdraw their application and/or withdraw consent after an application has been submitted to DBS for processing and processing has **not** been completed. DBS can stop the processing and withdraw the application (the speed of processing for many applications may mean there is only a small window of opportunity to stop and withdraw an application). • DBS provide guidance on withdrawing applications on GOV.UK.

	Accountable Officer • For an Accountable Officer submitting their application for a DBS Basic check via another Responsible Organisation see 'Basic Applicant' above with regard to consent. • For an Accountable Officer submitting their application for a DBS Basic check via the DBS Basic Digital service informed and explicit consent is captured on the online application form. • If consent is withheld the application for a DBS Basic check will not be processed however it is a DBS requirement that an Accountable Officer has a DBS Basic check as part of the Responsible Organisation registration process and so if consent is withheld the registration process cannot proceed (Organisation would need to nominate a new Accountable Officer and submit a new application to register as a Responsible Organisation).
What information is collected, used, disseminated, or maintained in the system?	For full details of what information is collected, how it is used and disseminated, see section on 'Information Flows'. **Basic Applicant** • For each individual a unique record will be created that will hold all their personal data, records of applications submitted and records of other DBS services used. • The individual will be able to notify DBS of any changes to their personal data. • DBS will retain data as per the DBS Data Retention Policy (subject to Home Office embargo on deleting data) **Accountable Officer** • Personal details collected from the RO registration application form will be held on the RO's DBS Organisation Profile. • The Accountable Officer will be responsible for ensuring these details are kept up-to-date. • These details will be held by DBS throughout the organisation's registration or until a new/ replacement Accountable Officer is put in place. • If an organisation's registration ceases and/or the individual ceases to be an Accountable Officer DBS will retain data as per the DBS Data Retention Policy (subject to Home Office embargo on deleting data) • Personal details captured as part of a DBS Basic check – see section on Basic Applicant

	above. • In some circumstances the Accountable Officer will be required to send DBS a set of specific identity documents, which are used by DBS to confirm their identity (see section 5.4 for more details).
Is there a specific legal power that enables the gathering and use of the information? Does the power mandate the collection of the data or merely permit it?	**Basic Applicant** • An individual is entitled under Part V of the Police Act 1997 to apply for and receive a criminal conviction certificate on the understanding they make an application in the prescribed form and pays any fee that is payable in relation to the application under regulations made by the Secretary of State. • There is no specific legal power that enables DBS to gather and use the information; DBS requires specific information to process an application for a DBS Basic check and can only process this information with the informed and explicit consent of the individual, if an individual does not provide this information or give consent DBS will not process the application. **Accountable Officer** • There is no specific legal power that enables DBS to gather data from an Accountable Officer.
Is there a specific business purpose that requires the use of this information?	**Basic Applicant** • Yes, the information collected is required to process the application for a DBS Basic check. • The personal information is used mainly to match against PNC records to help determine whether or not an individual has any convictions (No**t**e: DBS has appropriate data sharing and interchange agreements with the police to process and exchange information. Information exchange with the Police will be over the Protected Public Service Network (PSN), which is subject to HMG accreditation and restricted to a predominantly government community). **Accountable Officer** • The personal information collected on the RO registration application form is used mainly to contact the Accountable Officer in matters related to their Responsible Organisation.

	• As part of the RO registration process the Accountable Officer will also need to apply for a DBS Basic check; the outcome of this check will be used to determine the Accountable Officer's suitability for the role (also see paragraph on Basic Applicant above).	
Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?	Risks	Mitigation
	1. There is a risk that personal data provided by the applicant could be lost, tampered with and/or misused (for example identity theft) when transferred from the RO System to DBS via a web service.	• DBS will be deploying web service security features, as recommended by the National Cyber Security Centre (NCSC), that ensures only known users (ROs) can access the web services and ensures that no third party can eavesdrop or tamper with any message sent between the RO and DBS (more details on web service security features can be found in Appendix B)
	2. The original design for the Basic application form included the question 'Have you any unspent convictions? Because an applicant may be unsure whether any convictions they have had are spent or unspent they could inadvertently alert a potential employer of a previous spent conviction by answering 'Yes' to the question. Whilst the spent convictions would not be disclosed on their basic certificate the employer could discover that their employee has had a conviction, which they had no entitlement to know about, causing potential stress and/or damage to the applicant. **Note:** As an alternative, if the applicant answered 'No' to the question because they thought their convictions were spent and a conviction was disclosed on their Basic certificate an employer may believe that the individual was dishonest because they failed to declare they had an	• DBS investigated the need for previous conviction information and established that it was only used in exceptional circumstances. • It was recognised that the individual may not be able to answer the question correctly (the reason for applying for a DBS Basic check could be to determine if they had any unspent convictions?) Decision was made to remove this question from the application form, eliminating the risk.

	unspent conviction, which could cause potential stress and/or damage to the applicant.	
	3. After an application has been received by DBS an individual can withdraw their consent to have their application processed, but because it is expected that many applications will be processed quickly (some could be as little as a day) a Basic certificate may be issued and sent to a third party (if that was the option chosen) before processing of the application can be stopped, which could cause stress/ damage to that individual if the certificate contains sensitive information such as criminal convictions.	• DBS will publish details of expected processing times to manage an applicant's expectations and will provide an indication that most applications will be processed within the published time. Setting an unrealistically low expected processing time could generate an unnecessary high volume of enquiries and is considered to be a disproportionate response to this risk. • An applicant does not have to have their Basic certificate sent to a third party they can choose to have it sent to their own address removing the risk. • DBS provides guidance on GOV.UK on withdrawing applications.

	4. The DBS Basic application process automatically generates an electronic notification (an eResult) that gives an indication of whether or not the basic certificate discloses unspent convictions, which an RO can retrieve via a DBS web service. The original declaration by the applicant on the application has no reference to eResults nor does it capture explicit consent to allow for an RO to receive an eResult. Because there is no explicit consent captured on the basic application to allow DBS to generate an eResult and make it available to an RO, DBS would be processing the application unlawfully, which could result in DBS being fined for breach of the Data Protection Act, and suffer reputational damage. The eResult may also indicate to an RO that there are convictions disclosed on the applicant's certificate without their knowledge and/or explicit consent, which could cause damage and/or distress to the applicant (for example, an employer could make a recruitment decision purely on the basis that they believe the applicant has a conviction without seeing the conviction details). Note: DBS are not in a position to separate processing of the application for a basic check and the generation of an eResult ahead of the proposed go-live date of the service.	• DBS have amended the application declaration to include a statement that states that the applicant agrees to give consent to the Responsible Organisation receiving an electronic notification once the application has been processed which states either the 'Certificate contains no information' or 'Please wait to view applicant certificate'. • DBS have instructed the ROs that they must get explicit consent from the applicant to allow the RO to receive an eResult. • DBS will not process the basic application unless this consent is given • DBS have also included a statement within the DBS Basic Check applicant Privacy Policy, which will be published on GOV.UK, about the eResult and what the applicant can do if they still require a Basic criminal record check but do not wish to give consent for an eResult (current options Disclosure Scotland's Basic Disclosure service until 31/12/2017 or the DBS Basic Digital service, to be available January 2018).

