IPCO
Investigatory Powers Commissioner's Office

PO Box 29105, London
SW1V 1ZU

ico.
Information Commissioner's Office

Wycliffe House, Water Lane,
Wilmslow, SK9 5AF

XX December 2019

Dear [NAME],

You will be aware that Telecommunications Operators (TOs) are under an obligation to report personal data breaches to the Information Commissioner (IC) under both the Privacy and Electronic Communications Regulations 2003 (PECR) and the General Data Protection Regulation (GDPR).

You will also be aware that where an error by a TO results in communications data being disclosed wrongly under Part 3 of the Investigatory Powers Act 2016 (IPA), a report must be made to the Investigatory Powers Commissioner (IPC) by that TO.

In some cases, a reportable error may also be a personal data breach. As a result, there have arisen cases in which TOs have been required to report the same matter to both the IC and IPC. This 'dual reporting' has been a cause for concern in the telecommunications community, and the Information Commissioner's Office (ICO) and the Investigatory Powers Commissioner's Office (IPCO) have agreed to the following approach for reporting to them, in order to reduce the dual-reporting burden on TOs.

Reporting of errors to IPCO and the ICO

The Communications Data Code of Practice (November 2018 edition, at paragraph 24.41) states:

"Telecommunications operators and postal operators are only required to report errors made in response to authorisations or notices for communications data under Part 3 to the IPC. The IPC must consider whether any errors either reported or uncovered during inspections have resulted in personal data breaches that should be reported to the Information Commissioner, or whether details of the errors should be forwarded on because they are relevant to the Information Commissioner's role under Part 4 of the IPA."

Thus, any mistake/error on the part of the TO, that amounts to a reportable error under the IPA, must be reported to IPCO.

TOs will already be aware that a personal data breach within the meaning of the PECR, if it is being reported to IPCO as an error, does not also need to be reported to the ICO[1].

However, there remains an overlap between GDPR breaches and IPA errors. This is subject to the qualified breach reporting requirement under the GDPR (compared to the absolute requirement in the PECR).

The reporting obligation that arises is as follows:

1. If a personal data breach occurs that is an error reportable to IPCO,
    a. the TO must report the error to IPCO within 5 days,
    b. the TO must also assess whether the breach is reportable under GDPR Article 33; if it is, it must also be reported to the ICO within 72 hours of detecting the breach.
2. If a breach occurs that is not an error reportable to IPCO, it must be reported to the ICO in 24 hours.

A flow diagram is also appended to this letter, as Appendix B.

At step 1b, the TO must assess whether the breach is 'unlikely to result in a risk to the rights and freedoms of natural persons'. Based on previous examples of errors and breaches reported to IPCO and the ICO, we have established some parameters for how such risks might be assessed; these are also appended to this letter, as Appendix C.

We stress that it is the TO's responsibility to assess each breach to determine whether it is unlikely to result in a risk. In each case, the TO must record their decision about risk, and their reasons, in accordance with the accountability principle of the GDPR. These logs will be reviewed during the ICO's retained data security audits.

Data sharing

In addition to the above model, TOs should be aware that, pursuant to paragraph 24.41 and 24.42 of the Code of Practice, IPCO and the ICO have agreed to share details of relevant errors and breaches. This will ensure that the Commissioners are sighted on all matters relevant to their respective areas despite the reduced overlap in reporting.

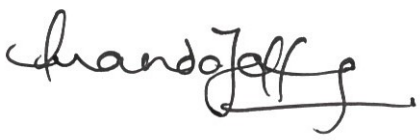
Conclusion

The requirements of the law concerning breach and error reporting are hopefully clearer than in the past. The model explained above will reduce the regulatory burden on TOs, with dual-reporting now required in only the most serious breaches. This should lead to far fewer dual reports, whilst bilateral sharing of reports by the Commissioners will maintain the same level of assurance to the public concerning oversight.

[1] See regulation 5A(9) of the PECR.

The Commissioners will continue to work together to ensure that TOs are supported to comply with the requirements of the law in their respective areas.

Yours sincerely,



Amanda Jeffery
Chief Executive, Investigatory Powers Commissioner's Office

James Dipple-Johnstone
Chief Regulatory Officer, The Information Commissioner's Office

Appendix A - the legislation

Article 33(1) of the GDPR states:

“In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.”

Regulation 5A(2) of the PECR states:

“If a personal data breach occurs, the service provider shall, without undue delay, notify that breach to the Information Commissioner.”

Article 2(2) of the European Commission Regulation 611/2013 states:

“The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible.”

Regulation 5A(9) of the PECR states:

“This regulation does not apply in relation to any personal data breach which is to be notified to the Investigatory Powers Commissioner in accordance with a code of practice made under the Investigatory Powers Act 2016.”

Paragraph 24.21 of the code of practice accompanying Part 3 of the IPA states:

“Where an error results in communications data being acquired or disclosed wrongly, a report must be made to the IPC (‘a reportable error’) by whoever is responsible for it…”

Appendix C – examples of what may, and may not, constitute a breach reportable to the ICO under Article 33 of the GDPR or Regulation 5A of PECR

Reportable as error to IPCO only

- **TO disclosure to wrong public authority (PA)** – IPCO only (low risk, secure transmission, easily detectable and no likelihood of executive action).

- **Excessive or inaccurate disclosure (correct individual identified, but too much or inaccurate data about that individual disclosed)** – IPCO only (low risk, secure transmission, data is for correct individual, issue is deeper privacy intrusion than authorised or else hampered investigation).

Reportable as error to IPCO and also to ICO under Article 33 GDPR

- **Incorrect disclosure (wrong individual) to requested PA** – IPCO and ICO (GDPR) (high risk, potential for executive action on wrong person).

Reportable as error to the ICO only under Regulation 5A PECR

- **Security breach not relating to authorised requests for communications data by PA (such as unauthorised access to or altering comms data)** – ICO only (no risk calculation necessary as the PECR is still in force)

The above are guidelines only; it is the TO's responsibility to assess each breach to determine whether it is unlikely to result in a risk. In each case, the TO must record their decision about risk, and their reasons, in accordance with the accountability principle of the GDPR. These logs will be reviewed during the ICO's retained data security audits.