

# **The Social Security Information-sharing (Scotland) Amendment Regulations 2024**

## **Data Protection Impact Assessment**

# DPIA for legislation for the Suspected risk of harm proposal to create regulations

## 1. Summary of proposal

Proposed regulations (the Social Security Information-sharing (Scotland) Amendment Regulations 2024) making provision to:

- Share the personal data of Social Security Scotland clients, or members of the clients household, with appropriate authority when there is a suspected risk of harm identified by our employees during our interactions.
- Share the information with the appropriate authority who are:  
Local Authorities  
Office of the Public Guardian (OPG)

This data sharing may include special category health data if the data is necessary to the suspected risk of harm being reported.

As part of this process, a detailed operational Data Protection Impact Assessment will be completed to identify and mitigate risk to data subject rights and freedoms.

## 2. Department

Social Security Policy Division, Scottish Government

## 3. Data protection support email

[dataprotectionofficer@gov.scot](mailto:dataprotectionofficer@gov.scot)

## 4. Is your proposal primary legislation, secondary legislation or other form of statutory measure?

We launched a public consultation<sup>1</sup> between 25 March 2022 and 17 June 2022 on proposals to develop regulations to create an explicit legal gateway, which enables the sharing of information with Local Authorities and the OPG where an employee of Social Security Scotland suspects risk of harm to a client or a member of their household. Under the proposed Social Security Information-sharing (Scotland) Amendment Regulations 2024 this information would be shared by way of an explicit legal gateway under section 85(5) and 95 of the Social Security (Scotland) Act 2018. We are of the view that in taking this approach it will ensure the law is clear and easily accessible.

In the interim we have been using the following lawful basis and legal gateway should we need to share such information where there is a suspected risk of harm to a client or a member of their household: -

Lawful basis –

---

<sup>1</sup> [Safeguarding data sharing: consultation - gov.scot \(www.gov.scot\)](https://www.gov.scot/publications/consultations/data-sharing/consultation-2022-03-25-17-june-2022/html)

Safeguarding considerations around children and vulnerable adults falls within the definition given by Section 8 of the Data Protection Act 2018 (DPA 2018) and Art 6(1)(e)<sup>2</sup> to justify the lawful processing of information relating to suspected risk of harm (section 8(a) and (c) of the Data Protection Act 2018 are most relevant).

There is an additional requirement for processing special category of personal data, under article 9 of UK-GDPR 9(2)(g) provides an exception:

(g) processing is necessary for reasons of substantial public interest, on the basis of [domestic law] which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

Section 10(3) of the DPA 2018<sup>3</sup> makes further provision for the lawful processing of personal data in the UK under Article 9(2)(g) of the UK GDPR, and relevantly one of those conditions is set out at para. 18 of Part 2 of Schedule 1 of the DPA 2018<sup>4</sup>, safeguarding of children and of individuals at risk.

We have an appropriate policy document in place in relation to the data sharing that:

-

- explains Social Security Scotland's procedures for securing compliance with the principles in Article 5 of the UK-GDPR (principles relating to processing of personal data); and
- explains Social Security Scotland's policies for the retention and deletion of the data, giving an indication of how long such personal data is likely to be retained.

The lawful basis for the proposed Social Security Information-sharing (Scotland) Amendment Regulations 2024 will be the same as the ones used in the interim process described above.

Legal Gateway –

The legal gateway used in the interim sharing process described above is found in Section 1A of the NHS(S) Act 1978.<sup>5</sup>

The proposed Social Security Information-sharing (Scotland) Amendment Regulations 2024 will provide a bespoke, social security-specific legal gateway once they come into force on 16 January 2024.

**5. What stage is the legislative process at? Please indicate any relevant timescales and deadlines.**

---

<sup>2</sup> [Data Protection Act 2018 \(legislation.gov.uk\)](https://legislation.gov.uk/ukpga/2018/12/section/8)

<sup>3</sup> [Data Protection Act 2018 \(legislation.gov.uk\)](https://legislation.gov.uk/ukpga/2018/12/section/10)

<sup>4</sup> [Data Protection Act 2018 \(legislation.gov.uk\)](https://legislation.gov.uk/ukpga/2018/12/schedule/1/paragraph/18)

<sup>5</sup> [National Health Service \(Scotland\) Act 1978 \(legislation.gov.uk\)](https://legislation.gov.uk/ukpga/1978/12/section/1a)

We issued a public consultation ending in June 2022 on the proposals for legislation. Our Ministers are content and legislation will be prepared and come into force on 16 January 2023.