Human Rights Act: Will your actions interfere with the right to privacy under Article 8? Have you identified the social need and aims of the project? Are your actions a proportionate response to the social need?	• An individual is required to provide DBS with details of their current and previous names to enable DBS to process their application for a DBS Basic check; for individuals who are transgender this could involve revealing details of their previous gender to a 3rd party, which they do not wish to reveal; this could interfere with their right to a private life. However without the full set of personal details DBS may not be able carry out an accurate criminal record check, which could result in criminal convictions being missed and not disclosed on the criminal conviction certificate. As it is expected that most Basic checks will be required in relation to employment if a conviction is not disclosed then it could, for example, impact on public safety. • DBS have recognised that some individuals do not wish to provide details of their previous identity/gender to a 3rd party and have in place a service that gives individuals the option to provide these details separate to the application submitted by the RO, retaining their privacy, and ensuring the application is processed with a full set of data (this is an existing service). • This is considered to be a proportionate response where the individual's privacy can be maintained and any impact on the general public can be avoided. • The purpose of a DBS Basic check is to determine if an individual has any unspent convictions, which if found will be disclosed on the applicant's basic certificate. DBS have introduced a rigorous process to identify unspent convictions to reduce the risk of confidential information, in this case spent convictions, being disclosed. Because the individual may have to share this information, with for example an employer, it is essential that DBS do not disclose information on the basic certificate that third parties are not entitled to see. DBS will be continually reviewing the process to identify spent/unspent convictions and will implement changes if required. • Similarly DBS have a rigorous process for identifying PNC matches, which if not applied correctly could lead to unspent convictions not related to the individual being disclosed on their basic certificate. • DBS require explicit consent to process a DBS Basic check and to share information. • DBS require explicit consent from the individual if they wish to allow a third party to view their electronic certificate; where consent is given on the application form, as a safeguard, the DBS system will automatically revoke consent if unspent convictions are to be disclosed

	on their certificate to give the individual the opportunity to view their certificate before they decide whether to share this sensitive information with a third party. • Where the individual has chosen to have their paper certificate sent by post to a third party's address, DBS has set out in the Basic privacy policy the possible consequences, for example the third party would be able to view any unspent convictions before the individual has had a chance to check the details for accuracy and the impact this could have on the individual. DBS recognised that a DBS Basic check is often used for recruitment purposes and that providing the individual with the option to have their certificate sent direct to a potential employer in some cases can speed up the recruitment process but respecting that some confidential information could be disclosed DBS considered it a proportionate response to set out the risks and enable the individual to make an informed decision on whether to give consent to have their certificate sent to a third party or not.

5.2. Data protection Act Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

What are the main uses of the information? Does your project plan cover all of the purposes for processing personal data?	• The information collected is used to process an application for a DBS Basic check; the main use of the data is to match against nominal personal data provided by the Police to identify a match to a PNC record. The process will generate a basic e-Certificate and a paper basic certificate, if requested. An eResult (see 3.1.3 for details) will also be generated. • DBS can also use the data it receives to perform other DBS functions linked to the original purpose for capturing the data, such as Management Information reporting. The R1 system includes the Oracle Business Intelligence Enterprise Edition (OBIEE) software which provides the capability to perform analytics and reporting on the data. • OBIEE will refresh on a daily basis and will be used operationally by DBS to monitor receipts, work in progress, certificates despatched and performance every day. It will also be used for more in-depth reporting, particular processes, for example applying Rehabilitation of Offenders rules to identify spent convictions, on research (customer behaviour, demographics etc...) and forecasting. All the data held will be subject to

<table>
<tr><td></td><td colspan="2">Freedom of Information and Parliamentary Question requests and will be subject to audit.
• No personal data used for reporting purposes, unless it has been anonymised, will be shared.
• Project documentation covers all the purposes for processing personal data.</td></tr>
<tr><td>Have you identified potential new purposes as the scope of the project expands?</td><td colspan="2">Basic Applicant
• The information has been collected for processing an application for a DBS Basic check and associated purposes, such as producing an eResult and an e-Certificate, and reporting. No new purposes have been identified.

Accountable Officer
• The personal information has been collected to process a DBS Basic check to determine the suitability of the individual to be an Accountable Officer. No new purposes have been identified.</td></tr>
<tr><td rowspan="2">Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?</td><td>Risks</td><td>Mitigation</td></tr>
<tr><td>5. There is a risk that sensitive information could be disclosed on a basic certificate revealing details of applicant’s previous identity and gender because the certificate was sent to a third party; ‘outing’ the applicant (Where an applicant was convicted of an offence under their previous name/identity if this offence is unspent it would appear on their basic certificate against their previous name).</td><td>• The applicant can opt to use the DBS sensitive application process for transgender applicants that minimises the risk of ‘outing’ the applicant because a case can be identified and the certificate examined and edited, if necessary, before it is despatched. Details of this service are published on the GOV.UK website.
• The applicant can choose to have the certificate sent to their own address rather than a third party, which will allow them to examine the certificate first and have it amended if necessary.</td></tr>
</table>

	6. There is a risk that sensitive information could be disclosed to a third party via a telephone enquiry revealing details of applicant's previous identity and gender; 'outing' the applicant.	• TCS call centre staff follow the TCS Telephone Security Guidance Questions (TSQ) to verify the identity of the caller. They are trained to answer only general telephone queries and will not divulge any information to the caller regarding a case or application. If they are unable to answer a query, they will transfer the call to the onsite DBS Helpline Team, who follow the DBS TSQ before answering any telephone queries.
	7. There is a risk that an incorrect match to a record on PNC is made resulting in a conviction not related to the applicant being disclosed to a third party on their basic certificate. Note: redress could result if it is found that DBS did not follow the correct procedures when making an incorrect match.	• DBS will be using IBM InfoSphere MDM (Master Data Management) a proven matching algorithm to identify possible matches to PNC. No automatic matches will be made. Possible matches can be rejected based on score (high scores more likely to be correct matches). All confirmed matches will involve manual intervention and confirmation. • Selected confirmed matches will be subject to DBS Quality Assurance (QA) checks. • When DBS are unable to confirm a match an applicant can be referred to a Police Station to provide fingerprints, which confirms or eliminates a possible match (this information is retained on the applicant's DBS Profile and will help prevent incorrect PNC matches on future applications for DBS checks). • DBS have a well established disputes process in place to enable an applicant to challenge an incorrect match. • The number of incorrect PNC matches identified using the existing matching algorithm

		equates to less than 0.007% of applications (which would equate to approximately 120 per year of Basic applications out of approximately 1.7 million applications)
	8. There is a risk that spent convictions (sensitive information) are disclosed in error on an applicant's Basic certificate due to rules set out in the Rehabilitation of Offenders (ROA) Act 1974 being applied incorrectly by DBS and this information is then presented to an individual's employer revealing information they are not entitled to see. Note: redress could result if it is found that DBS did not follow the correct procedures when applying ROA rules and it resulted in spent convictions being disclosed.	• System will identify a specific set of spent convictions and determine what will be disclosed on the DBS certificate; automatic system decisions are straight forward, low complexity. • More complex decisions to determine whether or not a conviction should be disclosed will be referred for manual intervention. • Procedures for carrying out manual removal of convictions in line with the Rehabilitation of Offenders (ROA) Act 1974 have been produced. • All cases requiring manual intervention will be subject to 100% Quality Assurance (QA). • Testing on the automatic decision making to identify spent/ unspent convictions had a 100% success rate

