Privacy Impact Assessment (PIA)

The Police Act 1997 and the Protection of Vulnerable Groups (Scotland) Act 2007 Remedial Order 2018

February 2018

Scottish Government
Riaghaltas na h-Alba
gov.scot

Privacy Impact Assessment (PIA)

1. Introduction

What is a Privacy Impact Assessment (PIA)?

A PIA is a tool to identify and reduce the privacy risks of a project. A PIA can reduce the risks of harm to individuals through the misuse of their personal information.

The Information Commissioner's Office, as the public body chiefly concerned with data protection, have produced guidance on PIAs. Their guidance, including PIA screening questions, has been used in the development of this PIA.

This PIA explores the implications for confidentiality and privacy of information, as a consequence of the Police Act 1997 and the Protection of Vulnerable Groups (Scotland) Act 2007 Remedial Order 2018 ("the 2018 Remedial Order"), Scottish Statutory Instrument 2018 No. 28.

It provides:

- the background for the introduction of the 2018 Remedial Order,
- the PIA screening process questions and answers, and the conclusion,
- the information flows,
- details of how information is passed to the Scottish Government,
- the legal basis for gathering and storing information, and
- the mitigations in place to safeguard that information.

2. Document metadata

Name of project	The Police Act 1997 and the Protection of Vulnerable Groups (Scotland) Act 2007 Remedial Order 2018
Date of report	9 February 2018
Author of report	DS Policy Team
Information Asset Owner	Lorna Gibbs, Chief Executive
Date of review	The Privacy Impact Assessment was revised in light of the consultation on the Proposed Draft Police Act 1997 and the Protection of Vulnerable Groups (Scotland) Act 2007 Remedial Order 2018 ("the Proposed Draft Remedial Order") to take account of points raised during consultation.

3. Background

Standard and enhanced disclosures are issued under the Police Act 1997 ("the 1997 Act") and disclosures of PVG scheme records are issued under the Protection of Vulnerable Groups (Scotland) Act 2007 ("the 2007 Act") - these types of disclosures

are referred to collectively as 'higher level disclosures'. In 2015, the Police Act 1997 and the Protection of Vulnerable Groups (Scotland) Act 2007 Remedial (No. 2) Order 2015 ("the 2015 Remedial Order") amended the 1997 and 2007 Acts in relation to the spent conviction information which could be disclosed in a higher level disclosure. That 2015 Remedial Order introduced lists of offences into schedules 8A and 8B of the 1997 Act. Schedule 8A lists certain offences, spent convictions for which will continue always to be disclosed due to the serious nature of the offence (sometimes referred to as the 'Always Disclose List'[1]); schedule 8B lists certain offences, spent convictions for which are to be disclosed subject to rules depending on the length of time since conviction and the disposal of the case (sometimes referred to as the 'Rules List').

In the case *P v Scottish Ministers* [2017] CSOH 33, P raised a petition for judicial review in relation to the disclosure of a previous conviction for lewd and libidinous practices on his PVG scheme record. Although the conviction was spent, the offence had been included in P's scheme record due to it being in the Always Disclose List. On 17 May 2017 the court declared that, insofar as they require automatic disclosure of P's conviction before the Children's Hearing, the provisions of the 2015 Remedial Order unlawfully and unjustifiably interfered with the petitioner's right under Article 8 of the European Convention on Human Rights (ECHR), and Scottish Ministers had no power to make the provisions in terms of section 57(2) of the Scotland Act 1998 ("the 1998 Act").

The effect of the court order was suspended under section 102 of the 1998 Act for nine months (to 17 February 2018) to allow Ministers to remedy the legislation.

Following the court's decision, the Scottish Ministers undertook an assessment of the 1997 Act and the PVG Scheme operated under the 2007 Act and concluded that the legislation should be amended further to limit the circumstances in which convictions are automatically disclosed. The functions of the Scottish Ministers under the 1997 Act and the 2007 Act are exercised through Disclosure Scotland.

