Department for Work & Pensions

Procedures ▸ RIPA - Information Returned

Procedures > Pages > Civil-Enforcement > RIPA-information-returned

# RIPA - Information Returned

This procedure is for the communications single point of contact (SPOC) and follows the receipt of information requested in a CSF977. The regulation of investigatory powers act (RIPA), allows criminal legal enforcement investigators (at EO or HEO grade) to request information relevant to criminal enforcement from communication service providers (CSPs). This procedure tells you how to check the information is complete and correct before forwarding it to the investigator who originally asked for it.

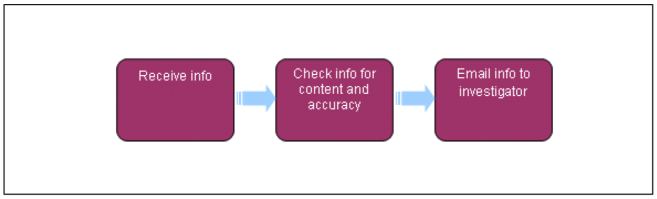
Once you are satisfied the information contains no errors, collate it and send it to the investigator, who use the information to update the relevant criminal investigations file.

If you identify errors, refer the application, notice and any related papers to the senior responsible officer (or their deputy), who returns an action plan within three days.

Where it is established that the errors have been caused by the CSP, contact them and provide full details.

Where information is acquired or disclosed wrongly, report this to the interception commissioner within five days of discovery.

For more information refer to the Policy, Law and Decision Making Guidance


Receive info
Check info for content and accuracy
Email info to investigator

## Receive information

1. When the communications data is received from the communications service provider (CSP), check:
   - If all the information requested has been received.
   - It fulfils the requirements of the CSF977 notice.
   - Whether any excess information been received.
   - Are there any errors?
2. Check if any errors have been identified in the information received. For example:
   - Has the Child Maintenance Group (CMG) received information it has no right to?
   - Has the CSP given excess information?
   - Has the CMG asked the CSP for information it was impossible for them to provide?
   - Is the information received for the wrong person?
   - Has the CSP highlighted an error in the request for information and advised the CMG it is not possible to provide the data?

   When you confirm there are no errors in the information, complete the following actions:
   - Access the Communications Data spreadsheet in the shared drive.
   - Update the column for the date the communications product was received, using the format day/month/year.
   - Access the CSF976 SPOC log for the application.
   - Update the CSF976 SPOC log with the latest information.
3. Where the communications data product has been received electronically, insert a hyperlink to the communications data product received from the CSP. Save the communications data product received, in the individual folder for the application, which will be stored under the unique reference number,
4.

   If the data has been received by fax or post, record in the spreadsheet the method it was sent to the CMG and the data received.

   For sensitive cases:
   - Print off the communications data product and the covering email if it was emailed to you

- Delete the email from the CSP
- Store the hard copy of the product and covering email in the file for the sensitive case in the secure locked cabinet

5.

Where the communications data product has been received by fax or post, store the communications data product in the secure locked cabinet.

For sensitive cases, store the communications data product in the sensitive case secure locked cabinet.

6. In either case, ensure that the CSF976 SPOC log has an up to date entry for this action and there is a hyperlink in the log to the stored information.

7. Collate all the information to be returned to the investigator and send all the communications data acquired to the investigator in an email marked RESTRICTED – PERSONAL – RIPA Communications Data Information.

For sensitive cases:

- If the investigator is in the same business area as the SPOC, personally hand the information over to the investigator.
- If the investigator is not in the same business area as the SPOC, call the investigator to advise that you are going to fax the communications data product for the case but a test fax will be sent through first, to which you must receive a response.
- Fax a sheet of paper with: **TEST – please respond to:** (your name and telephone number)
- Once you have received a telephone call confirming receipt of the test fax, fax the communications product with a covering sheet marked for the attention of the investigator. Request that the investigator confirms receipt of the fax immediately.
- If the investigator does not telephone within five minutes, contact them to confirm receipt.
- Store the copy in the secure locked cabinet, along with all fax papers.

## Investigator

8. Once the Communications data information has been received, you must:

- Assess the information received from the CSP and update the criminal investigations file with the relevant information.
- Store all communications data product received in the sub folder. This should include any section 15 applications made as a result of information obtained from the regulation of investigatory powers act (RIPA) product and documents or information returned as a result of such an application.
- Proceed with the investigation.

## Communications SPOC

9. When you have identified errors in the information, you must: access the communications data spreadsheet and select the **Error** tab.

