Data Protection Impact Assessment (DPIA)

Disclosure (Scotland) Bill

June 2019

Scottish Government
Riaghaltas na h-Alba
gov.scot

Disclosure (Scotland) Bill – Data Protection Impact Assessment (DPIA)

1. Introduction

The purpose of this document is to report on and assess against any potential Privacy Impacts as a result of the implementation of the Disclosure (Scotland) Bill ("the Bill").

It is acknowledged that further assessment and/ or revision of the Disclosure Bill DPIA may be required as the Disclosure Scotland Transformation Programme progresses.

2. Document metadata

2.1 Name of Project: **Disclosure (Scotland) Bill**

2.2 Author of report: **Disclosure Scotland Policy Team**

2.3 Date of report: **17 May 2019**

2.4 Name of Information Asset Owner (IAO) of relevant business unit: **Gerard Hart**

2.5 Date for review of DPIA: **Date of Bill implementation. The Disclosure (Scotland) Bill DPIA will be updated as the Transformation Programme DPIA is updated.**

Review date	Details of update	Completion date	Approval Date
7 January 2019	Initial draft	28 February 2019	
15 January 2019	Risk content reviewed to reflect Transformation DPIA review	15 January 2019	
7 February 2019	Reviewed following Transformation DPIA review	7 February 2019	
2 April 2019	Reviewed following release of updated ICO guidance	5 April 2019	
3 April 2019	Reviewed following discussions with SGLD.	8 April 2019	

3. Description of the project

3.1 Description of the work:

Disclosure Scotland is an Executive Agency of the Scottish Government. It exercises the functions of the Scottish Ministers under the Police Act 1997 ("the Police Act") and the Protection of Vulnerable Groups (Scotland) Act 2007 ("the PVG Act") to issue criminal record checks to support recruitment. Disclosure Scotland operates the PVG Scheme (established in February 2011) and holds the lists of individuals barred from doing regulated work with children and/or protected adults.

The intention of the Bill is to modernise and improve proportionality in the disclosure system in Scotland. This will simplify the system and aim to strike the right balance between strengthened safeguarding of the public and helping people with convictions get back to work. The Bill has been developed following a detailed public consultation, extensive engagement with stakeholders and from intelligence gathered during the eight years the PVG Scheme has been in operation.

It will:

- introduce a mandatory PVG Scheme for people working with vulnerable groups;
- overseas work which would be a regulated role, f done in Scotland, will be a specified regulated role so that such work benefits from the same level of safeguarding as regulated roles done in Scotland;
- introduce an internal process which will enable applicants to apply directly to Disclosure Scotland for the removal of spent convictions from a disclosure;
- expand the role of the Independent Reviewer, as appointed under the Age of Criminal Responsibility (Scotland) Bill, to review the disclosure of relevant police information, convictions for offences accrued under the age of 18 years, and removable convictions for offences List A and List B;
- strengthen referral powers for police and local authorities in relation to people carrying out regulated roles;
- safely end the requirement of courts to refer relevant offences to Disclosure Scotland;
- ensure organisations requesting disclosures are formally accredited and their processing and storage of personal data regulated;
- provide Disclosure Scotland with powers to impose standard conditions on scheme members who are under consideration for listing where considered necessary;
- provide Disclosure Scotland with powers to send notifications to personal employers, detailing the scheme member's consideration for listing / barred status and details of any conditions imposed on membership pending the outcome of any consideration for listing;
- allow bodies to register to make disclosure applications and to have access to vetting information for the sole purposes of offering a service to personal employers to help them consider suitability of prospective self-employed workers
- coincide with the development of an IT system that will increase the extent to which applicants may interact digitally with Disclosure Scotland and with prospective employers in the context of disclosure, and give applicant's greater control over the sharing of their information with third parties (effectively creating a right of veto for the individual).

3.2 Personal data to be processed.

Variable	Data Source
Personal information relating to specific applications – this will include name(s), addresses over last five years and contact details	Paper or electronic application, bulk data transfer from accredited bodies
Payment details relating to applying for disclosure records – this may include individuals or a group of individuals' credit card details, cheque, postal order, invoice	Application - paper or electronic. Invoices to organisations for bulk transfers
Identity verification	Application - paper or electronic. Organisations conduct identity verification for bulk applications
Matching individuals to criminal convictions	Protecting Vulnerable Groups System (PVG) Protecting and Safeguarding Scotland (PASS) System Criminal History Service (CHS) Police National Computer (PNC) Criminal Record Viewer (CRV) Police cross checking (PLX) Safeguarding Vulnerable Groups (SVG) Disclosure Internal Admin List (DIAL) Barred List
Relevant police Information (formerly "ORI")	UK police forces, individual
Childhood information - relating to convictions accrued between the ages of 12- 17 years.	Chief Constable, the Principal Reporter, the Scottish Courts and Tribunal Service, the individual and any

