Home Office

Detention Services Order 02/2015

Regulation of Investigatory Powers Act 2000 (RIPA)

July 2023

© Crown copyright 2023

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 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.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.uk/government/collections/detention-service-orders

Any enquiries regarding this publication should be sent to us at DSOConsultation@homeoffice.gov.uk

Contents

Document Details

Process: To make all staff aware of the legislative requirements of the Regulation of Investigatory Powers Act 2000 (RIPA), and how they relate to surveillance within a Home Office immigration removal centre.

Implementation Date: February 2015 (reissued July 2023)

Review Date: July 2025

Version: 4.0

Contains Mandatory Instructions

For Action: Immigration removal centres (IRCs), pre-departure accommodation (PDA) and residential short-term holding facilities (RSTHFs).

For Information: Escorting Officers

Author and Unit: Kate Gowans, Detention Services Security Team, Detention Services

Owner: Michelle Smith, Head of Detention Operations

Contact Point: Detention Services Security Team

Processes Affected: Surveillance undertaken within the removal estate.

Assumptions: All staff will have the necessary knowledge to follow these procedures.

Notes:

Instruction

Introduction

1. This order provides guidance on the legislative requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) to all staff in Home Office immigration removal centres (IRCs), pre-departure accommodation (PDA) and residential short-term holding facilities (STHFs).

2. This DSO does not apply to those detained in a non - residential STHF or Residential Holding Rooms (RHRs).

3. RIPA provides a framework to ensure investigatory techniques are used in a way that is compatible with the Article 8 right to respect for private and family life, enshrined in the European Convention on Human Rights (ECHR). RIPA ensures that these techniques are used in a regulated way and provides safeguards against the abuse of such methods. Use of these covert techniques will only be authorised if considered legal, necessary and proportionate.

Purpose

4. The purpose of this order is to ensure that all staff within the removal estate, as well as escorting staff, are fully aware of RIPA and how it applies to surveillance and other covert techniques within a detention facility or to escorting activity. References to “centre” in this document cover IRCs, RSTHFs, PDA and escort activity.

Policy

5. RIPA sets out the authorisation requirements for all covert surveillance carried outby public authorities where that surveillance is likely to result in the obtaining of private information about a person.

6. Surveillance, for the purposes of RIPA, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

7. Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place.

Procedures

8. Staff in centres can undertake general observations, or surveillance, as part of their daily duties.

9. Surveillance in a centre could include overt activity such as general observations of detained individuals and routine monitoring of overt CCTV cameras or body worn cameras.

10. In accordance with RIPA, the use of overt camera systems for general observational duties, such as CCTV or body worn cameras, does not normally require an authorisation. Members of the public should be made aware that such systems are in use. For example, by virtue of cameras or signage being clearly visible[1].

Authorisation procedures for directed surveillance

11. Staff can also undertake covert observations, which are carried out discreetly to ensure the detained individual who is being monitored is unaware that the surveillance is taking place. The planned use by supplier security staff of covert techniques to investigate detained individuals or other individuals in a centre, without alerting them to the fact that they are under investigation, is likely to require a directed surveillance authorisation under RIPA. Directed surveillance is defined in section 26(2) RIPA as surveillance which is covert, but not intrusive, and:

a) Undertaken for the purposes of a specific investigation or specific operation;

b) Conducted in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

c) Is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of RIPA to be sought for the carrying out of the surveillance.

12. Where overt CCTV cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance authorisation is likely to be required. Such covert surveillance is likely to result in the obtaining of private information about a person (namely, a record of their movements and activities) and therefore falls properly within

[1] The Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 sets out a framework of good practice that includes existing legal obligations, including the processing of personal data under the data protection legislation and a public authority's duty to adhere to the Human Rights Act 1998.

the definition of directed surveillance. The use of the CCTV system in these circumstances goes beyond their intended use for the general prevention or detection of crime and protection of the public.

13. Covert surveillance activity does not require application or authorisation when it takes place as an immediate response to an event or during a patrol, rather than being pre-planned. Once directed surveillance is considered operationally necessary by the IRC centre manager, an application detailing the need for surveillance should be completed by a member of the IRC security team (the applicant) and the security manager should forward the application to the Home Office Central Authorities Bureau (CAB) and relevant Home Office Compliance Team Area Manager (Grade SEO or above) via the agreed process. Staff should note that surveillance can only be sought for purposes related to the prevention and detection of crime or in the interests of public safety. The CAB will quality assure the surveillance application to assure its compliance with the legislation before passing to the Home Office authorising officer for authorisation.

14. The Home Office authorising officer[2] must believe that the proposed surveillance is necessary and proportionate to what is sought to be achieved or surveillance will not be authorised. This involves balancing the intrusiveness of the activity on the individual or individuals subject to the surveillance and others who might be affected by it (known as collateral intrusion), against the need for the activity in operational terms. Collateral intrusion is defined in the Covert Surveillance and Property Interference Revised Codes of Practice 2018 4.11 as:

> ".. the risk of obtaining private information about persons who are not subjects of the surveillance activity…."