	9. There is a risk that a basic application could be submitted unlawfully in an applicant's name without their consent and/or knowledge, which could result in sensitive information e.g. convictions being disclosed to a third party. **Note:** an RO could have the applicant's employer as a client and the employer has sufficient personal data to submit a valid application without the applicant's consent or knowledge. And as the address to which the basic certificate is sent does not have to be the applicant's, the applicant may not find out about the application.	• An RO is responsible for validating application data and ensuring that the applicant's identity has been verified in accordance with the DBS ID checking guidelines and that consent has been received from the applicant. • Any breach of the terms and conditions of becoming an RO could result in the suspension or cancellation of an organisation's registration and/or the registration of the Accountable Officer, • In exceptional circumstances the Accountable Officer could be prosecuted (under Section 123 of the Police Act 1997 a person commits an offence if he or she Knowingly makes a false statement for the purpose of obtaining, or enabling another person to obtain, a Certificate), • Applications submitted without the consent of the individual could breach the Data Protection Act and lead to the RO being fined by the Information Commissioners Office (ICO) • If an applicant's mobile phone number has been provided on their application and they have agreed to receive SMS messages from DBS the applicant will be sent an SMS message when their application has been received by DBS (an SMS message is also issued when the certificate is issued). • If an applicant has a DBS online account when their application is submitted a notification will be sent to their account when their application is received by DBS (On day 1 very few, if any,

		applicants will have a DBS online account and so as mitigation this will have a greater impact as time moves on and more applicants have DBS online accounts). • After a Basic certificate has been issued the applicant will be either be sent a notification to their DBS online account informing them that their certificate has been issued or if they do not have a DBS online account a letter will be sent to their home address, which will alert them to the fact that they have recently applied for a DBS check. If the individual hasn't submitted a DBS check they will be able to contact DBS to investigate. This mitigation is intended as a deterrent to ROs who might consider submitting applications without the applicant's knowledge – the applicant will be notified and find out. • DBS will be carrying out compliance checks, which will include checks to confirm that an individual has given consent for a DBS Basic check being submitted in their name

	10. A variation of risk 9 The applicant may have given consent for a basic application to be processed but did not give consent for the RO to view their electronic basic certificate and so there is a risk that entries on the application form could been changed unlawfully or inadvertently before submission to DBS to allow a third party to view sensitive personal data without the applicant's knowledge or consent.	• The mitigation that describes the actions that could be taken against an RO in risk 9 also applies here. • If there are convictions/ cautions to disclose on a basic certificate the DBS system automatically revokes consent and so the RO lead contact and/or third party will not be able to view the applicant's electronic certificate (neither party are notified that consent has been revoked). The applicant will be notified that consent has been revoked and will be advised that if they wish to reinstate consent they can do so via their DBS online account. • An applicant can remove consent via their DBS online account (if they have a DBS online account when their application was submitted consent can be removed as soon as the certificate is issued, otherwise they would need to create a DBS online account after their they have been notified that their certificate has been issued). • If there are no convictions to disclose on the basic certificate consent will not be revoked and the RO lead contact and/or third party could view the electronic certificate online via their own DBS online account (no more personal information can be viewed on the electronic certificate than would appear within an eResult). An applicant can still remove consent if they wish via their DBS online account. • Because consent to view an electronic certificate can be automatically revoked or

		removed by the applicant (and in both cases the recipient of consent is not notified), not being able to view an electronic certificate does not infer that there are convictions/ cautions disclosed on the certificate. • An applicant can view details of their basic application via their DBS online account and will be able to check what application data was submitted and if anything has been changed

5.3. Data protection Act Principle 3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	
Is the quality of the information good enough for the purposes it is used?	• The information collected is validated by the Responsible Organisation who must ensure the data submitted to DBS meets DBS's data requirements (applications will be rejected by DBS if validation fails). • DBS provide web service specification documents that set out in detail data requirements. • The Responsible Organisation is also responsible for verifying the individual's identity by examining relevant identity documents that should help to ensure quality of information. • DBS request a minimum set of personal information to process a DBS Basic check
Which personal data could you not use, without compromising the needs of the project?	• No personal data collected will be used for purposes outside the needs of the project.

5.4. Data protection Act Principle 4 Personal data shall be accurate and, where necessary, kept up to date.	
If you are procuring new software does it allow you to amend data when necessary?	• New software has been procured and it allows DBS to amend data when necessary.
How are you ensuring that personal data obtained from individuals or other organisations is accurate?	**Basic Applicant** • Organisations can only submit DBS Basic checks after they have successfully completed the DBS registration process and agree to specific Terms and Conditions, signed up to Data Processing agreements and satisfied our security requirements. • Responsible Organisations must verify the identity of all individuals (applicants) by examining specific identity documents (as set out in DBS guidance) and must ensure that the personal application data submitted is valid and satisfies all DBS's data requirements. • Personal data submitted to DBS by organisations via the new 'submit application' web service must pass all data validation or the application will be rejected. • DBS provide ROs with details of data requirements within a web service specification document. • Failure to comply with DBS's Terms and Conditions, Interchange Agreement etc. can result in that organisation's registration being suspended or cancelled. **Accountable Officer** • Accountable Officers will be required to apply for a DBS Basic check to enable DBS to determine their suitability to be an Accountable Officer; they can apply for a DBS Basic

	check via another Responsible Organisation (see section on Basic Applicant above) or via the DBS Basic Digital service (an online self-service channel for submitting basic applications). In both cases personal data provided is validated. • In addition, Accountable Officers that submit their DBS Basic check via a Responsible Organisation or via the DBS Basic Digital service where their identity has been verified by the Post Office will be required to send DBS a set of identity documents with their basic certificate, which will be used to confirm their identity and check the accuracy of personal data provided (The minimum document set that can be used to confirm a basic applicant's identity by the Post Office or by a Responsible Organisation is not to the level required by DBS to confirm the identity of an Accountable Officer as per the Responsible Organisation registration process hence the requirement for acceptable identity documents to be sent to DBS). • Accountable Officers that use the DBS Basic Digital service who have their identity verified by GOV.UK Verify (a Government identity checking service) will not have to send DBS any identity documents with their basic certificate because the identity check carried out by GOV.UK Verify on the Accountable Officer is at the level required by DBS as per the Responsible Organisation registration process. After verifying a Basic applicant's identity GOV.UK Verify pre-populates some of the personal data on the online Basic check application form (current name, date of birth and current address), which cannot be amended or deleted by the applicant. This ensures that the application submitted contains the personal data of the person whose identity was checked and contributes to the accuracy of the personal data collected.