The Proposed Draft Remedial Order set out the proposed amendments to the 1997 and the 2007 Acts. It proposed that individuals convicted of schedule 8A offences should in certain specified circumstances have the right to apply to a Sheriff in order to seek removal of that conviction information before their disclosure is sent to a third party such as an employer.

We are satisfied that this policy should provide an ECHR compliant system.

This PIA aims to assess and manage the risks associated with data protection and information privacy. The first stage in our PIA is the screening process.

[1] Schedule 8A was inserted into the Police Act 1997 by *the Police Act 1997 and the Protection of Vulnerable Groups (Scotland) Act 2007 Remedial (No. 2) Order 2015* (Scottish Statutory Instrument 2015 No. 423).

4. Privacy Impact Assessment (PIA) screening process

We conducted a screening process to evaluate whether a full-scale PIA should be conducted. The screening questions and answers are detailed below.

Technology

1. Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?

No.

Identity

2. Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?

No, the same identifiers are used as those under the previous regime. National Insurance (NI) numbers, dates of birth and address/address history are all collected as part of the official collection and recording of information. These are subject to all appropriate safeguards. None of this information could ever be published or released to the general public.

3. Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?

No.

Multiple organisations

4. Does the project involve multiple organisations, whether they are government agencies (e.g. in 'joined-up government' initiatives) or private sector organisations (e.g. as outsourced service providers or as 'business partners')?

Yes, there is a possibility that information from police forces across the UK could be involved, depending on applicants' criminal history. However, all appropriate measures have been taken to ensure data sharing with the various police forces across the UK is secure and compliant with the Data Protection Act 1998 ("the 1998 Act"). This has not changed and follows the same processes and procedures as those under the previous regime.

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.

Data

5. Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?

No. The process for handling data for criminal history appeals to a Sheriff in similar circumstances already exists, there is no change caused by this new legislation other than widening the circumstances.

6. Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?

No. There is no change to the collection or handling of personal data.

7. Does the project involve new or significantly changed handling of personal data about a large number of individuals?

No. The process for handling data in similar circumstances already exists. In addition we anticipate the numbers of people who use the appeals process to be very limited.

8. Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?

No, this process already exists.

Exemptions and exceptions

9. Does the project relate to data processing which is in any way exempt from legislative privacy protections?

No.

10. Does the project's justification include significant contributions to public security measures?

No.

11. Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?

No. The only additional parties who will receive information are Sheriff Courts and SGLD, both of whom are subject to the 1998 Act.

5. Conclusion from Screening

The answers to the screening process suggest that there are limited concerns in terms of privacy as a result of the additional information being provided as part of the appeals process. The parties who will receive this information (Sheriff Courts and SGLD) are both subject to the 1998 Act.

Based on the answers to the screening exercise we do not believe that a full-scale PIA is required. We have proceeded on the basis that a small-scale PIA is appropriate.

6. Consultation

A formal consultation on the Proposed Draft Remedial Order ran for 60 days from 11 September to 26 November 2017, as set out in Convention Rights (Compliance) (Scotland) Act 2001. Notification about the consultation was sent to over 200 key stakeholders.

Fifty one written observations were received. The majority of respondents 37 (72%) supported the proposals, though several did so with qualifications. Eight respondents (16%) were opposed to the proposals and six respondents (12%) did not express a view.

Specific comments on privacy were made by ten respondents. Two drew attention to the public nature of the appeal proceedings. This point is not new. The reforms introduced by the 2015 Remedial Order provide that appeal proceedings under either the 1997 Act, or the 2007 Act may take place in private if the Sheriff considers it appropriate. This is provision has not been changed by the 2018 Remedial Order. No new issues about privacy were raised by respondents.

In light of the written observations received on the Proposed Draft Remedial Order, Ministers concluded that it was not necessary to make any amendments other than to change some minor points noted by the Scottish Parliament's Delegated Powers and Law Reform Committee. The 2018 Remedial Order is otherwise unchanged from the Proposed Draft Remedial Order.