15. The application for an authorisation should include an assessment of the risk of any collateral intrusion and details of what measures are being taken to limit this. The authorising officer will take this into account, when considering the proportionality of the proposed surveillance.

16. The authorising officer must give authorisations in writing, except in urgent cases when they may be given orally by the authorising officer. An urgent case for oral authorisation should only be made if the applicant believes that the time required for an authorising officer to grant a written authorisation would, in the applicant's judgement, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being sought.

17. In such cases contact should first be made with the CAB to confirm the case meets the urgent oral criteria. The applicant will then be put in contact with the authorising officer to discuss the case. Both the applicant and authorising officer should make contemporaneous notes of their conversation and record the date and time the

[2].. The authorising officer for surveillance within IRCs is a prescribed role.

authorisation was given. Copies of these contemporaneous notes must be copied to the CAB for their records. It should be clear from these notes what was expressly authorised by the authorising officer. An urgent oral authority lasts 72 hours from the time the surveillance was first authorised, unless renewed. A standard written authorisation for surveillance will cease to have effect after 3 months unless cancelled or renewed. Authorities must not "lapse" and must be cancelled as soon as they are no longer necessary or proportionate. Surveillance authorities must be regularly reviewed during the period they are valid.

Scotland

18. Where surveillance takes place in Scotland, authorisation would normally be granted under RIP(S)A. However, public authorities listed in section (46(3) of RIPA 2000 and the Regulation of Investigatory Powers (Authorisations Extending to Scotland) Order 2000; SI No. 2418, are able to obtain authorisation for surveillance under Part II of RIPA where the conduct authorised will be taking place in Scotland. The Home Office is one of those public authorities. This code of practice is extended to Scotland in relation to authorisations granted under Part II of RIPA which apply to Scotland. A separate code of practice published by the Scottish Government applies in relation to authorisations granted under RIP(S)A.

Safeguards and Handling Data

19. Information acquired or gathered under the authority of a covert surveillance authorisation is safeguarded data and must be handled in accordance with relevant policy. This will ensure that such information complies with relevant legal frameworks and surveillance Code of Practice. Compliance with these legal frameworks, including data protection requirements, will mean that private information obtained continues to be lawful, justified and strictly controlled. Dissemination, copying and retention of such data must be limited to the minimum necessary for the authorised purpose.

20. Material that is gathered as part of a directed surveillance authority is categorised as either *Evidential* or *Non-Evidential.*

- *Evidential* material is that which is used to directly aid in an investigation, enforce local/national restrictions or may be of interest to wider law enforcement.
- *Non-Evidential* material is that which is gathered during the course of an investigation but is of no operational use.

21. All material gathered, both evidential and non-evidential, including any authorities and accompanying paperwork, must be handled and stored securely in one location.

Access to this material and storage location must be restricted to reduce the risk of data loss and/or unauthorised access.[3]

22. Duplicates must not be made of any evidence or information gathered through covert surveillance, save that which is requested by another law enforcement agency and only where approval is given by the Authorising Officer. All stored information must be classified as Official-Sensitive under the government security classifications. Stored information containing sensitive information must contain the following handling instructions:

> OFFICIAL SENSITIVE - Contains personal sensitive information, subject to confidentiality requirements under the Data Protection Act. Do not circulate this information further without prior approval from [insert details of local Information Security Manager].

23. Any sharing of material must be justified and be fully auditable. The number of people material is disclosed to and the extent of any disclosure, both internally and externally, should be limited to the minimum necessary for the authorised purpose.

24. Following the conclusion of the directed surveillance authority, *Evidential* material will be stored in line with evidential CCTV footage (see DSO 04/2017 Surveillance Camera Systems) and must be destroyed after 6 years.

25. The Detention Services Security Team (DSST) will review all *Evidential* material annually to ensure the data remains valid for the authorised purpose. If not, it will be re-categorised as *Non-Evidential.*

26. Following the conclusion of the directed surveillance authority, *Non-Evidential* material will be stored in line with non-evidential CCTV footage (see DSO 04/2017) and must be stored for a period of 120 days before being destroyed.

27. To demonstrate compliance with UK GDPR[3], ad hoc monitoring logs must be present in areas where CCTV can be independently controlled. Logs should be completed to evidence activity if an operator must take control of the system.

28. To ensure residents who provide intelligence are afforded the necessary safeguards, any resident noted as a source of intelligence must be recorded and shared with DS Security monthly.

[3] Article 30, UK GDPR – Maintaining Records of Processing Activity (ROPA).

Revision History

Review date	Reviewed by	Review outcome	Next review
April 2019	J Andrews	Reformat	April 2021
February 2020	S Ali	RIP(S)A guidance updated	February 2020
July 2023	T Amisu	General Update Requirements for the review of Evidential Material have been updated.	July 2025