	other person Ministers (as Disclosure Scotland) considers appropriate.
Internal application for the removal of convictions	Chief Constable, the individual, the Principal Reporter, the Scottish Courts and Tribunals Service, any other person the Scottish Ministers (as Disclosure Scotland) considers appropriate.
Production of disclosure record	Disclosure Scotland
Independent Review - relevant police information - childhood information - removal of spent convictions	Chief constable, the Scottish Courts and Tribunal Service, Disclosure Scotland, the individual and any other person the independent reviewer considers appropriate.
Imposing standard conditions on people under consideration for listing and notifying persons other than an organisation or personnel supplier of considerations for listing and standard conditions	Disclosure Scotland

3.3 Describe how this data will be processed:

Disclosure Scotland is an Agency of the Scottish Government and the use of Disclosure Scotland services is specified in legislation, namely the Police Act and the PVG Act. There will also be provisions about the processing of personal data set out in the Bill which will repeal and restate the Police Act and amend the PVG Act.

Disclosure Scotland has a 'Data Protection and Privacy Statement' which explains data subjects rights, as a Disclosure Scotland customer, under the Data Protection Act 2018 (“DPA”). This applies whether information is held on paper or in an electronic format. Disclosure Scotland retains personal information in line with the DPA. This involves only retaining the personal information we need for business, regulatory or legal reasons. Once personal information is no longer needed, it is securely destroyed. All data is disposed of in accordance with the aforementioned Acts and in line with current HMG secure disposal guidance.

Disclosure Scotland is fully committed to compliance with the DPA. All operations and processes are in accordance with the Act. We are compliant with the EU General Data Protection Regulation (“GDPR”). We require information from data subjects, police forces and police records to protect the vulnerable. At present it is only disclosed to legitimate organisations who are legally entitled to have access to this information under Part 5 of the Police Act or the PVG Act. However, Disclosure Scotland may share information with the police where it believes a crime may have been committed as a result of the statutory offences contained in the Police Act and the PVG Act pertaining to falsification of disclosures, unlawful sharing of disclosures, barred individuals doing regulated work and failure to make referrals. These provisions are restated in the Bill.

Mandatory scheme

The handling of information will not change as a result of the introduction of a mandatory scheme. Anyone doing work with vulnerable groups will be required to be a member of the PVG Scheme and it will become an offence to work in such a role without first joining the PVG Scheme. It will also be an offence to offer any type of regulated role without first confirming their membership of the PVG Scheme.

Those who are no longer undertaking regulated roles, and have no intention to do so in the near future, will be able to remove themselves from the scheme and no longer be subject to ongoing monitoring. Disclosure Scotland will also notify individuals who are no longer in regulated roles that they can end their scheme membership. This will help to ensure the PVG Scheme will only interfere with the privacy of those who are actually doing or seeking to do regulated roles with children or adults. As part of implementation of the new legislation, Disclosure Scotland will engage with users of the Scheme to make them aware of their right to terminate membership at any point, where they are no longer doing a regulated role.

Disclosure Products

The Bill will offer two main levels of Disclosure, comprising of four products. Level 1 will replace the current basic disclosure under the Police Act and within Level 2 there will be 3 variants, the extent of disclosure increasing with the nature / sensitivity of the role. As part of the policy development of the Bill, there has been detailed consideration of the information to be included on each level of disclosure, to ensure that what is being disclosed for specific purposes is adequate and relevant. However, the new system has been designed to work within the existing self-disclosure framework, that being the Rehabilitation of Offenders Act 1974 ("the 1974 Act") and orders made under that Act which dis-apply the protections of the 1974 Act against the disclosure of spent convictions, to set out the circumstances and purposes for which individuals must self-disclose spent convictions. It is vital that the state and self-disclosure regimes continue to be aligned.

The requirement to be a member of the Scheme will be placed on those who exercise power or influence over children and vulnerable adults. The design principle is that customers should only need to know the role that they intend to do and the online system should take care of guiding them to the appropriate disclosure. This will be done by working with our customers to design a digital system that allows information input about the job or role to lead to a clear outcome for the customer. There will be alternative provisions for those with no access to digital or who face other challenges using it.

Digital delivery

The Disclosure Bill supports increasing the extent to which applicants may interact electronically with Disclosure Scotland and with employers in the context of disclosure. The details of how the Bill's proposals will be implemented digitally will be designed in close consultation \ engagement with customers and stakeholders including the ICO. The implementation of increased electronic services will modernise and simplify the disclosure system, and enhance the operational efficiency, portability, ownership of information for the applicant and give greater control over whom they share that information with the process of issuing a certificate directly to the employer will end. Under the Bill it will be necessary for the individual to authorise the release of their disclosure to a third party, after the individual has had a chance to see it for themselves.