5.5. Data protection Act Principle 5 Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.	

What retention periods are suitable for the personal data you will be processing?	**Basic Applicant**
	
	• Subject to Home Office embargo on deleting data, DBS have a Data Retention Policy that sets out retention periods for the DBS checks:
	
	  ○ Where an application has been processed and no conviction information was found the personal data is retained for 7 years;
	
	  ○ Where an application has been processed and conviction information is found the personal data is retained for 15 years.
	
	• Due to the Home Office embargo on deleting data no records that have reached their deletion date can be deleted. In the meantime DBS are exploring options to place this information out of operational use whilst the embargo is in place.
	
	• Most of the personal data held on the current DBS systems and earmarked for migration to the new R1 system will not be migrated until DBS Standard and Enhanced checks move to the R1 solution (date yet to be decided). And so it is expected that in most cases on day 1 of the new DBS Basic check service new DBS Profiles will be created and all will have a minimum of 7 years retention period.
	
	• Data retention periods and the DBS Data Retention policy are reviewed at the least annually. The introduction of General Data Protection Regulation (GDPR) in 2018 may also impact on our Data Retention Policy.

	Accountable Officer • In relation to the DBS Basic check submitted by the Accountable Officer, which is used by DBS to determine their suitability, see section Basic Applicant above. • Accountable Officer personal data held on the Responsible Organisation's DBS Profile will be retained whilst the Responsible Organisation's registration is active. If the registration is cancelled data will be retained for the period set out in the DBS Data Retention policy (subject to Home Office embargo on deleting data).
Are you procuring software that will allow you to delete information in line with your retention periods?	• The new R1 system will have software that will automatically delete information once it reaches its retention period, other information will be reviewed. Due to the current Home Office embargo on deleting data the automatic deletion of information has been put on hold.
Is the information deleted in a secure manner which is compliant with HMG policies once the retention period is over? If so, how?	• The DBS aligns to Home Office standards for retention and disposal of records. These standards apply to all formats of records, including but not restricted to paper, digital, audio and video tapes, films, DVDs and CD ROMs. These schedules shows the point at which particular types of records should be either reviewed to determine if there is an ongoing business need to retain it, preserved for historical value or be destroyed. Due to various ongoing inquiries there is a moratorium on the destruction of all information held by the Home Office group which includes DBS. As such, no paper files, including case files, or digital information held by the department may be destroyed. This moratorium is in place until further notice.
What are the risks associated with how long data is retained and how they might be mitigated?	Any potential risks related to how long data is retained will be investigated in full within the R1 Standard and Enhanced DBS checks PIA when specific personal data from the current DBS IT system will be migrated to the new IT system, some of which will be associated and linked to basic applicants.

5.6. Data protection Act Principle 6 Personal data shall be processed in accordance with the rights of data subjects under this Act.	
Will the systems you are putting in place allow you to respond to subject access requests more easily?	• Yes, the new system will provide functionality that will automatically gather all relevant data and provides an inbuilt document management tool that allows DBS to respond to subject access requests.

5.7. Data protection Act Principle 7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	
Who will have access to the system? Please provide role and responsibilities.	• The new system introduces a more rigorous Role Based Access Controls (RBACs) that will ensure that access is restricted to only the functionality, records and personal data that the user needs to fulfil their role. • User access is restricted to only allow users to view case records and/or activities they have been allocated to and are within their workload. It is further restricted to only allow users to access screens within the case records relevant to their role. Some of this access is also restricted to read-only access if that is required. • All access to records is audited and must be for a legitimate business reason. DBS also have access assurance checks in place to monitor record access. • Only Managers defined within the RBACs hierarchy will be able to view their team's workloads. • The audit history of a case is also restricted; only managers can view. • Full access will be limited to Super-user type roles that will have the relevant security clearance and are very limited numbers. • The R1 system also allows users to 'discount' themselves from being allocated specific cases. This is used where there is a potential conflict of interest between the user and the

	subject of a case (e.g. family member, friend, neighbour etc). **TCS System Users** • TCS Back Office and Contact Centre who will deal with first line enquiries from service users either by telephone or by white mail/scanned images will be covered under the TCS RBACs.
What level of security clearance is required to gain access to the system?	• All DBS staff who have access to the data, are subject to a minimum of Baseline Personnel Security Standard (BPSS) security clearance. • All DBS Live PNC users will also need to have NPPV (Non Police Personal Vetting) level 2 clearance, which is a higher level of security clearance to that in place currently. • All TCS staff will either hold Baseline or Security Check (SC) clearance depending on their role and responsibilities.
Does the system use 'roles' to assign privileges to users of the system?	Yes
How is access granted to the system?	• Access to the system is granted by means of a request to TCS to create a user account and password. • The request is raised by a DBS line manager and also goes to DBS Security for approval. • The line manager will request the appropriate role for the individual from within the RBAC, which will control the level of access to the system. • A line manager can request a change of role (within the existing RBAC) for a staff member and this is subject to approval in the usual DBS hierarchy. • A user can only be allocated one role in Siebel (DBS's new Customer Relationship Management system) at any time.
How are the actual assignments of roles and rules verified?	• All the roles in the RBACS have been approved by DBS security. • If a new role is being created then DBS security are part of the approval process
How is this data logged and how is this reported to prevent misuse of data?	• DBS will provide TCS with a list of all users/roles ready for go live, after which the information will be stored in Seibel but only accessible (via a report) to those DBS staff who require it.

	• A full audit trial is available from Siebel (DBS's new Customer Relationship Management system) of users and which records have been accessed.

What training is provided to cover appropriate use and basic security to users? How is the training refreshed? Is the training tiered?	• All DBS staff undertake annual mandatory 'Responsible for Information, General User' training, which is designed for anyone who handles information and needs to share and protect it, it also covers the government security classifications and introduces aspects of fraud and bribery, it is also supported by an annual face-to-face briefing at work. There are also a number of tiered training sessions for other types of user; ;
	• DBS security and the Information Governance Officer produce, for all users, reactive ad hoc security messages where security issues have been identified and proactive ad hoc security messages to reinforce best practice (for example, Golden Rules for Handling data);
	• DBS also produce a number of policies and procedures that are regularly shared with all users to ensure their knowledge is refreshed, they include but are not limited to:
	  • Information Security Incident Management Policy
	  • User Security Operating Procedure
	  • User Security Incident Handling procedures
	  • TCS Acceptable Use Policy
	  • DBS Acceptable Use Policy
	  • Password Policy

Has or is the system going to be formally accredited using HMG standards to process and store the information, if so who is the accreditation authority (person/organisation)?	• Yes, the system will be formally accredited using HMG standards to process and store the information. • DBS is the accreditation authority and the accreditation will be carried out by the DBS Senior Accreditor. • The solution has also been subject to independent NCSC (National Security Cyber Centre – the government's technical security authority) assessment. • The system has also been subject to extensive external penetration testing by approved providers under the CHECK ITHC (IT Health Check) scheme.
Given access and security controls, what privacy risks were identified and how might they be mitigated?	• DBS agents will be restricted to only the functionality, records and data relevant to their job. The Role Based Access Controls (RBACs) are used to manage access to the appropriate functionality – no privacy risks were identified. • A comprehensive set of security risks and mitigations are captured within the solutions Risk Management and Accreditation Document Set (RMADS), which will be signed off and

	approved by the DBS Accreditor and DBS Senior Risk Owner (SIRO) prior to service go live.