10. Complete each field within this tab as follows:

- Input the Unique reference number of the CSFapplication/CSF9777 notice
- Choose the Error type **Reportable** or **Recordable** from the drop down list
- Input the Investigator's name in the **Applicant Name** box
- Choose a reason for error from the drop down list
- Input the date of error
- Input the time of error
- Confirm if the CSP has been notified
- Input the name of designated person
- Input the date sent to designated person
- Include any comments the designated person needs to be aware of in the **Comments to Designated Person From SPOC** box

⚠ If the data was sent to the CMG and has no relevance or connection to the investigation, include a statement here that the CSP and the senior responsible officer (the manager responsible for overseeing the entire RIPA process) have been notified. When the Interception Commissioner has been notified, update this box with the date the senior responsible officer gave authority for the documents to be destroyed. If the data received refers to the case under investigation but is in excess of that requested, include a statement here that authorised conduct by the CMG has resulted in excess data being received which will be retained.

- Only complete the Interception of Communications Commissioner's Office (IOCCO ) Notified box, if the error is recordable
- Only complete the Date IOCCO Notified box if the error is recordable

11.

On completion of the spreadsheet refer the application, notice and any relating papers to the senior responsible officer, or the deputy senior responsible officer in their absence, copying the relevant designated person into the email. The email should include the error details and if IOCCO has been notified.

If the case is sensitive:

- If the senior responsible officer and the designated person are in the same business area as you, personally hand the information over to the officers
- If the senior responsible officer and/or the designated person are not in the same business area as you, contact the senior responsible officer/designated person and advise them that you are faxing information relating to an error to them and that a test fax will be sent through first to which you must receive a response saying they have received it.
- Fax a sheet of paper with: TEST – please respond to: (your name and telephone number).
- Once you receive a telephone call confirming receipt of the test fax, fax the communications error information with a covering sheet marked for the attention of the senior responsible officer/designated person. Request that they confirm receipt of the fax immediately.
- If they do not telephone within five minutes, contact them to confirm receipt.
- Store the copy in the secure locked cabinet, along with all fax papers.

12. Await return of the action plan. This should be within three working days.
13. When the action plan has been returned update the **Error** tab of the communications data spreadsheet with any further information or instructions from the designated person/senior responsible officer and the date.
14. Where communications data is acquired incorrectly or disclosed wrongly a report must be made to the Interception Commissioner. This is a reportable error. It is your responsibility to write a report on the error using the information input to the communications data spreadsheet. The report must include:
    - unique reference number of the CSF977 notice
    - Details of the error
    - An explanation of how the error occurred
    - An indication of whether any unintentional collateral intrusion has taken place
    - If the error was made by the CSP, confirmation that the CSP has been informed and if not why not
    - An indication of what steps have been or will be taken to ensure a similar error does not recur
15. Email the report to the interception commissioner no more than five working days after discovering the error.
16. Where the CSP has provided data that has no relevance or connection to any investigation undertaken by the CMG, alert the senior responsible office that the communications data should be destroyed.
17. On written authorisation (by email) of the senior responsible officer, shred all data with no connection or relevance to any CMG investigation.
18. Update the **Communications Data** spreadsheet in the **Comments** box that this action has been taken.
19. Update CSF976 SPOC log for the case for which the data was received and include a hyperlink to the email from the senior responsible officer authorising the destruction of the data.
20. Confirm if the error was caused by the CMG or by the CSP. The error would be a CSP error if:
    - Disclosure of the wrong data - you need to check that all the CMG's documentation are in order and that the CMG has provided the correct information to the CSP
    - Excess information
    - Information for the wrong period
    - Information that involves collateral intrusion
    - Information the CMG is not entitled to see
    - information the CMG has not asked for
21. When it has been established that the CSP has made the error, contact the CSP in written or electronic form:
    - Access Outrigger and input the SPOC PIN number.
    - Obtain email address of the CSP. If an email is not available, obtain the address noted in Outrigger.
22. Contact the CSP providing them with a report including the following:
    - Unique reference number of the CSF977 notice
    - Details of the error including the action the CMG has taken
23. Complete the **Error** section on the **Communications Data** spreadsheet to confirm that the CSP has been informed of the error and the date.
24. Save the report and the email in the shared folder in the individual folder relating to the application.
25. Update the CSF976 SPOC log to show the action taken and the date the report was sent to the CSP. Include a link to the email and the report.

## RIPA information is not returned

26. If the RIPA information is not returned within 10 days of the RIPA notice being issued, you must:
    - Contact the CSP by telephone if a number is available to confirm the reason for the delay.

  - If a telephone number is not available, contact the CSP by email.
  - Remind the CSP of the request and the unique reference number of the notice.

27. BF the case for 25 days from date the notice was served. The 25 day period includes weekends and any bank holidays occurring during the period. The BF data needs to take into account these additional days to ensure there is sufficient time for the designated person to reassess the application and take next steps.
28. Update the **Comments** box on the **Communications Data** spreadsheet with the details of the contact including data, time and response from the provider.

CSF976 SPOC log

CSF977 Notice

RIPA - Apply For Information

RIPA  - SPOC Considers Referral

RIPA - SPOC Issues Notice

RIPA - Pay Invoices

RIPA - Weed Applications

Terminology Changes