7. The information flows for the 2018 Remedial Order

There are three information flows to and from Disclosure Scotland that already exist and will continue to exist for the processing of applications under the amended approach. These are:

1. Information transfer and collection from Criminal Database Providers

Under the amended approach this process is exactly the same as before.

2. Information collection from Applicants

Under the amended approach there is no change to the way information is collected from applicants. Applications are submitted to Disclosure Scotland on a standard application form developed by Disclosure Scotland. The application form requests all the information required to process an application. The information from the application form details private information about the applicant, their household, and their employer.

The application form includes a declaration for the applicant to sign. The declaration makes it clear to the applicant what the information they supply may be used for. The declaration is detailed below.

Declaration

I understand the following:

- Disclosure Scotland will use the information I have given to verify my identity and to check and process my application.
- Disclosure Scotland will use this information for the purposes of the prevention or detection of crime and for other related purposes.
- Disclosure Scotland may pass the information it holds about me to other Government departments or organisations, the police and other law enforcement agencies for the purposes of the prevention and detection of crime, of the apprehension and prosecution of offenders and for other related purposes.

I declare that the information I have given is complete and correct. I understand that to knowingly make a false statement in this application is a criminal offence. I will give any additional information that may be required to verify the information given and will immediately notify any changes to this information.

Signature:

Date:

3. Information collection and transfer to Sheriff Courts

Under the amended approach applicants will have the ability to appeal disclosure of certain convictions under specified circumstances. This will involve a formal appeal to a Sheriff, however the process for this is already in place under the current system for appeals for spent conviction for offences included in schedule 8B of the 1997 Act.

8. How is information passed to Disclosure Scotland?

1. Application Process

Applicants complete a paper application form, the applicant's identity is verified by the countersignatory ("CSG") to the form, the CSG signs and sends the application form to Disclosure Scotland. Once it arrives at Disclosure Scotland the application is uploaded onto our PVG system.

This system is secure and can only be accessed by authorised users. There is no functional ability to share this information externally.

Once uploaded on the system it is placed in a vetting queue and is then passed to vetting staff to begin the information gathering and matching process.

2. Quality improvement information gathering

We set out the process for information gathering and verification for CSGs. This guidance is available to all CSGs and is also available on the Disclosure Scotland website. There is a Code of Practice issued by Scottish Ministers under the 1997 Act that CSGs must follow when handling information from applicants.

Guidelines govern information gathering by the police and there is a Memorandum of Understanding with the National Police Chiefs' Council which determines how information should be shared.

Once the information has been received from the Criminal History System (CHS) or Police National Computer (PNC) this information is stored on a secure server.

Certificates are then printed and enveloped by the print system, the envelopes are sealed automatically.

3. Official monitoring and reporting

There is no official monitoring of the information. Applications are processed and can only be processed if the correct information is supplied. CSGs are audited by Disclosure Scotland's Customer Engagement Team who ensure their information gathering processes etc are compliant with the Code of Practice.

The information gathered is not publically available and cannot be accessed by the public or by a large number of staff within Disclosure Scotland. Information can be used to run management information reports internally. These focus on very high level information such as number of applications received. These reports do not have the capacity to drill down into personal information.

4. Data Transmission and Storage

The Internal Pacific Quay (PQ) Firewall which supports information flows between PQ and SCOTS/CJX is the same Cisco 6513 Firewall that also acts as the inner perimeter firewall for information flows across the internet perimeter. This firewall provides the barrier to protect PVG capabilities from unauthorised CJX end-points. Tuning of the IDS module on the Cisco firewall following go-live will determine the extent to which information exchanges with CJX end-points will be subject to IDS. A/V of all ingest from CJX end-points is conducted on first touch-down on PVG servers on the inside of the Cisco Firewall. As such, all information exchanged with CJX end points is subject to A/V checking within the PVG perimeter, and some of this may be subject to IDS. No additional content validation of CJX information exchanges is conducted. Validation of CJX end-points is managed by IP address validation of the end point. HTTPS and SFTP are used to encrypt information exchanges with CJX and SCOTS end points.

