Communications Service Provider Audits - The Data Retention Regulations 2014

End of Year Report 2016/17
Executive summary

Information Commissioner's Office

Introduction

On 17 July 2014, the Data Retention and Investigatory Powers Act 2014 (DRIPA) came into force. DRIPA was introduced to, among other things, provide a legal framework compelling a public telecommunications operator (as defined by section 2 (1) of DRIPA and section 2 (1) of the Regulation of Investigatory Powers Act 2000) in receipt of a Data Retention Notice (DRN) to retain relevant communications data (as defined by the Schedule to the Data Retention (EC Directive) Regulations 2009).

Using powers conferred within section 1 of DRIPA, the Secretary of State issued the Data Retention Regulations 2014 (DRR). Regulation 9 of the DRR places a duty upon the Information Commissioner to audit the integrity, security or destruction of data retained by a public telecommunications operator (hereafter referred to as a 'communications service provider' or CSP) by virtue of section 1 of DRIPA.

The primary objective of the ICO's audits is to ensure that the CSP 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 provide assurance to the public that their information is being kept securely and handled appropriately. These objectives align with the ICO's strategic goals, set out in our Information Rights Strategic Plan 2017-2021, to "increase the public's trust and confidence in how data is used and made available" and to "improve standards of information rights practice through clear, inspiring and targeted engagement and influence".

The ICO sees auditing as a constructive process with real benefits for CSPs, including demonstrating their commitment to, and recognition of, the importance of information security in relation to retained data; independent assurance of information security policies and practices; and the identification of risks along with practical, pragmatic, organisation-specific recommendations to address them, and so aims to establish, wherever possible, a participative approach.

During 2015/2016 and 2016/17 the ICO conducted DRR audits with all UK CSPs that were subject to a DRN as of April 2017. In addition to the formal DRR audits the ICO also witnessed the decommissioning of data retention and disclosure equipment.

DRIPA was superseded by the Investigatory Powers Act 2016 (IPA); the ICO continues to be responsible for undertaking audits under this new legislation.

Our Approach

The ICO has developed a control framework, based on the requirements of the Retention of Communications Data Code of Practice and a series of recognised industry best practice standards and accreditations, such as ISO 27001/2 & 11, as well as the European Network and Information Security Agency (ENISA) Guidance on the minimum security measures recommended in order to comply with Article 13a of EU Directive 2009/140/EC. Where appropriate, elements of the Home Office Compliance Questionnaire for Data Retention & Disclosure (DR&D) systems have also been incorporated into the control framework. The ICO considers that compliance with the requirements of this framework would be indicative of compliance with the associated legislation.

ICO DRR audits assess CSPs against this control framework to determine whether suitable technical and organisational measures are in place to allow the CSP to manage the risks posed to the security of DR&D systems, and whether they have taken measures to prevent and minimise the impact of security incidents to individual subscribers. The audits consist of a desk-based evidence review followed by on-site inspections, interviews and testing.

Following the audit a report is prepared, which is shared with the CSP and the Home Office, in which the ICO will make recommendations on how to mitigate any risks of non-compliance, reducing the chance of damage and distress to individuals and further regulatory action being necessary against the CSP for a breach of the DRR resulting in a breach of the other legislation that the ICO regulates.

Outcomes of ICO DRR Audits

The initial cycle of audits under the DRR were crucial to the ICO gaining an in-depth understanding of the data retention activities and controls within CSPs. Although DRIPA has now been replaced by the IPA, the ICO will use the experience gained from conducting these audits, along with its subsequent analysis, to inform its work under the IPA, which will be substantively similar.

Conclusions

Security across audited CSPs appeared generally mature and broadly effective, although there was significant variance between organisations in terms of how this was achieved.

The ICO is content that, where we identified weaknesses in controls, for the most part CSPs responded positively to recommendations made to address those areas of weakness. Where our recommendations have not yet been implemented adequately, the ICO will follow this up with our formal enforcement powers.

However, the ICO remains concerned about the strength and clarity of our oversight powers, and the extent to which that lack of clarity hinders our ability to meet our strategic goals to "increase the public trust and confidence in how data is used and made available" and "enforce the laws we help shape and oversee".

The ICO is also mindful of the tension between Home Office responsibility for costs, and the CSPs' responsibility for their data, and the difficulty this sometimes appears to create in determining who takes the lead when security remediations are required. We have raised this issue with the Home Secretary so action can be taken to resolve this uncertainty.

The ICO will continue to communicate these concerns and is committed to working with the Home Office to address them as the IPA progresses towards full implementation.