In the interim while the legislation is being developed we will report any cases of suspected harm using the lawful basis and legal gateway detailed in relation to the interim process mentioned above.

**6.** Have you consulted with the ICO using the Article 36(4) form

Yes

**7.** If the ICO has provided feedback, please include this.

The ICO are satisfied that the 36(4) process is complete.

**8.** Do you need to hold a public consultation and if so has this taken place

Yes the public consultation is now complete

**9.** Were there any comments/feedback from the public consultation about privacy, information or data protection?

Six respondents acknowledged Social Security Scotland requiring to work within the requirements of the Data Protection Act and the Information Commissioners Office.

Article 35(7)(a) – “purposes of the processing, including, where applicable, the legitimate interest pursued by the controller”

**10.** What issue/public need is the proposal seeking to address? What policy objective is the legislation trying to meet?

The Scotland Act 2016 made provision to devolve limited aspects of social security powers to Scottish Ministers, including 11 social security benefits.

Over 700,000 people are currently in receipt of UK disability and carer benefits that will be replaced by Scottish forms of assistance, and responsibility for delivering benefits for these people will require to be transferred from the DWP to Social Security Scotland.

The Adult Support and Protection (Scotland) Act 2007 outlines the obligation on public bodies to safeguard wellbeing. As Social Security Scotland did not exist when this Act came into force, we have had to factor these requirements in as a new government body.

The policy objectives the legislation is trying to meet are to balance the Government’s responsibilities and obligations of keeping people safe and meeting

their duty of care, along with complying with privacy and confidentiality obligations under data protection law and Article 8 ECHR

We will be processing client data in order to meet obligations set out in the Social Security Scotland's general duty to give assistance in s24 of the 2018 Act. <sup>6</sup>

Whilst undertaking these duties such as client communications, receiving digital applications, phone calls, and attending home visits in connection with this general duty, there are situations where we may encounter suspected risk of harm. Based on the volumes of clients we may engage with we believe there is a high likelihood we will encounter scenarios we may need to report to Local Authorities or Office of the Public Guardian.

Article 35(7)(c) "assessment of the risks to the rights and freedoms of data subjects" and Article 35(7)(b) "...necessity and proportionality of the processing operations"

**11.** Does your proposal relate to the processing of personal data? If so, please provide a brief explanation of the intended processing and what kind of personal data it might involve. Who might be affected by the proposed processing?

Intended processing.

The proposal outlined would process personal data in the instance a social security Scotland employee believes a client, or a member of their household, to be at risk of harm. The personal data would be passed onto the appropriate authority such as Local Authority/Office of the Public Guardian.

The data has been minimised to allow completion of the referral and will include the clients name, address and description of the suspected risk of harm.

**12.** Is the processing considered necessary to meet a policy aim? Is there a less invasive way to meet the objective (for example, anonymising data, processing less data).

How it meets the policy aim.

Only the minimum amount of data required for reporting the suspected risk of harm will be shared with an appropriate authority to allow them to investigate.

For the interim period until we introduce the legislation the information in the suspected risk of harm referral will be reviewed by the safeguarding team and Caldicott Guardian to assess proportionality then securely store, only the Authority name, date, reported suspected risk and client reference number will be stored as the detail of the suspected risk of harm will have been disclosed to the appropriate authority. An operational DPIA has been conducted ensuring UK GDPR principles are embedded in the design.

---

<sup>6</sup> [Social Security \(Scotland\) Act 2018 \(legislation.gov.uk\)](https://www.legislation.gov.uk)

**13.** Please also specify if this personal data will be sensitive or special category data or relate to criminal convictions or offences. (Note: 'special categories' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data about a person's sex life or sexual orientation and sensitive personal data means criminal information or history).

Special category, sensitive information and data relating to criminal convictions or offences.

Yes, health data may be shared if appropriate to the situation.

As part of the referral to the appropriate authority there may be inference to the data subject's residence in a care facility, this would be in the case of a client who has a corporate acting body e.g. care home is the corporate acting body and would have made the application to benefit on behalf of the client.

Part of your consideration in relation to Article 35(7)(a) and (b) should be in respect of ECHR.

**14.** Will your proposal engage any rights under ECHR, in particular Article 8 ECHR? How will the proposal ensure a balance with Article 8 rights? If the proposal interferes with Article 8 rights, what is your justification for doing so – why is it necessary?

Yes.

The proposal is necessary to allow the appropriate authority to safeguard the client or other member of the clients household against potential physical, mental or emotional harm.