All SCOTS and CJX information flows also pass through a second shared firewall, provided by BT as the SCOTS/CJX service provider. This firewall performs the complementary function to the internal PQ Firewall, protecting SCOTS and CJX end points from PVG capabilities. The firewall is outside of the accreditation scope for PVG, but forms part of the reliance scope, since it also provides an additional level of security for PVG. This additional firewall is physically coexistent with PVG capabilities, but responsibility for management of the firewall lies with BT.

5. Physical Hosting

The PQ, and Central Telephone Exchange ("CTE") sites are located at Pacific Quay Glasgow, and CTE Newcastle respectively. The Live environment at PQ provides the primary operational version of the PVG application. This environment presents the PVG public and business facing web interface, offers live PVG functionality to DS Caseworkers at the Disclosure Scotland Glasgow location, supports "back end" interfaces to CJX end-points, and enables interfaces and other support for STQ supporting capabilities. The Disaster Recovery (DR) environment at CTE is used as an offline environment where data is constantly replicated to from the Live environment and therefore always contains Live data. It is in a dormant state unless DR is invoked. It can also be switched to as an alternative Live environment should the need arise.

Both locations are subject to on-going security inspections and annual audits.

6. Application Management

The PVG system is managed by the Administrative Team in BT secure offices at CTE Newcastle. All administrative staff have SC clearance. No other staff in Disclosure Scotland have administrative access to the systems. The filtering system is managed by SG IT.

7. Backup

There is a policy in place, the Disclosure Scotland PVG Backup Policy. It describes the backup type and where the backup media is stored. A summary of the backup procedures states that the following activities occur:

- Daily incremental backups, retained locally.
- Weekly full backups, are exchanged between CTE and PQ.
- Monthly (four-weekly) are exchanged between CTE and PQ.
- All weekly and monthly backups are transported in locked containers, with tamper-evident seals each sporting a unique serial number.
- Keys for each container are held at each site, in appropriate safes (not the same safe as the backups).
- All tapes are encrypted, so that they can be used only on specific machines
- All tapes are stored in safes appropriate for the value of the information held. At CTE, this is the fire safe in the IL4 Operations Room. A restore exercise is carried out each quarter and rotated across all systems to confirm each environment has undergone a restore from tape exercise at least annually.

Information on what information should be backed up can be found in the Disclosure Scotland PROG SEC SPD – Backup Handling Policy.

8. Business Continuity:

BT provide the PVG DR environment that forms part of Disclosure Scotland's Business Continuity Plan (BCP). End to end BCP is the responsibility of Disclosure Scotland.

9. Legislation

The Data Protection Act 1998 ("the 1998 Act") is the main piece of legislation that deals with storing and processing information. The Act provides a set of principles to ensure that personal information is used only for legitimate purposes. The principles state that personal data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept any longer than necessary;
- processed in accordance with individual's rights;
- kept secure; and
- not transferred abroad without adequate protection.

A 1998 Act compliance check has been carried out as part of this PIA (attached at Annex B). We are content that this complies with the requirements of the 1998 Act.

Human Rights Act (Article 8) - This Article provides that everyone has the right to respect for his private and family life, his home and his correspondence.

The handling and processing of information by Disclosure Scotland does not infringe this right.

Code of Practice

The Scottish Ministers' Code of Practice on Records Management by Scottish Public Authorities, has been considered for the permanent arrangements. The storage of clerical information will be carried out in accordance with good practice in records management as detailed in the Code of Practice.

10. Future actions

The data sharing processes are the same for the amended system as they were for the previous system. There will be no change to this system unless there is a significant change in the law regarding the disclosure regime in Scotland and/or a change to the operational systems currently in place at Disclosure Scotland.