Alternatives will be provided for individuals with no access to digital or who face other challenges using it. These alternatives will be developed in collaboration with service users to ensure that they meet all relevant accessibility and data protection requirements.

There will be no changes in the data protection implications for internal processing of online applications. Further information on the impacts of digital delivery will be detailed within the *Disclosure Scotland Transformation Programme* DPIA.

Widening the functions of the independent reviewer

The independent reviewer appointed under the Age of Criminal Responsibility (Scotland) Bill ("the ACR Bill") will be given additional functions, making the independent reviewer responsible for all types of review (childhood conviction information, removable convictions and relevant police information) relating to the disclosure of vetting information. We believe that unifying the review mechanisms will make the system as simple and coherent as possible for applicants and stakeholders.

The processes required for the independent reviewer will be based around existing practice so will meet all privacy and data protection requirements. The independent reviewer will be appointed by Scottish Ministers and will agree to all necessary protections for handling sensitive information. As part of their review, the independent reviewer will contact various public bodies in order to obtain additional information regarding the individual and the behaviour that is proposed to be disclosed. There will be a new link needed between the Disclosure Scotland IT system and the Scottish Government network to be used by the independent reviewer. Information can also be shared via secure email or by Royal Mail. All appropriate measures will be taken to ensure data sharing with the various organisations is secure and compliant with the DPA and the GDPR. This

will follow the same processes and procedures as those under the current system. Further information on the role of the Independent Reviewer is detailed within the *Age of Criminal Responsibility (Scotland) Bill* PIA.

The new review processes will also lead to new categories of data being processed by the Independent Reviewer and Disclosure Scotland. These will include any representations made by the individual as part of the review process, the outcome of any reviews and reasons for decisions.

Internal application for the removal of spent convictions

The Bill will introduce an internal process through which an applicant can apply directly to Disclosure Scotland for the removal of spent convictions. An internal assessment will be faster than an application to a sheriff, and cheaper for the applicant as legal representation is not required. The applicant can make an application to Disclosure Scotland to have a conviction removed from their certificate. There will be a prescribed fee for this application. Information will not be shared with a third party without authorisation from the applicant. Applicants will be able to provide representations in support of their application to have the conviction removed from their disclosure. If Disclosure Scotland refused to remove the conviction, the applicant would then have a right to apply to the independent reviewer to consider removal of the conviction, instead of applying to the sheriff. Under the new system an appeal to a sheriff would be available for the decision by the independent reviewer but on a point of law only.

The process required will be based on existing practice which meets all privacy and data protection requirements. As digital capability of the IT system increases, any process put in place will be equal to or better that the current processes which meet the required levels for DPA and GDPR.

Other Relevant Information ("ORI")

ORI is information currently provided by the chief officer of a police force to Disclosure Scotland for inclusion in an enhanced disclosure or PVG scheme record. It is presently used very infrequently but is very important for public protection.

The Bill will change the point at which the individual becomes aware of the police intention to include relevant police information on a Level 2 disclosure, meaning individuals will have the opportunity to provide representations before relevant police information is shared with, for example, a potential employer. This will bring the disclosure regime in Scotland into line with the rest of the UK, where police forces follow Home Office guidance regarding the disclosure of relevant police information. Disclosure Scotland will publish statutory guidance for Police Scotland and the independent reviewer about making decisions on the provision of relevant police information.

An individual will be able to share representations with Police Scotland, Disclosure Scotland and the independent reviewer through existing channels of secure email or by Royal Mail. As digital capability of the IT system increases, any process put in place will be equal to or better existing processes which meet the required levels for DPA and GDPR. The process by which Police will share proposed relevant police information with Disclosure Scotland will not change. Information is shared through the secure Scottish Government IT network. Applicants will be notified securely of relevant police information to be disclosed, given the opportunity to submit representations to the police, and will have the option to have police decisions reviewed by the independent reviewer before any relevant police information is shared with a third party. There will be a new link needed between the Disclosure Scotland IT system used for processing relevant police information and the Scottish Government network to be used by the independent reviewer.

There will be new categories of data created as part of this, including any reasons given by the police for their decision to disclose relevant police information. This will be processed by Disclosure Scotland for the purposes of enabling a review to the Independent Reviewer.

Disclosure provisions childhood conviction information

Building on the work that is being taken forward in the ACR Bill, the Disclosure Bill will further improve the prospects of people with childhood convictions. There will be no possibility of automatically disclosing a

conviction for offences accrued under the age of 18, on any type of disclosure. This is a positive step as it potentially reduces the amount of sensitive personal information being disclosed. If there are childhood convictions present, Disclosure Scotland will make an assessment on whether or not to disclose information about the conviction. If the decision is to disclose the information the applicant will be informed through existing processes, such as Royal Mail. The applicant will be given the choice to apply for a review by the independent reviewer and have an opportunity to provide representations. Representations will be provided through existing processes. Once the independent reviewer has concluded their review, the individual and Disclosure Scotland will be securely notified. As digital capability of the IT system increases, any process put in place to share sensitive information will be equal to or better than the current processes which meet the required levels for DPA and GDPR.