5.8. Data protection Act Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?	**No**
If you will be making transfers, how will you ensure that the data is adequately protected?	**N/A**

5.9. Internal sharing within the Home Office

With which parts of the Home Office is the information shared, what information is shared and for what purpose?	**None of the data collected for a DBS Basic check is shared with the Home Office.**
How is the information processed or disclosed?	**Not applicable**
What are the privacy risks associated with internal sharing within the Home Office and how they might be	**None identified**

mitigated?	

5.10. External sharing and disclosure **(If you have already completed a DBS Data sharing toolkit then please attach and leave these questions blank).**	
With which external organisation(s) is the information shared, what information is shared, and for what purpose? Has DBS specifically asked suppliers to undertake PIAs?	**Police** • During the Basic application process DBS may not be able to resolve a possible match to a PNC record. In these circumstances DBS can refer applicants to the Police to have their fingerprints taken to resolve the possible match. • This an existing and well established process that requires the consent of the individual who will be required to visit a local police force to have their fingerprints taken. • The individual must also provide DBS with a passport size photo, which will be scanned and will form part of an electronic notification to the local police force. • The individual's name, date of birth and addresses within the last 5 years will be shared with the police. • The police will access notifications via an intranet DBS online account. The police arrange the fingerprint appointment with the individual. • The police record the results of the fingerprinting within their intranet DBS online account (result could confirm a match to the PNC record, or possibly a match to a different PNC record or that there is no match to a PNC record). • If an applicant fails to give consent or fails to provide fingerprints their application will be withdrawn. • DBS have not asked the Police to undertake a PIA. **Responsible Organisations**

	• The RO captures all the Basic application data (see Appendix A) from the individual and passes this information to DBS via the DBS Submit Disclosure Application web service for DBS to process the DBS Basic check. If the application passes validation DBS will return a unique application reference number together with an RO unique reference (that is used by the RO to link the information to the application held on their system), no personal data is returned by DBS. • The RO can check the status (the progress) of any Basic applications they have submitted via the DBS Check Application Status web service. The RO must share the application reference number, date of birth and surname for each application they wish to check the status (this information has already been shared with DBS when the Basic application was submitted). DBS will return the status of the application together with application reference number, date of birth and surname, as provided in the request from the RO; no additional personal information is shared with the RO. • When a Basic application has been processed DBS generate an eResult that the RO can retrieve via the DBS Get Application Result web service. The request by the RO for an eResult requires only the application reference number; the request contains no personal data. The eResult provided by DBS includes the applicant's forename(s), surname, date of birth, place of birth (town and country), gender and address (all these personal details will have been provided by the RO when the Basic application was submitted) and an indication of the result of the check; a blank response indicates that the certificate contains no unspent convictions or alternatively the RO is advised to wait to view the certificate; no sensitive information is returned within the eResult. The eResult also includes a unique certificate number, which can be used to confirm that the correct certificate is presented if the RO needs to view it.
Is the sharing of personal information outside the DBS compatible with the original collection? If so, is it addressed in a data-sharing agreement? If so, please describe.	**Police** • Sharing information with Police is compatible with the original collection of data, that is, to determine whether or not the individual has any criminal convictions. • DBS have a Service Level Agreement (SLA) with the Police, the NPCC DBS Police SLA that sets out the Police fingerprinting requirements. • DBS has appropriate data sharing and interchange agreements with the police to process and exchange information.

	• Information exchange with the Police will be over the Protected Public Service Network (PSN), which is subject to HMG accreditation and restricted to a predominantly government community. **Responsible Organisations** • All information shared with the RO is solely related to the reason for the original collection, which is to process a DBS Basic check. • DBS Terms & Conditions and an Interchange Agreement, which defines and documents the agreement between the DBS and ROs using the DBS web services with respect to each RO's use of, and the DBS's provision of, the DBS web services (data is shared via the web services).
How is personal information shared outside DBS and what security measures, compliance and governance issued safeguard its transmission?	**Police** • The information is shared via an intranet DBS online account that enables the Police to receive and send information to DBS. **Responsible Organisations** • Information is shared via the DBS web services (See Appendix B for web service security features and measures).
Is a MoU in place for the DBS to verify that an external organisation has adequate security controls in place to safeguard information?	**Police** • DBS have a well established working relationship with the Police that will not change due to the implementation of this project; the existing MoU still applies. **Responsible Organisations** • Must sign up to DBS Terms and Conditions, which specifies minimum security standards and the need for compliance with the Data Protection Act 1998 in handling information; • DBS also require the RO to sign up to an Interchange Agreement, which defines and documents the agreement between the DBS and ROs using the DBS web services with respect to each RO's use of, and the DBS's provision of, the DBS web services; • DBS also have an MoU for public sector ROs and a separate Deed for private sector ROs, which private sector ROs must sign-up to (each of these documents is referenced within the Interchange Agreement);

Given the external sharing, what are the privacy risks and how might they be mitigated?	**No additional privacy risks have been identified.**

5.11. Notice	
Do individuals have an opportunity and/or right to decline to disclose or share information?	**Basic Applicant** • DBS require all the application personal information to process the DBS check. If an applicant declines to disclose or share this information DBS will not process the application. • To submit a DBS Basic check via a Responsible Organisation the individual should provide that organisation with all the relevant personal application data however the individual does have an option to provide sensitive information separately to DBS using the DBS sensitive application process (this allows transgender applicants to provide details of their previous identity direct to DBS rather than having to reveal this information to the organisation). • DBS also provide a separate Basic Digital service (an online self-service Basic application service) that allows an individual to submit their application without the involvement of a Responsible Organisation. • After processing an application no specific information will be shared with an organisation unless the individual has provided consent. • The Basic certificate is sent by post to the individual's current home address unless the individual has specified on their Basic check application that the certificate is sent to an alternative address or to a 3rd party address, for example their employer. • No other sharing of information occurs. **Accountable Officer** • For an organisation to register with DBS as a Responsible Organisation, DBS require personal information from the Accountable Officer to enable DBS to determine their suitability by carrying out PNC checks. This is set out in the RO Terms and Conditions.