Any changes to the above will be made only following consultation and consideration of any privacy impacts.

11. Conclusion

We have conducted this PIA to establish the risks and the mitigation of these risks, in terms of privacy, to the information that we will be handling, and storing.

This PIA has identified that there is no change to the 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.

12. Authorisation and publication

The PIA report should be signed by your Information Asset Owner (IAO). The IAO will be the Deputy Director or Head of Division.

Before signing the PIA report, an IAO should ensure that she/he is satisfied that the impact assessment is robust, has addressed all the relevant issues and that appropriate actions have been taken.

By signing the PIA report, the IAO is confirming that the impact of applying the policy has been sufficiently assessed against the individuals' right to privacy.

The results of the impact assessment must be published in the eRDM with the phrase "Privacy Impact Assessment (PIA) report" and the name of the project or initiative in the title.

Details of any relevant information asset must be added to the Information Asset Register, with a note that a PIA has been conducted.

I confirm that the impact of The Police Act 1997 and the Protection of Vulnerable Groups (Scotland) Act 2007 Remedial Order 2018 has been sufficiently assessed against the needs of the privacy duty:

Name and job title of a Deputy Director or equivalent	**Date each version authorised**
K L Gill CHIEF EXECUTIVE	13/02/18.

Privacy Impact Assessment - Mitigation Summary **Annex A**

Questions to identify Privacy Issues	Answer and Risk rating	Mitigation
1. Does the proposal include the use of new or additional technologies with the potential for privacy intrusion?	No –**Low**	
2. Identity: Does the proposal include new identifiers, or substantially change or re-use existing identifiers or any intrusive or onerous identification, authentication or identity management processes?	No -**Low**	There is no change to the information collected.
3. Identity: Does the proposal affect anonymity or pseudonymity; will previously anonymous or pseudonymous transactions be identified?	No -**Low**	As above.
4. Is the justification for the proposal either unpublished or unclear?	No -**Low**	
4. a) Does the proposal involve new or changed data collection policies or practices that may be unclear or intrusive?	No -**Low**	Existing data collection techniques have been tried and tested under the previous regime.
4. b) Does the proposal involve new or changed quality assurance or security processes or standards that may be unclear and/or unsatisfactory?	No -**Low**	Existing data collection techniques have been tried and tested under the previous regime.
4. c) Does the proposal involve new or changed data access or disclosure arrangements that may be unclear or permissive?	No -**Low**	Existing data collection techniques have been tried and tested under the previous regime.
4. d) Does the proposal involve new or changed data retention processes that may be unclear or extensive?	No -**Low**	As above.
4. e) Does the proposal involve a new or changed medium or method of disclosure for publicly available information so data is more readily accessible?	No -**Low**	As above.

5. Will the proposal involve multiple organisations, either government agencies (e.g. 'joined-up government' initiatives) or the private sector?	Yes – **Low**	No change in the information exchange or the processes. Only change is the group of individuals able to apply to a Sheriff.
6. Does the proposal involve personal data of particular concern to individuals?	Yes – **Medium - Low**	Names, D.O.B, addresses, NI Number and conviction information. The information is securely transmitted and held.
7. Does the proposal involve the linkage of personal data with data in other collections, or any significant change to existing data links or holdings?	No - **Low**	No
8. Will the proposal handle a significant amount of data about each person, or significantly change existing data-holdings?	No - **Low**	The process will not handle information other than what is required to process the appeals.
9. Will the proposal handle data about a significant number of people, or change significantly the existing population scope or coverage?	No - **Low**	No, the number of anticipated appeals is very low.
10. Does the proposal consolidate, inter-link, cross-reference or match personal data from multiple sources?	Yes – **Low**	Yes, matching will be done with information held on Police databases (PNC & CHS). This process has not changed.
11. Is the proposal to process any data that is exempt from legislative privacy protections?	No - **Low**	We have no plans to process any data that may be exempt from legislative privacy protections.
12. Does the proposal's justification include significant contributions to public security measures?	No - **Low**	There should be no impact on public security measures as a result of these changes.
13. Does the proposal intend to disclose personal data to, or access by, third parties that are not subject to EU or comparable privacy regulation?	No - **Low**	We do not intend to disclose any data to anyone or anywhere that is not subject to EU or comparable privacy regulations.