Childhood conviction information will be a new category of data processed by Disclosure Scotland as a result of the Bill.

New referral powers for local authorities

At present there is no legal mechanism for local authorities to make referrals to Disclosure Scotland within the context of their normal safeguarding functions, even if formal child or adult protection investigations find evidence of physical, financial or sexual abuse of vulnerable people. The Bill will give local authorities and health and social care partnerships powers to refer individuals to Disclosure Scotland. By making a referral, local authorities will be sharing sensitive personal information about an individual, gathered within the context of their normal safeguarding functions. A template for this already exists as local authorities make referrals to Disclosure Scotland as an employer of people doing regulated work. The existing methods by which local authorities share sensitive information with Disclosure Scotland will not change as a result of this new referral power.

Wider referral powers for Police Scotland

Police Scotland presently cannot provide information to Disclosure Scotland about a person who is not a PVG scheme member. A mandatory PVG scheme means that Police Scotland will be able to give information to Disclosure Scotland about all those involved in working with vulnerable people. In circumstances where a person is doing such work unlawfully outside the PVG Scheme, Police Scotland must provide information as if the person concerned had been in the PVG Scheme.

Referral information will be shared through existing processes through the secure Scottish Government IT network, which meets the required levels for DPA and the GDPR.

Ending court referrals

Under section 7 of the PVG Act, courts are required to refer certain convicted individuals to Disclosure Scotland for consideration for barring, even if the individual has never sought or done regulated work with vulnerable groups. This enables Disclosure Scotland to pre-emptively consider and possibly bar those convicted of serious offences against children, lowering the risk that they might engage in regulated work without joining the PVG Scheme. The Disclosure Bill presents the opportunity to safely end the court referral process because, with a mandatory scheme, it will no longer be lawful carry out a regulated role without PVG membership. To continue these court referrals would be an unnecessary intervention in safeguarding terms. The Bill will help to ensure the PVG Scheme will only interfere with the privacy of those who are actually doing or seeking to carry out a regulated role with children or protected adults.

For extremely serious offences individuals will still be automatically barred, under section 14 of the PVG Act. The process by which courts share this information with Disclosure Scotland will not change.

Accredited bodies

Disclosure Scotland offers businesses the ability to submit bulk applications of basic disclosures (B2B disclosures). We will continue to offer this service for the basic disclosure successor, Level 1 disclosures, to organisations that require it, but will bring these organisations within the scope of accredited bodies, replacing

the current non statutory definition of 'responsible body'. This will assure the protection of personal data as the service moves onto new digital platforms, whilst still allowing for the efficient delivery of the service.

It is worth noting that although the consultation paper referred to 'consent' in this context, it is not intended to rely on consent as the legal basis for processing. What is meant by consent is that the B2B organisation has the explicit consent of the applicant to submit the application on behalf of the applicant.

Accredited bodies will also replace 'registered persons', under the Police Act, for access to Level 2 disclosures. The system of registering accredited bodies remains an important part of the disclosure regime as it ensures disclosures are issued to persons who are considered suitable to receive potentially sensitive information and to ensure that those receiving the information are legally entitled to see it for the purposes of the employment they are offering.

A noteworthy improvement is that control over the sharing of disclosure data will pass to the disclosure applicant. The practice of issuing a certificate directly to an employer, at the same time that it goes to the applicant, will end. The individual will have to explicitly elect to share electronic access to their disclosure record (or non-electronic equivalent), which means that sharing the disclosure with an employer will only be possible if the applicant chooses not to apply for any review, or after any review procedures have been exhausted.

Notification of consideration for barring and the outcome

The Bill will give Disclosure Scotland a power to issue section 30 notices (notification of listing, etc) to individuals who do not employ other persons in the course of a business, detailing the individual's consideration for listing / listed status. The PVG Act does not enable Disclosure Scotland to currently send section 30 notices to anyone who does not fall under the definition of "organisation" or "personnel supplier". This information will be shared securely using existing practices so will meet all privacy and data protection requirements.

Disclosure arrangements for personal employers

Organisations will be able to register to become umbrella bodies, entitling them to countersign applications and have access to vetting information, for the sole purposes of them offering a service to individuals who do not employ other persons in the course of a business to help them consider suitability of, for example, potential self-employed workers. The purpose of this is to prevent sensitive disclosure information from being shared more widely than is necessary and ensures the disclosure regime is lawful and proportionate. As part of the registration process for accredited bodies, Disclosure Scotland will ensure by having regard to vetting information that accredited bodies are suitable to have access to Level 2 disclosures.

