

The Mutual Recognition of Supervision Measures in the European Union (Scotland) Regulations 2014 - Privacy Impact Assessment (PIA)

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 Mutual Recognition of Supervision Measures in the European Union (Scotland) Regulations 2014 ('the ESO').

2. Document metadata

2.1 Name of project: Mutual Recognition of Supervision Measures in the European Union (Scotland) Regulations 2014.

2.2 Date of report: 29 August 2014.

2.3 Author of report: Neil Robertson – Criminal Justice Division – EU Implementation Team.

2.4 Information Asset Owner: Elspeth MacDonald, Deputy Director.

2.5 The Privacy Impact Assessment will be reviewed if any concerns are highlighted by stakeholders once the policy is in force.

3. Description of the project

3.1 The ESO enhances the mutual recognition of judicial decisions relating to non-custodial pre-trial supervision of accused persons in criminal proceedings (such as bail). Mutual recognition of judicial decisions is the process by which a decision taken by a judicial authority in one Member State is recognised and enforced by another as if it were taken by the judicial authorities of that other Member State. The aim for the ESO is, in certain circumstances, to allow an accused person to return home and be supervised there until their trial takes place in the Member State where the offence took place.

Accordingly the Regulations set out in Scots law provide the framework to allow, in certain circumstances, a suspected person to return home and be supervised there until their trial takes place in the Member State where the offence takes place, in terms which are in accordance with the provisions of the Directive.

The Regulations specify that Scotland, as part of the UK Member State, must recognise and monitor supervision measures that impose an obligation on the accused person concerned to :

- inform the authority monitoring the supervision measures of any change of residence;
- not enter certain locations;
- stay at a specified location;
- comply with certain restrictions for leaving the territory of the monitoring country;
- report at specified times to the designated authority; and
- refrain from contacting specific persons connected to the alleged crime.

The ESO requires the Competent or Central Authority in the issuing Member State to forward the decision on the supervision measures, accompanied by a certificate detailing the types of measures imposed including an estimate of the amount of time they will last and other details, to the Competent or Central Authority in the executing Member State where the accused person is lawfully and ordinarily residing.

The ESO must be transposed into Scot's law by 1 December 2014 as part of the UK's opt-in to a number of Justice and Home Affairs Directives. Failure to opt-in may result in infraction proceedings against the UK and reputational damage.

3.2 Describe the personal data to be processed.

Personal data about an accused person in the following categories will be processed:

Name, Alias, Sex, Nationality, Identity or Social Security Number, Date of Birth, Place of Birth, Address, Languages spoken, Identity Card or Passport Number, Offences accused of (including a summary of facts), conditions of bail to which the accused is subject.

3.3 Describe how this data will be processed:

The data will be gathered during the course of criminal and court proceedings brought against an accused person. It will be accessed by the Crown Office and Procurator Fiscal Service ('COPFS'), Police Scotland ('PS') and Scottish Court Service ('SCS') in line with current protocols. Information will be shared with the Competent Authorities of EU member states. Within Scotland data will be transmitted, stored, disposed of, owned and managed in line with current Integration of Scottish Criminal Justice Information Systems (ISCJIS) protocols. EU member states are subject to the [EU data protection Directive](#) and thus a similar level of protection will be afforded to information supplied to them.

3.4 If this data is to be shared with internal or external partners, explain the legal basis for the sharing.

The ESO is EU law and the EU Framework Decision provides the underpinning legal basis for the sharing of data.

4. Stakeholder analysis and consultation

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

Scottish Government officials: responsible for transposition of the EU Framework Directive.

COPFS, SCS and PS: responsible for the day to day operation of the ESO upon implementation.

4.2 Detail the method used to consult with these groups when making the PIA.

A series of meetings have been held between Scottish Government officials and the relevant justice partners.

4.3 Discuss the means used to communicate the outcomes of the PIA with the stakeholder groups.

The PIA was copied to stakeholder groups as part of the submission of the ESO draft instrument.

5. Questions to identify privacy issues

5.1 Involvement of multiple organisations

- The ESO will involve COPFS, PS, SCS and other partners from the wider EU.

