



Investigatory Powers
Commissioner's Office

PO Box 29105, London
SW1V 1ZU

By Email

April 2020

Dear Sir/Madam,

Assurance of data handling and retention safeguards

In light of the recent and serious compliance failings by part of the UK intelligence community, I have asked the IPCO inspectorate to carry out a full review of the ways in which data is handled by the public authorities we oversee. This work, which was initiated in late 2019, has comprised initial discussions with a range of authorities in relation to their data holdings. This includes any data obtained under the Investigatory Powers Act (IPA) 2016 and the Regulation of Investigatory Powers Act (RIPA) 2000 and which is therefore the subject of oversight by my office. This programme is intended to promote compliance with these acts and the Codes of Practice, and with other legal obligations including the Data Protection Act (DPA) 2018. You will be aware that the current restrictions have meant that our working model has changed and that any contact with our inspectors will be conducted remotely for the foreseeable future. Nonetheless, my inspectors will contact you to discuss data assurance alongside our usual inspections.

The objectives of the Data Assurance programme are:

- To inspect and investigate compliance with data safeguards to establish a high level of confidence that all data obtained under the powers overseen by IPCO is retained lawfully.
- To embed and encourage best practice for compliance at each authority we oversee.
- To assist the authorities we oversee to understand and investigate the compliance challenges arising from the use of bespoke, off-the-shelf and shared data handling programmes and technical storage environments.

My inspectors have identified that many organisations are retaining data for longer than is necessary or appropriate for a number of reasons. Firstly, in many cases authorities have not fully implemented data retention and disposal policies, secondly, many authorities operate with a culture of comprehensive retention to prevent operational data loss, and finally, systems used to transfer and securely store data may not promote or enable appropriate disposal processes.

For example, consider that an authority seeks and is granted a directed surveillance authorisation. Under that authorisation, surveillance is conducted for a period of time and provides information to meet the objectives of the investigation. As part of the investigation, one officer emails the results of the surveillance to a colleague and their manager, both of whom save a copy on their desktop and in Outlook for future reference. The officer also emails the product to a legal colleague so that the product may be used as evidence during criminal proceedings, it is therefore disclosed to a court and retained in a password-protected file for further use in the event of an appeal. At this point, no decision is taken as to how long that data should be retained, and the copies on both Outlook and the desktops are retained.

Although this example demonstrates legitimate use of the data for investigative and evidential use of the data, this approach is unlikely to be compliant with the code of practice for surveillance. The data pathway described includes retention on a personal desktop and in Outlook as well as a password-protected evidential copy. In this example, no retention, review or disposal process is in place for either pathway. In cases such as this, my inspectorate have found that data is being retained longer than is necessary, and at times indefinitely. I urge you to review your obligations under IPA and RIPA and to revisit the safeguards in the Codes of Practice¹ to ensure that appropriate policies and processes are in place within your authority.

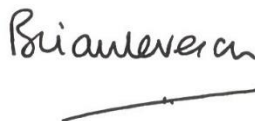
Starting in 2020, IPCO inspections will include data assurance and will require the following to be made available to my inspectors: safeguarding policies; retention and disposal schedules; access to any systems used to store data obtained under IPA and RIPA. Through each inspection, my office will ask you to demonstrate the adequacy of your policies, including physical security of data, adequacy of staff training, steps to minimise copying of data and processes to ensure all relevant data and copies are deleted at the appropriate time.

This work is a central part of IPCO's role to assist public authorities to use these powers lawfully, in the public interest. I anticipate that this programme will allow my office to establish a good level of confidence in the safeguarding practices of the authorities I oversee. I recommend that you take the following actions, which will assist you in demonstrating compliance and adherence to your obligations to safeguard any data you have obtained or may obtain:

- 1) Review the safeguarding obligations in the relevant Code of Practice for any powers used by your authority.
- 2) Ensure that internal safeguard policies for retaining, reviewing and disposing of any relevant data are accurate and up-to-date.
- 3) Ensure that the authorising officer for your authority has a full understanding of any data pathways² used for RIPA or IPA data.
- 4) Ensure that all data obtained under IPA and RIPA is clearly labelled and stored on a data pathway with a known retention policy.
- 5) Review the wording of safeguards in any applications to obtain data under IPA and RIPA and ensure that they accurately reflect the retention and disposal processes at your authority³.
- 6) Review whether data obtained under previous authorisations is being retained for longer than is necessary and, if appropriate, consider disposing of retained data.

If you have any questions about this programme or the recommendations we have made, please do not hesitate to contact IPCO at Info@IPCO.org.uk. Although we are not conducting inspections in person, my inspectors are available to answer any questions you have, and will be conducting inspections remotely, on a rolling basis, throughout the year.

Yours sincerely



The Rt. Hon. Sir Brian Leveson
The Investigatory Powers Commissioner

¹ Communications Data Code of Practice Chapter 13, CHIS Code of Practice Chapter 8 and Property Interference and Surveillance Code of Practice Chapter 9 set out safeguarding requirements.

² For example, directed surveillance data may be simultaneously stored on several data pathways: Pathway one – CCTV video product is transferred onto a CD and kept in a secure cabinet; Pathway two – a copy of the video is sent via email and stored on a common storage drive; Pathway three – a copy of the video is received via email and saved in an Outlook folder by a legal officer; Pathway four – a copy of the video is received via email and stored in a password protected evidential casework folder by a legal officer.

³ For example, if all data will be retained for a set number of years this should be stated in your application, or the application should refer to the internal safeguards policy document.