When acting in the role of umbrella body, organisations will be subject to the registration system that applies to all accredited bodies, including a Code of Practice containing provisions on the safe handling of the disclosure certificates and will be subject to offence provisions in relation to the proper use of disclosure information.

Standard conditions

In the most serious of cases, details of any standard conditions to which a scheme member is subject while under consideration for listing will be disclosed to legitimate persons who have a legal right to have access to this information. If standard conditions were imposed, these would appear on confirmations of scheme membership. The processes required will be based around existing practice so will meet all privacy and data protection requirements.

3.4 Explain the legal basis for the sharing with internal or external partners:

Disclosure Scotland on behalf of Scottish Ministers protects the people of Scotland by providing disclosures under the Police Act 1997 (as amended) and the Protection of Vulnerable Groups (Scotland) Act 2007(as amended).

4. Stakeholder analysis and consultation

4.1 List all the groups involved in the project, and state their interest.

Group	Interest
Police Scotland	Police Scotland will have to notify Disclosure Scotland and the applicant of proposed 'relevant police information', and offer the applicant the opportunity to provide representations as to why 'relevant police information' should not be disclosed. Individuals and Disclosure Scotland will have to be notified of the outcome.
Local Authorities	Local authorities will have strengthened referral powers to refer individuals to Disclosure Scotland. Local authorities may be contacted by the independent reviewer to provide additional information during review process.
Accredited bodies	Accredited bodies are formally accredited and their processing and storage of personal data regulated.
PVG Review Consultation respondents	Use the disclosure regime as individuals or organisations, must be kept informed of any changes in legislation/ processes which may affect them.
Scottish Courts and Tribunal Service	Court referrals under section 7 of the PVG Act will end. May be contacted by the independent reviewer to provide additional information during review process.

4.2 Method used to consult with these groups when making the DPIA.

Following extensive pre-consultation engagement between January and August 2017 with over 300 individuals and organisations, and an online survey generating over 800 responses, Disclosure Scotland published a consultation paper the 'Protection of Vulnerable Groups and the Disclosure of Criminal Information'. The public consultation ran from 25 April 2018 until 18 July 2018 and received over 350 responses from a range of stakeholders with varying backgrounds including judicial bodies, the legal sector, local government, voluntary organisations, the health sector and individual scheme members. The consultation paper included a specific question on impacts to individuals' privacy by the options set out in the consultation.

Disclosure Scotland has an existing Stakeholder Advisory Board, which includes representation from local authorities, health boards, care sector, regulatory bodies and victims groups, that provides advice and guidance on changes in operation.

Disclosure Scotland's User Research team have been conducting face to face interviews and user testing with individuals and organisations throughout the UK. This research has included testing the privacy statement and capturing user needs around privacy and data protection such as simplifying the privacy statement and ensuring it is in plain English.

Regular meetings have been held with major data providers (Home Office, Police Scotland, PSNI) and critical stakeholders such as ITECS who can support the delivery of the security processes required to implement the new systems. Regular meetings are also held with Disclosure Scotland's independent security assessor.

4.3 Method used to communicate the outcomes of the DPIA.

The DPIA will be published on gov.scot. Disclosure Scotland will also provide an update via a quarterly e-bulletin, which is issued to over 15,000 countersignatories.

The Disclosure Scotland Bill Team will continue to engage with relevant advocacy and representative groups for input on developing proposals and guidance materials.

5. Questions to identify privacy issues

5.1 Involvement of multiple organisations

There is a possibility that information from police forces, courts, professional registration bodies, local authorities and judicial bodies in EU member states in connection with Directive 2011/93/EU could be involved, depending on applicants' criminal history. All appropriate measures have been taken to ensure data sharing is secure and compliant with the DPA and GDPR. The Disclosure Bill will not affect this and the processes and procedures as those under the previous regime will remain.

The independent reviewer will be appointed by Scottish Ministers and will be required to comply with all necessary protections for handling sensitive information. As part of their review, the independent reviewer may contact various public bodies in order to obtain additional information regarding the individual and the information that is proposed to be disclosed. All appropriate measures will be taken to ensure data sharing with the various organisations is secure and compliant with the DPA and GDPR. This will follow the same processes and procedures as those under the current system.

Disclosure Scotland will share proposed information with the independent reviewer through the secure Scottish Government IT network. Additional information that the independent reviewer has requested will come in to Disclosure Scotland from various organisations and representations will come from the individual. Any additional information received will be shared with the independent reviewer through the secure Scottish Government IT network. Further information on the role of the independent reviewer is detailed within the Age of Criminal Responsibility (Scotland) Bill PIA.

