Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's Office (ICO) response to Consultation on updating Ofcom's guidance on security requirements in sections 105A to D of the Communications Act 2003

The ICO

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 ("DPA"), the Freedom of Information Act 2000 ("FOIA"), the Environmental Information Regulations ("EIR") and the Privacy and Electronic Communications Regulations 2003 ("PECR"). She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

Imminent legislative developments

The Commissioner should note that data protection laws are undergoing significant reform at the present time, with a Data Protection Bill announced in the Queen's Speech which will replace existing data protection legislation.

The General Data Protection Regulation (GDPR) will take effect in the UK from 25 May 2018. The Government has confirmed that the UK's decision to leave the EU will not affect the implementation of the GDPR next year.

In January 2017 the European Commission published a draft proposal for a new ePrivacy Regulation (ePR) as part of the EU data protection reform package to sit alongside the GDPR and would repeal and replace the current ePrivacy Directive implemented in the UK by PECR. Work is ongoing with a view to adopting an agreed text to come into effect in May 2018, at the same time as the GDPR.

Regulatory overlap

The Information Commissioner welcomes the opportunity to respond to

the Ofcom consultation on updating guidance on security requirements in sections 105A to D of the Communications Act 2003. She recognises the essential importance of telecoms services in underpinning a modern economy and society, and is supportive of measures to help companies to protect the security and reliability of their services. The Commissioner's response is restricted to those areas that fall within her regulatory remit.

To this end, the Commissioner is keen to ensure that her powers, and those of other regulators such as Ofcom, are exercised in a coordinated and consistent manner. She believes that ensuring different regulators' enforcement action does not unnecessarily overlap or duplicate effort is key to ensuring effective, proportionate and cost-effective regulation. This approach also synchronises with the Government's better regulation agenda.

Cyber Security

The Commissioner recognises that security of communications and reporting of incidents are an area of potential regulatory overlap, as is also noted in section 3.2 of Ofcom's existing guidance on security requirements[1].

Whilst a significant component of the wider security picture, the loss of service aspects of security and reporting are not the principal focus of the ICO's regulatory interest, which pertains to personal data breaches. However, as noted in the consultation, the profile and frequency of cyber security incidents has grown since the guidance was last published. Technical capabilities have evolved, and the boundaries have blurred between threats to the security of networks and to the data which they carry.

The Commissioner welcomes Ofcom's focus on cyber security as a key threat needing to be addressed as part of s105A compliance, and agrees that this is a continuing trend. She welcomes the proposal to modify the guidance to stress that appropriate management of cyber security risks is essential to compliance with s105A and merits inclusion alongside considerations such as compliance with data protection obligations. This complementary relationship will only become deeper with the introduction of the GDPR and ePR.

The Commissioner agrees with Ofcom that the effectiveness of the security measures should be best judged by testing. She welcomes both the current project to develop a telecoms sector cyber vulnerability testing framework, and the proposal for providers to participate in this scheme once complete.

Resilience

[1] https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf

The Commissioner welcomes Ofcom's proposal to update the guidance to reflect the growing risk to availability from flooding and power resilience, and to reflect Ofcom's expectation that providers manage these risks appropriately.

The loss of service through such incidents can lead to loss of data, and resilience has acquired even greater importance since the guidance was last updated thanks to the enormous growth of cloud services. The Commissioner's PECR audits consider business continuity and disaster recovery preparedness amongst other security elements, and will continue to do so.

Third Parties
Like Ofcom, the Commissioner has noted the reliance of some providers on third parties for infrastructure, support and even operation of their networks. She agrees that such arrangements can raise concerns about availability, oversight and governance.

Reporting
The Commissioner notes that Ofcom are concerned about differences in reporting between operators, and propose to adopt new mobile reporting thresholds and amend guidance on the incident follow-up process.

The Commissioner sees as a positive step Ofcom's proposal to update its guidance to ensure all providers are aware that cyber incidents are reportable, and agrees that cyber incidents will often have a significance in breaches of data confidentiality or integrity that outweighs the level of service outage they inflict.

The proposal to add a qualitative criterion to the list of reportable incidents so that incidents involving cyber security breaches are included is particularly welcome.

The Commissioner shares the disquiet that Ofcom notes about enquiries or media reports being the first information a regulator receives about serious incidents. Like Ofcom, the ICO does not wish to further complicate incident management processes, but notes time can be a factor in the impact of such incidents on individuals.

This is reflected in the current obligation imposed by PECR where service providers have to notify the Information Commissioner's Office about a personal data breach within 24 hours of detection. Until modified by new legislation, this will remain a legal requirement for a provider with an incident that involves a breach of personal data. The Commissioner has imposed monetary penalties on several occasions in recent years due to failures to comply with this requirement.

The Commissioner nevertheless welcomes Ofcom's proposal of a deadline of 72 hours for 'non-major' incidents to align with the notification requirements in GDPR (replacing the current "within a few days" wording) and appreciates that the most urgent incidents would be notified within hours. However, the requirement for CPs to report PECR breaches within a 24 hour time frame will remain in place until the ePR comes into force.

The Commissioner should also note that there is an existing requirement on providers under PECR to inform subscribers of a significant risk to the security of the service. The GDPR also reflects this expectation, and if the ePR features breach reporting requirements, it will presumably similarly align.

Audit

The Commissioner welcomes Ofcom's proposal to amend the current guidance to reflect a possibly increased exercise of its power to conduct audits.

Although providers do not pay for ICO audits under PECR, the Commissioner recognises the burden on providers of supporting an audit, and the importance of targeting audits to risk areas.

As with breach reporting, there is a strong possibility of regulatory overlap between the Commissioner's and Ofcom's existing audit and enforcement activities, and those which will be introduced with GDPR and ePR in 2018.

Until then the ICO will continue to pursue its current program of PECR security audits, which share some common ground with those outlined in the consultation.

The Information Commissioner welcomes the opportunity to respond to Ofcom's consultation and looks forward to closer working between regulators to meet the evolving risks of cyber attacks on infrastructure and individuals.

September 2017