5.2 Anonymity and pseudonymity

- The project does not require the matching of data sources together.

5.3 Technology

- There be no new or additional information technologies that have substantial potential for privacy intrusion.

5.4 Identification methods

- Existing unique identifiers (Identity Card, Passport, National Insurance and Identity numbers) will be re-used.
- There be no new or substantially changed identity authentication requirements that may be intrusive or onerous.

5.5 Personal data

- There will be new or significant changes to the handling of types of personal data that may be of particular concern to individuals. Sensitive personal data will be shared with the Central Authorities of EU member states (as is currently the case with the European Arrest Warrant).
- There will be no new or significant changes to the handling of personal data about a large number of individuals. It is estimated that the ESO will impact approximately 14 individuals per year.
- There be no new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources.
- The project will not involve the linkage of personal data with data in other collections, or any significant change to existing data links or holdings.

5.6 Changes to data handling procedures

- There will be no new or changed data collection policies or practices that are unclear or intrusive.
- There will be no changes to data quality assurance or processes and standards that are unclear or unsatisfactory.
- There will be no new or changed data security access or disclosure arrangements that are unclear or extensive.
- There will be no new or changed data retention arrangements that are unclear or extensive.
- There will be no changes to the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before.
- When sent by email, data will be transferred through the secure Police National Network. If sent by post, recorded delivery or international recorded delivery will be used.

5.7 Statutory exemptions/protection

- Section 29(1)(b) of the Data Protection Act 1988 provides that personal data processed “for the purposes of the apprehension or prosecution of offenders” are exempt from the first data protection principle (that data must be processed fairly and lawfully), except to the extent that it requires compliance with the conditions in Schedules 2 and 3 (which set out the conditions relevant to the processing of personal and sensitive personal data).

- Additionally, section 35(1) exempts personal information from the non-disclosure provisions (as defined in section 27(3) of the DPA) where the disclosure is “required by or under any enactment, by any rule of law or by the order of the court”. As we are subject to (and transposing) EU law, by definition anything done under its power is allowed under the DPA. Additionally, section 35(2)(a) exempts personal data from the non-disclosure provisions where that disclosure is necessary “for the purpose, or in connection with any legal proceeding”.
- Where the data being processed is sensitive personal data, the exemptions do not go so far as to remove the requirement that at least one of the conditions in both Schedule 2 and Schedule 3 are met. In this case, the “administration of justice” condition in paragraph 5(a) of Schedule 2 and paragraph 7(1)(a) of Schedule 3 would appear to be clearly met. There is no need for consent from the data subjects.
- The project does not involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation. EU justice partners are subject to EU data protection Directive.

5.8 Justification

- The project contributes to public security measures by allowing accused persons to be subject to supervision measures in other EU member states.
- The justification for the new data handling procedure is contained within the EU Framework Decision and the policy note that accompanies the proposed regulations.

5.9 Other risks

- There are no risks to privacy not covered by the above questions.

6. Risks identified and appropriate solutions or mitigation actions proposed

Is the risk eliminated, reduced or accepted?

Risk	Solution or mitigation	Result
Sensitive personal data is being shared out with ISCJIS, with EU justice partners.	The regulations do not propose to disclose personal data to, or access by, third parties that are not subject to EU or comparable privacy legislation.	Eliminate.
Sensitive personal data is being transferred out with ISCJIS.	Personal/sensitive data will be transferred securely, using normal secure process, via police national network or recorded/international recorded delivery.	Minimised.

7. 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	How risk will be incorporated into planning	Owner
Sensitive personal data is being shared out with ISCJIS, with EU justice partners.	The risk will be incorporated into planning by ensuring that the regulations identify that the information can only be shared with the Central or Competent Authority in another EU member state.	Neil Robertson
Sensitive personal data is being transferred out with ISCJIS.	The risk will be incorporated into planning by ensuring that information is shared using normal secure processes that are currently used for other data transfers e.g. transfer of financial penalties.	Neil Robertson

8. 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 European Supervision Order has been sufficiently assessed against the needs of the privacy duty:

Elsbeth MacDonald Deputy Director, Criminal Justice 	Date each version authorised 6th November 2014
---	--