To ensure reporting is appropriate and proportionate all cases will be reviewed by the Caldicott guardian and safeguarding team before sharing with the appropriate authority. In the first instance the case will be discussed anonymously and Local Authorities will then advise in their professional capacity if the case should be referred for them to investigate. The process flowing from the new regulations will also be underpinned by robust guidance to ensure fair decision making when sharing.

There is a potential question to be raised around article 8 ECHR, as we are proposing to share information with Local Authorities and the OPG in cases where there is a real risk of harm, but not immediate risk and of significant harm. However, the propose sharing is justified on public interest grounds, has been supported in the public consultation and the regulations contain appropriate safeguards for sharing

It is of note at this juncture that the Department for Work and Pensions have such processes in place for their clients identified as being at risk of harm, and it is many of these clients who will be transferring to Social Security Scotland to administer their benefits.

Article 35(7)(b) "...necessity and proportionality of the processing operations"  
Article 35(7)(c) "assessment of the risks to the rights and freedoms of data subjects"  
Article 35(7)(d) "measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with [UK GDPR] taking into account the rights and legitimate interests of data subjects and other persons concerned"  
Note Article 32 UK GDPR for s.4 also

**15.** Will the proposal require regulation of :

- technology relating to processing
- behaviour of individuals using technology
- technology suppliers
- technology infrastructure
- information security

No

**16.** Please explain if the proposal will have an impact on the use of technology and what that impact will be.

No

**17.** Will the proposal require establishing or change to operation of an established public register (e.g. Accountancy in Bankruptcy, Land Register etc.) or other online service/s?

No

Article 35(7)(b) "...necessity and proportionality of the processing operations"  
Article 35(7)(c) "assessment of the risks to the rights and freedoms of data subjects"  
\*Note exemptions from UK GDPR principles where applicable

**18.** Please provide details of whether the proposal will involve the collection or storage of data to be used as evidence or use of investigatory powers (e.g. in relation to fraud, identify theft, misuse of public funds, any possible criminal activity, witness information, victim information or other monitoring of online behaviour)

We will retain the minimum amount of data required as a record in case the authority needs to come back to us for any clarification. The record will contain:

- Client name/other household members name
- The suspected risk of harm
- Date reported
- Authority shared with
- Reason for non-referral

The appropriate authority will retain the details of the reason for referral allowing them to investigate if necessary.

Article 35(7)(b) "...necessity and proportionality of the processing operations"  
Article 35(7)(c) "assessment of the risks to the rights and freedoms of data subjects"  
Article 35(7)(d) "measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with [UK GDPR] taking into account the rights and legitimate interests of data subjects and other persons concerned"

**19.** Would the proposal have an impact on a specific group of persons e.g. children, vulnerable individuals, disabled persons, persons with health issues, persons with financial difficulties, elderly people? (Please specify) In what way?

This proposal relates to the collection of data and information in relation to clients, or members of the clients household, applying for or receiving benefits administered by Social Security Scotland.

As such the group may contain children, vulnerable individuals, disabled persons, persons with health issues, persons with financial difficulties and elderly people.

**20.** Will the Bill necessitate the sharing of personal data to meet the policy objectives? For example

- From one public sector organisation to another public sector organisation;
- From a public sector organisation to a private sector organisation, charity, etc.;
- Between public sector organisations;
- Between individuals (e.g. practitioners/ service users/sole traders etc.);
- Upon request from a nominated (or specified) organisation?

(If so, does the Bill make appropriate provision to establish a legal gateway to allow for sharing personal data Please briefly explain what the gateway will be and how this then helps meet one of the legal basis under Article 6 of the UK GDPR).

The sharing will take place between public sector organisations Social Security Scotland, the Local Authority or Office of the Public Guardian.

The legal gateway has to be established, this is intended to be carried out via powers under Section 85(5) and Section 95 of the 2018 Act.

**21.** Is there anything potentially controversial or of significant public interest in the policy proposal as it relates to processing of data? For example, is the public likely to view the measures as intrusive or onerous? Are there any potential unintended consequences with regards to the provisions e.g. would the provisions result in unintended surveillance or profiling. Have you considered whether the intended processing will have appropriate safeguards in place? If so briefly explain the nature of those safeguards and how any safeguards ensure the balance of any competing interests in relation to the processing.