	• If the Accountable Officer declines to disclose or share information, which is their right, then they may not be able to hold the position of Accountable Officer and a replacement may be required.
Do individuals have an opportunity to consent to particular uses of the information, and how?	**Basic Applicant** • DBS cannot process the application without the individual's consent. • There is a 'Declaration by Applicant' on the form submitted by the RO confirming that they have read and understood the DBS Privacy notice. • The Privacy notice explains that the information provided will be used to identify possible matches to PNC records. **Accountable Officer** • A privacy notice that contains details of how their information will be used and a declaration that they agree to ID and criminal record checks being carried out is included on the application to become an Accountable Officer. • The DBS form on which the Accountable Officer provides their personal details will also capture their consent and make it clear what they are consenting to, that is an initial PNC record check followed by continuous regular PNC record checks throughout their time as an Accountable Officer.
How could risks associated with individuals being unaware of the collection be mitigated?	• The purpose for which the data is collected is clearly defined within the relevant Privacy notice. • The individual provides the personal data for the sole purpose of applying for a Basic criminal record check – no other data is collected that the individual would be unaware of. • DBS also have a Privacy policy published on GOV.UK that provides more details on how DBS use data. **No additional risks have been identified**

5.12. Access, Redress and Correction.	
How are individuals notified of the procedures for correcting their information?	• The Basic certificate provides information on how to get information on the certificate corrected if errors are identified. The notice also provides DBS contact details and where to find other relevant guidance, such as the DBS disputes process. • The DBS Home page on GOV.UK provides details on how to dispute information on their DBS certificate. • DBS have a Complaints Policy that incorporates the DBS Redress Policy – redress can only be considered if maladministration by DBS is identified.
If no formal redress is provided, what alternatives are available to the individual?	**Not applicable**
What are the privacy risks associated with redress and how might they be mitigated?	DBS will consider redress if maladministration is identified. Several risks have already been identified that may result in redress if it is found that DBS failed to follow their own procedures, they include: • If sensitive data concerning an individual's gender identity (details of their previous gender) are disclosed to a third party, which would be handled via DBS complaints procedures, this could lead to compensation payments. • If an incorrect match has been made to a PNC record and then incorrect conviction information is disclosed on the basic certificate and DBS had failed to follow their own procedures in making an incorrect match this could lead to compensation payments. • If spent convictions are incorrectly disclosed on a basic certificate, which could result in a third party, such as an employer, being able to see information that they are not entitled to see. This could lead to compensation payments. **Each of these risks and how they may be mitigated have been identified under other DPA principles where they are covered in more detail (see risks 5, 7 and 8 respectively in the next section for details).**

6. PRIVACY RISKS AND EVALUATION

This section evaluates each of the identified risks and determines whether the risk has been eliminated, reduced or accepted. Where considered necessary recommendations have been made.

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
1	There is a risk that personal data provided by the applicant could be lost, tampered with and/or misused (for example identity theft) when transferred from the RO System to DBS via a web service.	DBS will be deploying web service security features, as recommended by the National Cyber Security Centre (NCSC), that ensures only known users (ROs) can access the web services and ensures that no third party can eavesdrop or tamper with any message sent between the RO and DBS (more details on web service security features can be found in Appendix B)	No recommendations	Reduced	The impact on the individual should be minimal because DBS have implemented a secure mechanism for transferring personal data from the RO to DBS. It is accepted that this risk cannot be eliminated because of the speed of change of Technology but the system implemented does minimise the risk.
2	The original design for the Basic application form included the question 'Have you any unspent convictions? Because an		**Solution:** Decision was made to remove this question from the Basic	Eliminated	Removal of the question has eliminated the risk.

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
	applicant may be unsure whether any convictions they have had are spent or unspent they could inadvertently alert a potential employer of a previous spent conviction by answering 'Yes' to the question. Whilst the spent convictions would not be disclosed on their basic certificate the employer could discover that their employee has had a conviction, which they had no entitlement to know about, causing potential stress and/or damage to the applicant. **Note:** As an alternative, if the applicant answered 'No' to the question because they thought their convictions were spent and a conviction was disclosed on their Basic certificate an employer may believe that the individual was dishonest because they failed to declare they had an unspent conviction, which could cause potential stress and/or damage to the		application form on the grounds that the information was not required to process the application and because user research had shown that this question was confusing for some and for others it was not possible to answer the question correctly. **Note**: a question about previous convictions has also been removed from the Accountable Officer application form on the same grounds, although the risk was considerably less because no certificate is issued.		

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
	applicant.				
3	After an application has been received by DBS an individual can withdraw their consent to have their application processed, but because it is expected that many applications will be processed quickly (some could be less than a day) a Basic certificate may be issued and sent to a third party (if that was the option chosen by the applicant) before processing of the application can be stopped, which could cause stress/ damage to that individual if the certificate contains sensitive information such as criminal convictions.	• DBS will publish details of expected processing times to manage an applicant's expectations and will provide an indication that most applications will be processed within the published time. Setting an unrealistically low expected processing time could generate an unnecessary high volume of enquiries and is considered to be a disproportionate response to this risk. • An applicant does not have to have their Basic certificate sent to a third party they can choose to have it sent to their own address removing the risk. • DBS provides guidance on GOV.UK on withdrawing applications.	None	Reduced	DBS do provide the facility for applicants to withdraw consent to have their application processed but at the same time DBS are aiming to provide a quick and efficient service, which may limit the time available to withdraw consent and stop applications being processed. It is considered that there is sufficient mitigation to reduce this risk.
4	The DBS Basic application process automatically generates an electronic notification (an eResult) that	• DBS have amended the application declaration to include a statement that states that the applicant	Recommendation 1: DBS should consider separating the processing of a basic	Reduced	The changes to the applicant's declaration to include reference to

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
	gives an indication of whether or not the basic certificate discloses unspent convictions, which an RO can retrieve via a DBS web service. The original declaration by the applicant on the application has no reference to eResults nor does it capture explicit consent to allow for an RO to receive an eResult. Because there is no explicit consent captured on the basic application to allow DBS to generate an eResult and make it available to an RO, DBS would be processing the application unlawfully, which could result in DBS being fined for breach of the Data Protection Act, and suffer reputational damage. The eResult may also indicate to an RO that there are convictions disclosed on the applicant's certificate without their knowledge	agrees to give consent to the Responsible Organisation receiving an electronic notification once the application has been processed which states either the 'Certificate contains no information' or 'Please wait to view applicant certificate'. • DBS have instructed the ROs that they must get explicit consent from the applicant to allow the RO to receive an eResult. • DBS will not process the basic application unless this consent is given • DBS have also included a statement within the DBS Basic Check applicant Privacy Policy about the eResult and what the applicant can do if they still require a Basic criminal record check but do not wish to give consent for an eResult (current options Disclosure Scotland's Basic Disclosure service until	application from an eResult; this would allow an applicant to have their basic application processed without the RO receiving an eResult; the applicant could provide separate explicit consent if they wished for the RO to receive an eResult. Note: Under GDPR where consent is to be more clearly defined, the likelihood is that consent would be invalidated if a single consent is used for both eResults and processing the basic application.		the electronic notifications (eResults) and the inclusion of details within the Basic applicant privacy policy should (1) make the applicant aware that an eResult is produced and (2) allows the applicant to make an informed decision on whether to permit the RO to receive an eResult. Whilst the changes and other mitigation is considered sufficient to reduce the risk at present the changes to be introduced by GDPR in 2018 are likely to require DBS to make changes to meet these new requirements.