Information to support an appeal will need to be provided to a Sheriff and to the Scottish Government's Legal Department ("SGLD") as part of the appeal process, as is current procedure.

5.2 Anonymity and pseudonymity

The new review processes will lead to new categories of data being processed by the independent reviewer, Police Scotland and Disclosure Scotland. These will include any representations made by the individual as part of the review process, the outcome of any reviews and reasons for decisions.

The independent reviewer will be subject to a privacy policy. All appropriate measures will be taken to ensure data sharing with the independent reviewer is secure and compliant with the DPA and GDPR. Disclosure Scotland's privacy policy will be updated to reflect the changes made by the Bill.

5.3 Technology

The systems, processes and data will be securely stored and will be accredited and tested to provide an assured level of security around the personal data required to execute the programme and the future service.

Disclosure Scotland has a security policy, technical architecture and security governance to provide compliance for the systems and services. This includes independent testing, assurance and accreditation by key stakeholders. The IT system being developed has been subject to extensive CHECK technical IT penetration testing by an approved supplier. Vulnerabilities are addressed in a current risk treatment plan.

Further information on digital security can be found in the Disclosure Scotland Transformation Programme DPIA.

5.4 Identification methods

The same identifiers will be used as those under the existing regime. Name and previous names, National Insurance (NI) number, date of birth and address/address history are all collected as part of the official collection and recording of information. There will also be a continuation of existing powers to verify the identity of an individual through fingerprint data in some cases, as a means of preventing fraud. These are all subject to all appropriate safeguards. None of this information could ever be published or released to the general public.

5.5 Sensitive/Special Category personal data

The Bill will not result in the routine processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, data concerning health or data about a person's sex life or sexual orientation. Some biometric data will be processed in the form of fingerprints. The powers in the Bill to process such data replicate existing powers under the Police Act 1997. The processing of biometric data is necessary for reasons of substantial public interest (fraud prevention) on the basis of specific powers in the Bill. There are measures to safeguard the security of that information. All personal and sensitive data collected will continue to be treated the same as the current regime. This will include specific access controls, security clearances and specific design to meet the standards required by our security accreditor.

5.6 Changes to data handling procedures

There may be changes in processes as the Transformation programme evolves and digital capability increases. There will be no change to the level of data protection applied. Revised processes will be equal to or better than current processes which pass the required levels for DPA and GDPR.

The processes and systems needed for the independent reviewer will be based around existing practice, meeting all privacy and data protection requirements. The independent reviewer will be appointed by Scottish Ministers and will be required to comply with all necessary protections for handling sensitive information.

5.7 Statutory exemptions/protection

If personal information is shared with third parties through data sharing agreements or for legal/statutory requirements, Disclosure Scotland will confirm the third party has the appropriate legal justification. Disclosure Scotland is entitled to share information with the police for the law enforcement purposes within the meaning of section 31 of the DPA.