As mentioned above, there is a potential for questions to be raised around article 8 ECHR, as we are proposing to share information with Local Authorities and the OPG

in cases where there is a real risk of harm rather than an immediate risk of significant harm. However, the propose sharing is justified on public interest grounds, has been supported in the public consultation and the regulations contain appropriate safeguards for sharing

**22.** Are there consequential changes in other legislation that need to be considered as a result of the proposal or the need to make further subordinate legislation to achieve the aim? (This might include, for example, regulation or order making powers; or provisions repealing older legislation; or reference to existing powers (e.g. police or court powers etc.).)

No

**23.** Will this proposal necessitate an associated code of conduct? If so, what will be the status of the code of conduct (statutory, voluntary etc.)?

No

**24.** Do you need to specify a Data Controller/s?

Social Security Scotland are data controllers and will retain a record that information was provided to an authority and the appropriate authority will be data controller of the information we share with them about the suspected risk of harm.

**25.** Have you considered whether the intended processing will have appropriate safeguards in place, for example in relation to data security, limitation of storage time, anonymisation? If so briefly explain the nature of those safeguards. Please indicate how any safeguards ensure the balance of any competing interests in relation to the processing.

The existing safeguarding measures will remain in place for new cases which include:

- Retention schedule to delete or anonymise personal data where there is no longer purpose to retain.
- Data minimisation of the information we will retain.

The new regulations themselves also contain consent provisions that act as a safeguard in the regs for sharing and information will only be shared with consent unless specific tests, as set out in the regulations, for non-consensual sharing are met. There is also the general provision in the principal Social Security Information-sharing (Scotland) Regulations 2021 (that the new regulations will amend) that no more information than is necessary will be shared, which will also apply to the provisions allowing sharing inserted by the new regulations.

**26.** Will the processing of personal data as a result of the proposal have an impact on decisions made about individuals, groups or categories of persons? If so, please

explain the potential or actual impact. This may include, for example, a denial of an individual's rights or use of social profiling to inform policy making.

No Social Security Scotland will not be involved in any decision making this will be appropriate authority's responsibility.

**27.** If the proposal involves processing, do you or stakeholders have any relevant comments about mitigating any risks identified in the DPIA including any costs or options, such as alternative measures?

Social Security Scotland are of the view that public task, as set out above, is the appropriate lawful basis for processing information where there is a suspected risk of harm. In addition, using section 1A of the 1978 Act as a legal gateway as an interim solution to share data relating to the suspected risk of physical or mental harm. As noted above, suspected risk of harm would require to be limited to risk of harm to health (physical or mental) to a person and could not extend to financial harm. Whilst we are confident we can rely on these powers to share information in the manner set out above, we remain concerned as to how clear and easily accessible the law is and for this reason Social Security Scotland should still proceed to set this out by way of regulations under section 85(5) (and possibly section 95) of the 2018 Act.

If we retain more data than is required to keep our record then we will be holding information without business purpose this could result in data subjects rights and freedoms being potentially impacted; reduced understanding of the breadth of data involved in a data breach, and a breach of data protection compliance

If there are no processes in place employees may choose to take their own personal action and report outside the organisation resulting in data subject's rights and freedoms being potentially impacted and a breach of data protection compliance.

Our mitigation is to create a formal process with robust controls and guidance to allow any data share whilst protecting the individual, employee and organisation.

## **28.** Authorisation

The DPIA report should be signed by your Information Asset Owner (IAO). The IAO will be the Deputy Director or Head of Division or the relevant person in the business area sponsoring the Bill/proposals.

Before signing the DPIA report, an IAO should ensure that she/he is satisfied that the impact assessment is robust and has addressed all the relevant issues.

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

The results of the impact assessment must be published in the eRDM with the phrase "Legislative DPIA" 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 DPIA has been conducted.

I confirm that the impact of the suspected risk of harm (Scotland) Regulations 2023 has been sufficiently assessed in compliance with the requirements of the UK GDPR

Name and job title of a IAO or equivalent: Ian Davidson, Deputy Director of Social Security Policy Division

Date each version authorised: 03 November 2023



© Crown copyright 2023

**OGL**

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit [nationalarchives.gov.uk/doc/open-government-licence/version/3](https://nationalarchives.gov.uk/doc/open-government-licence/version/3) or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: [psi@nationalarchives.gsi.gov.uk](mailto:psi@nationalarchives.gsi.gov.uk).

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at [www.gov.scot](http://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: 978-1-83521-699-6 (web only)

Published by The Scottish Government, December 2023

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA  
PPDAS1386134 (12/23)

**W W W . g o v . s c o t**