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
	and/or explicit consent, which could cause damage and/or distress to the applicant (for example, an employer could make a recruitment decision purely on the basis that the applicant has a conviction without seeing the conviction details). Note: DBS are not in a position to separate processing of the application for a basic check and the generation of an eResult ahead of the proposed go-live date of the service.	31/12/2017 or the DBS Basic Digital service, to be available January 2018).			
5	There is a risk that sensitive information could be disclosed on a basic certificate revealing details of applicant's previous identity and gender because the certificate was sent to a third party; 'outing' the applicant (Where an applicant was convicted of an offence under their previous name/identity if this offence is unspent it would appear	• The applicant can opt to use the DBS sensitive application process for transgender applicants that minimises the risk of 'outing' the applicant because a case can be identified and the certificate examined and edited, if necessary, before it is despatched. Details of this service are published on	None	Reduced	For the expected number of applications for which this risk may apply, it is considered that DBS have provided a more than a proportionate response to address this risk and reduce the impact on the

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
	on their basic certificate against their previous name). **Note:** this could lead to redress if DBS receive a complaint and maladministration is identified.	the GOV.UK website. • The applicant can choose to have the certificate sent to their own address rather than a third party, which will allow them to examine the certificate first and have it amended if necessary. • The applicant can choose to use the DBS digital basic application service where no application data is shared with a third party and they can choose to have the certificate delivered to their own address. • The number of transgender applicants that chose to use the DBS sensitive application service in 2016 was 376, which equated to less than 0.01% of total applications, and of these only (approximately) 10% matched to Police information (there is no information on how many of these were convictions under their previous			applicant. In turn the likelihood of this risk resulting in redress is minimised.

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
		identity). This would equate to approximately 170 Basic applicants using the sensitive application service per year out of 1.7 million.			
6	There is a risk that sensitive information could be disclosed to a third party via a telephone enquiry revealing details of applicant's previous identity and gender; 'outing' the applicant.	• TCS call centre staff follow the TCS Telephone Security Guidance Questions (TSQ) to verify the identity of the caller. They are trained to answer only general telephone queries and will not divulge any information to the caller regarding a case or application. If they are unable to answer a query, they will transfer the call to the onsite DBS Helpline Team, who follow the DBS TSQ before answering any telephone queries. • When a transgender applicant uses the DBS sensitive application service their DBS profile will be flagged to show that this is a 'sensitive' record, which will alert TCS and DBS users.		Reduced	DBS have put in place procedures that if followed correctly should minimise the risk and any impact on the applicant. With transgender applicants forming less than 0.01% of DBS applicants it is considered that DBS have provided a more than a proportionate response to address this risk.

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
7	There is a risk that an incorrect match to a record on PNC is made resulting in a conviction not related to the applicant being disclosed to a third party on their basic certificate. **Note:** redress could result if it is found that DBS did not follow the correct procedures when making an incorrect match.	• DBS will be using IBM InfoSphere MDM (Master Data Management) a proven matching algorithm to identify possible matches to PNC. No automatic matches will be made. Possible matches can be rejected based on score (high scores more likely to be correct matches). All confirmed matches will involve manual intervention and confirmation. • Selected confirmed matches will be subject to DBS Quality Assurance (QA) checks. • When DBS are unable to confirm a match an applicant can be referred to a Police Station to provide fingerprints, which confirms or eliminates a possible match (this information is retained on the applicant's DBS Profile and will help prevent incorrect PNC matches on future applications for DBS	No Recommendations	Reduced	There is a low probability of an incorrect PNC match (less than 0.007% of applications currently) however due to the introduction of a new matching algorithm DBS have taken steps to minimise the likelihood of such a match occurring by introducing manual intervention before a match is confirmed. In conjunction with other processes in place, which help to mitigate the risk, it is considered that DBS have provided a more than a proportionate response to address and reduce this risk and the impact on the applicant. With well established

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
		checks). • DBS have a well established disputes process in place to enable an applicant to challenge an incorrect match. • The number of incorrect PNC matches identified using the existing matching algorithm equates to less than 0.007% of applications (which would equate to approximately 120 per year of Basic applications out of approximately 1.7 million applications)			procedures in place together with the DBS checking regime the likelihood of this risk resulting in redress is mitigated and minimised.
8	There is a risk that spent convictions (sensitive information) are disclosed in error on an applicant's Basic certificate due to rules set out in the Rehabilitation of Offenders (ROA) Act 1974 being applied incorrectly by DBS and this information is then presented to an individual's employer revealing information they are not entitled to see.	• System will identify a specific set of spent convictions and determine what will be disclosed on the DBS certificate; automatic system decisions are straight forward, low complexity. • More complex decisions to determine whether or not a conviction should be disclosed will be referred for manual intervention.	No recommendations	Reduced	DBS have put a number of processes in place to help ensure that spent convictions are correctly identified. It is expected that about 4% of applications (approximately 70,000 cases) will require intervention to identify spent convictions.

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
	Note: redress could result if it is found that DBS did not follow the correct procedures when applying ROA rules and it resulted in spent convictions being disclosed.	• Procedures for carrying out manual removal of convictions in line with the Rehabilitation of Offenders (ROA) Act 1974 have been produced. • All cases requiring manual intervention will be subject to 100% Quality Assurance (QA). • Testing on the automatic decision making to identify spent/ unspent convictions had a 100% success rate			Because this is a new process DBS have adopted a risk averse approach, which will be reviewed as part of continuous evaluation of the process. It is considered that DBS have applied a more than proportionate response to reducing this risk and minimising the impact on the applicant. With the risk averse approach adopted by DBS the likelihood of redress arising is considered minimal.
9	There is a risk that a basic application could be submitted unlawfully in an applicant's name without their consent and/or knowledge, which could	• An RO is responsible for validating application data and ensuring that the applicant's identity has been verified in accordance with the DBS ID checking	Recommendation: A notification should be sent to all applicants when DBS receive a valid basic	Reduced	It is considered that there is sufficient mitigation to minimise this risk. The impact on the RO could be

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
	result in sensitive information e.g. convictions being disclosed to a third party. **Note:** an RO could have the applicant's employer as a client and the employer has sufficient personal data to submit a valid application without the applicant's consent or knowledge. And as the address to which the basic certificate is sent does not have to be the applicant's, the applicant may be unaware that an application has been submitted in their name.	guidelines and that consent has been received from the applicant. • Any breach of the terms and conditions of becoming an RO could result in the suspension or cancellation of an organisation's registration and/or the registration of the Accountable Officer, • In exceptional circumstances the Accountable Officer could be prosecuted (under Section 123 of the Police Act 1997 a person commits an offence if he or she Knowingly makes a false statement for the purpose of obtaining, or enabling another person to obtain, a Certificate), • Applications submitted without the consent of the individual could breach the Data Protection Act and lead to the RO being fined by the Information Commissioners Office	application		considerable; registration cancelled, fines imposed by the ICO and/or possible prosecution if applications were submitted without the consent or knowledge of the applicant. With the different notifications that are issued to the applicant the likelihood of them being unaware that a Basic check has been submitted in their name is further diminished. The main gap identified is that the applicant is not always notified when DBS have received a basic application for processing, which the recommendation should address. Whilst the risk is not eliminated it is

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
		(ICO) • If an applicant's mobile phone number has been provided on their application and they have agreed to receive SMS messages from DBS the applicant will be sent an SMS message when their application has been received by DBS (an SMS message is also issued when the certificate is issued). • If an applicant has a DBS online account when their application is submitted a notification will be sent to their account when their application is received by DBS (On day 1 very few, if any, applicants will have a DBS online account and so as mitigation this will have a greater impact as time moves on and more applicants have DBS online accounts). • After a Basic certificate has been issued the applicant			reduced considerably.