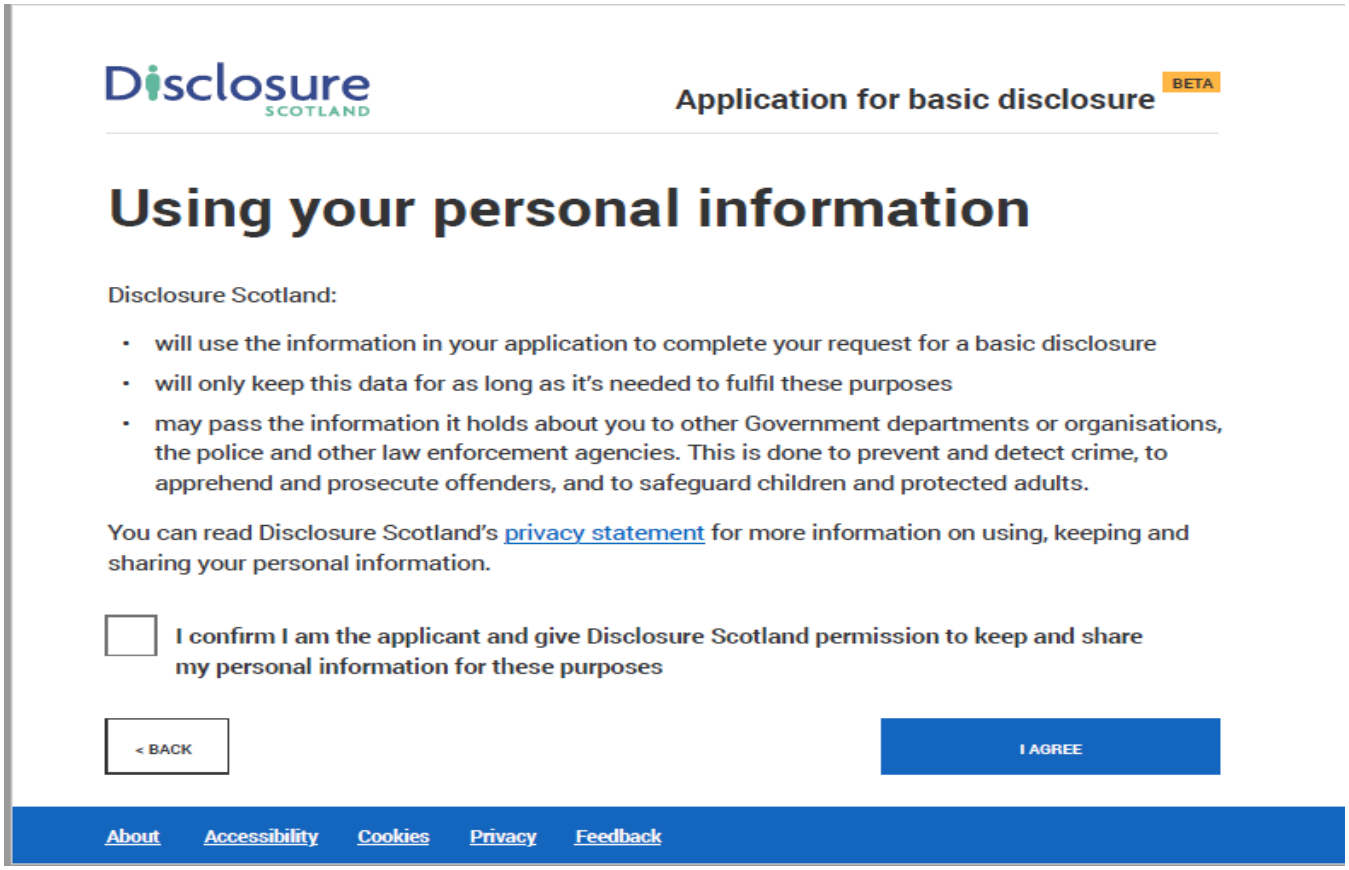
5.8 Justification

The new processes, and the changes in existing processes, are being made to ensure the disclosure system is rights respecting whilst continuing to safeguard the public. The changes are positive as they will simplify existing processes and will give applicants additional rights.

Disclosure Scotland collects, holds and processes personal information because the processing is necessary for the exercise of our functions as an Executive Agency as outlined in legislation that governs criminal records checks. This is a legitimate condition of processing as outlined under the DPA.

Individuals are made aware on the “declaration” section of the application of their personal data will be used. There is extensive information and guidance on Disclosure Scotland’s website. Information on the process for independent review will be provided to the applicant. Information on the appeals process will be provided to the applicant, as it already the case.

Below is a screenshot from the online application for a basic disclosure:



5.9 Other risks

There are currently numerous safeguards to protect all data privacy within Disclosure Scotland. The Transformation Programme delivering increased digital functionality will be implementing this measure as a minimal requirement. If a change is required, the new process will have to exceed the current security parameters.

This DPIA has identified that any changes in process are based on current data handling and storage arrangements and that these arrangements do not pose any significant risks to the privacy of that information.

We believe that the systems that are in place for managing the transfer and storage of data comply with legislative demands, and we will review any further legislative changes to ensure that the arrangements comply with them.

6. General Data Protection Regulation (GDPR) Principles

Principle	Compliant – Yes/No	Description of how you have complied

6.1 Principle 1 – fair and lawful, and meeting the conditions for processing	YES	The principal lawful basis for processing is Article 6(1)(e) of the GDPR. Some processing may also take place on the basis of article 6(1)(c). Special category data is processed under article 9(2)(g). Disclosure Scotland gathers and processes data under the Police Act and the PVG Act, in line with the DPA and GDPR. Data processing will take place under a similar framework under the Bill.
6.2 Principle 2 – purpose limitation	YES	Data will only be gathered for the purposes covered under the following pieces of primary legislation and secondary legislation made under them: The Police Act The PVG Act The Disclosure (Scotland) Bill
6.3 Principle 3 – adequacy, relevance and data minimisation	YES	Disclosure Scotland gathers and processes data under the Police Act and the PVG Act, in line with the DPA and GDPR. Data gathering and processing will take place under a similar framework under the Bill. Disclosure Scotland ensures all information gathered is adequate, relevant and not excessive. Information is processed in accordance with the individual's rights and is not kept for longer than is necessary.
6.4 Principle 4 – accurate, kept up to date, deletion	YES	Disclosure Scotland processes, gathers, retains and securely destroys data under the Police Act and the PVG Act, in compliance with DPA and GDPR. The new system will allow access for members to update their information. Individuals can also request a review of accuracy if they believe information held about them is incorrect. Members can ask to be removed from the Scheme if they are no longer in regulated work. The PVG Act does not currently give Scottish Ministers a power to remove a member from the Scheme unless the person is barred from regulated work. Under the Bill, a recurrent membership period ensures the Scheme is accurate and self-adjusts to the right size because people who do not need to be in it have the incentive and easy opportunity to safely leave.
6.5 Principle 5 – kept for no longer than necessary, anonymization	YES	Disclosure Scotland operates a data retention policy. This policy is inherent in the design of the new service and proposed processes. The Bill addresses the requirement not to keep data longer than necessary by making PVG scheme membership time limited, so that people can come out of the scheme when they are no longer doing a regulated role. This will help to ensure that personal data is only held for as long as necessary and relevant to Disclosure Scotland's functions.

