Telecommunications Operator Audits – s.244 Investigatory Powers Act 2016

ICO End of Year Report 2022-23 Executive Summary

Information Commissioner's Office

Introduction

The Investigatory Powers Act 2016 (the IPA) provides, amongst other things, a legal framework compelling a telecommunications operator (TO) in receipt of a Data Retention Notice (DRN) to retain relevant communications data. The data held by virtue of a notice is referred to as "retained communications data".

Section 244 of the IPA places an obligation on the ICO to "…audit compliance with requirements or restrictions imposed by virtue of Part 4 in relation to the integrity, security or destruction of data retained by virtue of that Part".

The primary objective of the ICO's audits is to ensure that the TO has taken appropriate technical and organisational measures to safeguard the integrity, security and destruction of the retained communications data. In doing so the ICO fulfils its role as an independent regulator by ensuring that individuals' data is suitably protected and providing oversight to give assurance to the public that their information is being kept securely and handled appropriately.

The ICO sees auditing as a constructive process with real benefits for TOs, in which they can demonstrate their commitment to, and recognition of, the importance of information security in relation to retained data. The ICO audits also offer an independent assurance of information security policies and practices, can aid in the identification of risks and provide practical, pragmatic, organisation-specific recommendations to address them. On this basis the ICO aims to establish, wherever possible, a participative approach.

During our most recent cycle of audits (across 2022 and 2023), the ICO conducted IPA s.244 audits with all UK TOs that were subject to a DRN.

This full audit cycle began a year later than might be expected from our previous audit cycle (2019-20); this is because we carried out a focused piece of audit work in 2021 with all UK TOs subject to a DRN regarding their breach and error reporting concerning PECR Regulation 5A in this area. Accordingly, we did not consider incident management or breach reporting in this cycle.

Our Approach

The ICO has developed a control framework, based on the requirements of the Communications Data Code of Practice and a series of recognised industry best practice standards and accreditations, such as ISO 27001/2 and 11. The ICO considers that compliance with the requirements of this framework would be indicative of compliance with the associated legislation.

ICO IPA s.244 audits assess TOs against this control framework to determine whether appropriate technical and organisational measures are in place to allow the TO to appropriately manage the risks posed to the security of Data Retention and Disclosure systems, and whether they have taken measures to prevent and minimise the impact of security incidents to individuals. The audits usually consist of a desk-based evidence review followed by on-site interviews and testing.

Following the audit a report is prepared, which is shared with the TO and the Home Office, in which the ICO will make recommendations on how to mitigate the risks of non-compliance, reducing the chance of damage and distress to individuals and regulatory action being taken against the TO for a breach of the security obligations in Part 4 of the IPA, resulting in a breach of the legislation that the ICO regulates.

Outcomes of ICO IPA s.244 Audits

The ICO audited each TO in receipt of a DRN and provided an audit report. The 2022-23 audit cycle confirmed again (as in our previous 2019-20 report) that information security in the TOs' retained data operations is in most cases mature, well-resourced and effective, although there was significant variance between organisations in terms of how this was achieved.

The ICO is content that, where it identified weaknesses in controls, for the most part TOs responded positively to recommendations made to address those areas of weakness. Where they have not, we have used the tools at our disposal to ensure retained data is effectively protected. If significant issues were identified, we have worked constructively with the Home Office and IPCO to improve the situation.

The ICO will continue to use its IPA s.244 audits to ensure the security, integrity and timely destruction of retained data, and is committed to working with the TOs, IPCO and the Home Office to address any issues that arise.