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
		will be either be sent a notification to their DBS online account informing them that their certificate has been issued or if they do not have a DBS online account a letter will be sent to their home address, which will alert them to the fact that they have recently applied for a DBS check. If the individual hasn't submitted a DBS check they will be able to contact DBS to investigate. This mitigation is intended as a deterrent to ROs who might consider submitting applications without the applicant's knowledge – the applicant will be notified and find out. • DBS will be carrying out compliance checks, which will include checks to confirm that an individual has given consent for a DBS Basic check being submitted in their name			
10	A variation of risk 9	• The mitigation that	Recommendation 1:	Reduced	It is considered that

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
	The applicant may have given consent for a basic application to be processed but did not give consent for the RO to view their electronic basic certificate and so there is a risk that entries on the application form could been changed unlawfully or inadvertently before submission to DBS to allow a third party to view sensitive personal data without the applicant's knowledge or consent.	describes the actions that could be taken against an RO in risk 9 also applies here. • If there are convictions/ cautions to disclose on a basic certificate the DBS system automatically revokes consent and so the RO lead contact and/or third party will not be able to view the applicant's electronic certificate (neither party are notified that consent has been revoked). The applicant will be notified that consent has been revoked and will be advised that if they wish to reinstate consent they can do so via their DBS online account (they may need to create one). • An applicant can remove consent via their DBS online account (if they have a DBS online account when their application was submitted consent can be removed as soon as the	The applicant should have the facility to remove consent to view their electronic certificate at any time during the application process. Recommendation 2: The notification that is sent to a recipient of consent that they have been given consent to view the applicant's electronic certificate should not be issued when there are convictions to disclose because consent will be automatically revoked before the certificate can be viewed.		there is sufficient mitigation to minimise this risk. The impact on the RO could be considerable; registration cancelled, fines imposed by the ICO and/or possible prosecution if applications were submitted without the consent or knowledge of the applicant. The inbuilt safeguard of automatically revoking consent does remove the risk of sensitive personal data being revealed to a third party. Whilst the RO could still view the electronic certificate if there are no convictions to disclose the information that can be viewed would be

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
		certificate is issued, otherwise they would need to create a DBS online account after their they have been notified that their certificate has been issued). • If there are no convictions to disclose on the basic certificate consent will not be revoked and the RO lead contact and/or third party could view the electronic certificate online via their own DBS online account (no more personal information can be viewed on the electronic certificate than would appear within an eResult). An applicant can still remove consent if they wish via their DBS online account. • Because consent to view an electronic certificate can be automatically revoked or removed by the applicant (and in both cases the recipient of consent is not notified), not being able to view an electronic			no more than can be viewed on a 'blank' eResult for which the applicant has given consent. Whilst the risk is not eliminated it is reduced considerably

	Risks	Mitigation	Recommendations/ Solutions	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:**
		certificate does not infer that there are convictions/ cautions disclosed on the certificate. • An applicant can view details of their basic application via their DBS online account and will be able to check what application data was submitted and if anything has been changed			

7. OVERVIEW

Of the remaining 9 risks it is considered that there is sufficient mitigation to minimise and reduce the risks. Some recommendations have been made and will be evaluated. The introduction of GDPR in 2018 will require DBS to look again at many of these risks because the current mitigation may not be sufficient to reduce these risks to satisfy the requirements of GDPR. And it is expected GDPR will create other privacy risks that DBS will need to identify and address.		
Signature of person completing the PIA	Date:	
	Name (in capitals)	
Approval Signature (Approval will be required by either the Senior Responsible Officer (SRO)/ the Information Asset Owner (IAO) or Head of Unit (HoU))	Date:	
	Name (in capitals)	

8. APPENDIX A - LIST OF DATA ITEMS

DBS will collect only the personal data they require to process a basic criminal record check.

List of the Data items DBS collects to process a basic criminal record check:

- Title
- Surname
- Forename
- Middle name(s), if applicable
- Date of Birth
- Current address
- Previous names – all previous names are required.
    - First name
    - Last name
    - Date from when person known by this name
- Email address
- Gender/Sex
- Place of birth (town)
- Place of birth (country)
- NINO (National Insurance number) – must be provided if they have a NINO
- Passport number - must be provided if they have a current passport
- Driving licence number – must be provided if they have a current
- Previous addresses (All addresses in last 5 years) if individual has lived at current address for less than 5 years
- Address to send basic certificate as an alternative to home address.
- Mobile number
- Contact Telephone number
- DBS Profile Number, if held

An Accountable Officer will also need to provide the same personal information as above because they are required to apply for a DBS Basic check; personal information relating to a DBS Basic check will be stored within their individual DBS profile.

In addition some personal data will be captured on the Responsible Organisation registration application form that will be stored within the DBS Organisation profile for the related Responsible Organisation:

- Title
- Forename(s)
- Surname
- Date of Birth
- Gender
- Contact telephone number (likely to be an organisation number)
- Role in the organisation

The Accountable Officer will also be asked to provide their work address details

9. APPENDIX B – WEB SERVICES – SECURITY OVERVIEW

Information will be passed between the Responsible Organisation (RO) and DBS via new web services.

The following web service security characteristics will be implemented for the [2]Submit Disclosure (Basic) Application web service:

- Network/Web Application Firewall rules will be required in order to validate/allow only configured messages through the DBS system.
- Syntactic/semantic checking of Web Service content will also be required in order to validate content against defined XML schemas.
- Client and Server SSL certificate based authentication over an encrypted SSL transport layer is mandatory to access this web service. This is commonly known as two way SSL authentication or mutual SSL authentication.
- Supported version of TLS is TLS 1.2 (Transport Layer Security (TLS)) is a protocol which provides privacy between communicating applications and their users, or between communicating services. When a server and client communicate, well-configured TLS ensures that no third party can eavesdrop or tamper with any message.
- The SSL certificate details must match the organisation (RB or RO) identifier in the web service request.
- Certificates will be checked for validity (not expired etc.) and will be checked against a static and online revocation list (Certificate Revocation Lists (CRL) or Online Certificate Status Protocol (OCSP).
- As part of on-boarding a web service the RO will provide details of the expected volume of requests they will be making. In the event of this being significantly exceeded (for example three times the expected volume), a security incident will be raised to investigate, and if it is determined that the end-point is being misused the web service certificate will be revoked.
- A system wide web request threshold will be implemented which will limit the number of web service requests an RO can submit during a defined period.
- There will be an overarching requirement that states that ROs shall comply with the agreed Memorandum of Understanding (MoU) / policy / usage agreements for consumption of that web service.

[2] Web services have been designed to be used for the submission of applications for DBS Basic, Enhanced and Standard checks however initially only Basic applications will be submitted by a web service.