The Information Commissioner's comments on the European Commission publication of the Commission Implementing Regulation pursuant to Art 16(8) of the NIS Directive (EU 2016/1148)

Introduction

1. The Information Commissioner (the 'Commissioner') has responsibility in the United Kingdom for promoting and enforcing the Data Protection Act 1998[1] (DPA) and the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004[2] (EIR) and the Privacy and Electronic Communications Regulations 2003[3], as amended (PECR). The Information Commissioner also has a more limited supervisory role under the Data Retention Regulations 2014 (DRR 2014) created under the Data Retention and Investigatory Powers Act 2014 (DRIPA). These powers and duties in relation to retained communications data have been carried forward under the Investigatory Powers Act 2016 (the IPA).

2. The Information Commissioner will be the competent authority for regulation of the General Data Protection Regulation (GDPR) (EU 2016/679) and the Law Enforcement Directive (EU 2016/680) when transposed into UK domestic law.

3. The Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals and taking appropriate action where the law is broken. Her duties include providing advice on policy and other initiatives that engage information rights concerns.

4. It has been proposed that the Information Commissioner will be the competent authority in the United Kingdom for regulation of Digital Service Providers (DSPs) under the NIS Directive (the Directive) and she therefore comments on the draft implementing regulations in light of this possible regulatory duty.

[1] Implementing Directive 95/46/EC
[2] Implementing Directive 2003/4/EC
[3] Implementing Directive 2002/58/EC

Digital Service Providers are:

- Cloud Services;
- Online Market Places; and
- Search Engines.

Summary

5. The Commissioner recognises the imperative of ensuring the security of network and information systems and the essential and business services they support, and considers that her office possesses expertise and experience which may be valuable in regulating the security of certain data processing systems and in particular the activities of DSPs. That experience, when regulating PECR, DRIPA and, more recently, the IPA, leads her to conclude that setting overly rigid parameters for the determination of an impact which is substantial (in accordance with Article 16(4) of the Directive), may be undesirable and may lead to a failure to report incidents which nevertheless have a substantial impact on the users of the service and which should, by the nature of that impact, be considered for regulatory action.

Digital Service Providers and 'significant impact'

6. The Commissioner recognises that many businesses, in the UK and across the EU, rely on cloud services, and many small and medium enterprises operate at least partly by virtue of their presence in online marketplaces. Any disruption to these services could have a significant operational and financial impact on these businesses, and by extension, the national economy. Similarly, search engines have established themselves as an essential tool for organisations at all levels. The Directive itself makes no specific provision for identification of DSPs but the Commissioner notes the approach in Article 16(11) of the Directive, that the provisions shall not apply to micro- and small enterprises. The definitions of the services, and the identification thresholds, should reflect the likely number of users of the services, and thus the potential disruption any significant impact on provision of those services would entail.

7. As to the extent of services disrupted, and the numeric values suggested in Article 4, the Commissioner considers that it may be helpful to recognise that some services (eg email, document access, eCommerce) will be more business-critical than others (eg, presentations, image processing) – and that these will vary depending on the nature of the business. Developing a concept of services which could be critical for users might be appropriate. To

the extent that these are business-critical processes, these could include (but not be limited to):

- Email and internet access;
- Telephony;
- eCommerce;
- Access to records (eg documents, spreadsheets, images);
- Backup and disaster-recovery services.

8. The Commissioner wishes to caution against the use of strict numeric thresholds at Article 4 to determine whether an incident should be notified to the competent authority. This implies a set of criteria which are more sharply defined and delineated than is perhaps desirable. It would be more helpful to focus on the magnitude of the effect for the users of the service, using the parameters specified in the Directive as a guide, with any figures suggested being merely indicative and not prescriptive.

9. Similarly, the Commissioner considers that the key parameter might not always be the number of affected users, or the length of time a service was unavailable. It might be helpful to consider whether an interruption to a more critical service should be notifiable at a lower level of interruption, and that less business-critical services could be tolerated to a higher level of interruption, or to a greater number of users. It should be recognised that DSPs may offer a variety of services, and that these may be affected to varying degrees, or not at all, during an incident.

10. A DSP offering a particularly wide and varied suite of services might seek to argue that, given only a small number of its services were affected, any numeric threshold for notification was not met, even though the services affected were those which were the most critical for many users.

11. The Commissioner would also like to propose that what comprises a substantial impact on provision, expressed in terms of the availability of that service, may not solely relate to the *unavailability* of a service as anticipated in Article 4; a service which is *disrupted* to the extent that it runs so slowly it is, to all effects and purposes, unusable, ought also to be considered unavailable in the terms expressed in Articles 3 and 4 of the draft implementing regulations.

12. Notwithstanding the Commissioner's views on the use of numeric parameters in paragraph 8 above, if numeric values for thresholds are to be considered, the Commissioner recommends that these values should be indicative values only, not formal

thresholds, and should be set by relation to the number of affected users. So, by way of a worked example: any incident affecting more than 10% of users of any of the business critical services listed. That way, if an incident suffered by a DSP causes 5% of users to have no email, 4% of users who can't access documents, and 2% of users report eCommerce sites running so sluggishly customers are failing to transact, that would exceed a threshold, where none of these individually may have done so.

13. The Commissioner is also conscious that a series of shorter incidents, in relatively quick succession, might be just as disruptive as, and possibly more disruptive than one longer incident. She considers that any series of incidents within a notional period which cumulatively amount to a substantial impact on the provision of the service, should also be notifiable even if none of the individual incidents would meet the threshold for notifying the competent authority.

14. Finally the Commissioner considers that the parameter at Article 4(1)(e) is unnecessary. Many digital services are multinational in their nature, so that an incident affecting such a service (at the DSP end of the operation) will in all likelihood affect the service in all Member States in which it is offered. This will have the unintended effect of meaning that a relatively minor incident, which nevertheless affects users in more than one Member State, would be deemed to be substantial in the terms expressed at Article 4(1)(e), (and hence subject to regulatory action) even if none of the other factors were relevant. Conversely, a substantial incident which affects users in only one Member State should still be considered eligible for regulatory action, even if its effects are quite localised. Thus, the parameter at Article 4(1)(e) is not required in order to determine whether to include or exclude an incident from regulatory action, and should be discarded.

Information Commissioner

10 October 2017