Data Protection Act 1998 Compliance Check Annex B

1. What type of personal data is going to be processed?
Names, addresses, NI Numbers and conviction information.

2. Which of the grounds in schedule 2 of the DPA will provide a legitimate basis for the processing?
We consider that Schedule 2 Condition 5 (d) is appropriate. Schedule 2 Condition 5 (d), states that "The processing is necessary for the functions of a public nature exercised in the public interest by any person"

3. If sensitive personal data is going to be processed, which of the grounds in schedule 3 (in addition to the schedule 2 grounds) will provide a legitimate basis for that processing?
Sensitive personal data is personal data consisting of information as to (a) the racial or ethnic origin of the data subject, (b) their political opinions, (c) their religious beliefs, (d) whether they are a member of a Trade Union, (e) their physical or mental health, (f) their sexual life, (g) the commission or alleged commission by them of any offence and (h) any proceedings for any offence committed or alleged to have been committed by them.

In accordance with the Act, information to be received, stored, and processed will be classified as "sensitive personal data".
To meet the second requirement we consider that Schedule 3 Condition 1 is appropriate. It states that "The data subject has given his explicit consent to the processing of the personal data."

In completing the application form the applicant will have signed to declare that they understand "… Disclosure Scotland may pass the information it holds about me to other Government departments or organisations, the police and other law enforcement agencies for the purposes of the prevention and detection of crime, of the apprehension and prosecution of offenders and for other related purposes..." and this declaration is the consent provided by the data subject.

Condition 7(c) will also apply, -"the exercise of any function of the Crown, Minister of the Crown or government department."

4. Are there any special considerations relating to Article 8 of the Human Rights Act that will not be covered by the PIA?
This Article provides that everyone has the right to respect for his private and family life, his home and his correspondence.

There are no special considerations not covered by this PIA

5. Will any of the personal data be processed under a duty of confidentiality? If yes, how is that confidentiality being maintained?
No

6. How are individuals being made aware of how their personal data will be used?
Individuals are informed on the "declaration" section of the application. There is extensive information and guidance on Disclosure Scotland's website. Information on the appeals process will be provided to the applicant, as is already the case.

7. Does the project involve the use of existing personal data for new purposes?
No

8. What procedures will be in place for checking that the data collection procedures are adequate, relevant and not excessive in relation to the purpose for which the data will be processed?
The process for collecting data is stated above in the section headed "How is information passed to Disclosure Scotland?"

9. How will the personal data be checked for accuracy?
Validation checks are in place as stated in the section on "How is information passed to Disclosure Scotland?

10. Has the personal data been evaluated to determine whether its processing could cause damage or distress to data subjects?
Yes – It has been determined that as the applicant has requested the disclosure certificate, they are aware of what information may be processed and shared with CSGs, therefore it is unlikely to cause damage or distress. The decision to appeal is made by the individual and they will be fully informed of its implications.

11. Will there be set retention periods in place in relation to the storage of the personal data?
Disclosure Scotland hold this information indefinitely. The PVG Scheme is one of continuous monitoring. Disclosure Scotland are in the process of reviewing their retention periods.

12. What technical and organisational security measures will be in place to prevent any unauthorised or unlawful processing of the personal data?
The section "How is information passed to Disclosure Scotland?" details the technical and organisational security arrangements for the security of the information.

13. Will you be transferring personal data to a country outside of the European Economic Area? If so where, and what arrangements will be in place to ensure that there are adequate safeguards over the data?
No.

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: 978-1-78851-599-3 (web only)

Published by The Scottish Government, February 2018

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS362446 (02/18)