6.6 GDPR Articles 12-22 – data subject rights	YES	As stated within the Disclosure Scotland Privacy Statement, individuals have the right to access the information held about them by Disclosure Scotland, and can ask for any data to be amended if it is incorrect. Individuals can ask Disclosure Scotland not to process information used for the disclosure certificate if it would cause substantial unwarranted damage or distress. Individuals can request that non-automated decisions are made regarding their data.
6.7 Principle 6 - security	YES	DS has a security policy, technical architecture and security governance to provide compliance for DS systems and services. This includes independent testing, assurance and accreditation by key stakeholders. <u>Appeal process:</u> The Independent Reviewer (IR) (appointed under the ACR Bill) will have the ability to gather additional information regarding an applicant. The processes and systems involved will be subject to the same strict privacy rules as other data held by Disclosure Scotland. The applicant will be aware that the IR's request relates to the proposed disclosure of their personal and sensitive personal data to a third party.
6.8 GDPR Article 44 - Personal data shall not be transferred to a country or territory outside the European Economic Area without additional safeguards.	YES	The design of the service ensures that no personal data is stored or transferred to a third party in a territory or country outside the European Economic Area (unless the data subject has consented). Disclosure Scotland has no stakeholders outside the EEA. In addition we are authorised to process and gather data under The Police Act and the PVG Act, in compliance with DPA and GDPR.

7. Risks identified and appropriate solutions or mitigation actions proposed

Risk	Ref	Solution or mitigation	Result
Introduction of new processes, specifically surrounding independent reviewer and internal appeal process.	001	This DPIA has identified that any new processes will use the current data handling and storage arrangements and that these arrangements do not pose any significant risks to the privacy of that information. The systems in place for managing the transfer and storage of data comply with legislative demands, and will be reviewed any further legislative changes to ensure that the arrangements comply with them.	Reduce

There is a risk that unauthorised 3rd Parties attempt to obtain access to our data or introduce malicious data or code to the service	002	Designs are approved tested to ensure all necessary controls are effective and fit for purpose. Anti-Virus products and security controls are in use across the estate to continually monitor the service. Maintenance activities are scheduled and acted upon to ensure the resilience and security standards of the service Access controls are in place to ensure that only trained and security cleared, authorised personnel have access to the system. All software is pre-approved by the Technical Design Authority and security risks are managed through the Security Working Group who are responsible for maintaining the overall integrity of the service. Security risks are reviewed at the Technical Design Authority	Reduce
There is an ongoing potential risk of human error, which may result in information being handled incorrectly or delivered to incorrect recipient.	003	New processes being introduced, such as the review to the independent reviewer and widened referral duties/powers for police and local authorities will introduce new channels of communication/ increased volume of communication between stakeholders. This may impact the potential for human error. The new processes will be based around existing processes. Disclosure Scotland staff will be given appropriate training before new processes are implemented. Disclosure Scotland will engage with the external stakeholders involved to agree process requirements.	Reduce

8. Incorporating Privacy Risks into planning

Explain how the risks and solutions or mitigation actions will be incorporated into the project/business plan, and how they will be monitored. There must be a named official responsible for addressing and monitoring each risk.

Risk	Ref	How risk will be incorporated into planning	Owner
Unauthorised access to DS Services	001	All solutions have specific acceptance criteria around the performance of the service. Maintenance activities are scheduled and form part of the service design.	Programme Delivery Manager
Unauthorised sharing of disclosure information	002	Ensure it is clear within legislation that the individual has control over which third parties can access their information. Specify the restrictions placed on a third party with access, e.g. cannot share the information with other third parties without the individual's consent.	Policy Manager

9. Data Protection Officer (DPO)

Advice from DPO	Action

10. Authorisation and publication

I confirm that the impact of the Disclosure Bill has been sufficiently assessed against the needs of the privacy duty:

Name and job title of a IAO or equivalent	**Date each version authorised**
Gerard Hart Director of Protection Services and Policy	

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at
The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-78781-915-3 (web only)

Published by The Scottish Government, June 2019

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS590270 (06/19)