The Information Commissioner's response to the Department for Digital, Culture, Media & Sport consultation on the Security of Network and Information Systems.

Introduction

1. The Information Commissioner (the 'Commissioner') has responsibility in the United Kingdom for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations (EIR) and the Privacy and Electronic Communications Regulations 2003, 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). The Data Protection Bill (DP Bill) that was recently introduced into Parliament envisages the Commissioner undertaking a similar regulatory supervisory role in respect of processing of personal data covered by the EU General Data Protection Regulation (GDPR), for activities not covered by EU law, law enforcement processing and the processing by the intelligence services.

2. 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. The Commissioner is responsible for regulating the aforementioned legislation. She also has powers of audit in respect of communications data retention systems under the Investigatory Powers Act 2016.

Summary

3. The Commissioner recognises the imperative of ensuring the security of network and information systems and the essential 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 digital service providers. Although the Commissioner has yet to be asked formally to take on the role of competent authority for digital service providers this would be consistent with existing regulatory functions and expertise. This additional role could not be undertaken within existing resources and sufficient funding would need to be made available to her office in order to undertake this work.

Relevant essential services and Digital Service Providers

4. Annex 2 of the Consultation proposes that the Information Commissioner's Office (ICO) serves as the competent authority for Digital Service Providers (DSPs), specified as 'cloud services; online marketplaces; search engines'. Definitions of these three terms are provided in Section 8 and are taken from Article 4 of the Directive. The Commissioner broadly agrees with these definitions.

5. The Commissioner agrees with DCMS' position that any proposed thresholds for identification of Operators of Essential Services (OES) should generally be set at *'such a level as to capture only the most important operators in each sector based on the potential of a disruption to their essential service resulting in what the government considers would be a significant disruptive effect'*.

6. 'Significant disruptive effect' is not defined, nor the applicable term for DSPs: 'significant impact on the provision of a service' but the Commissioner recognises that many UK businesses 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 financial impact on these businesses, and by extension, the UK economy. Similarly, search engines have established themselves as an essential tool for organisations at all levels. The NIS Directive itself makes no specific provision for identification of DSPs and the Commissioner suggests that if the DCMS is minded to set parameters for the identification of DSPs then it should adopt a similar approach, subject to Article 16(11) of the NIS Directive. The definitions of these 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.

Competent authority

7. The Commissioner accepts the Government view that the better model for regulation in the UK will be option 2: nominating multiple sector-based competent authorities. In principle, she has no objection to her office being nominated as the competent authority

for DSPs, subject to adequate funding being made available for the tasks to be undertaken. Comments made in this context are therefore made without prejudice to the Commissioner's acceptance of the role as the competent authority for DSPs.

8. The Commissioner further agrees with the nomination of the NCSC as the UK's Single Point of Contact, and CSIRT. She wishes, however, to make parties alive to the possibility that reportable incidents relating to both OESs and DSPs might also indicate a possible data breach, in terms defined under data protection legislation. It will therefore be important that parameters be agreed between NCSC and ICO so that data breaches are recognised as such and duly reported to the ICO, irrespective of any regulatory responsibilities under the NIS Directive. It should also be noted that any requirement to notify NCSC about a breach under the NIS Directive will not satisfy the requirement to inform the ICO of data breaches under the GDPR, so OESs and DSPs will still need to report data breaches separately to the ICO, by reference to the parameters for reporting set out in GDPR or domestic data protection legislation.

Incident reporting

9. The Commissioner agrees with the proposal that incident reporting timelines for both OESs and DSPs should be aligned with the requirements of the GDPR. However, the Commissioner believes that such an alignment would be more readily achieved by a direct transposition of the equivalent provision within Article 33(1) of the GDPR, as follows:

    - Consultation text: '*without undue delay and as soon as possible, at a maximum no later than 72 hours after having become aware of an incident*'

    - GDPR text: '*without undue delay and, where feasible, no later than 72 hours after having become aware […]*'

10. The Commissioner is aware of the current European Commission consultation on proposed implementing regulations, setting out the parameters to be taken into account by DSPs for determining whether incidents have a substantial impact. These regulations adopt a broadly numeric set of criteria for determining the scale of impact of incidents. The Commissioner would caution against the use of specific numeric values. 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.

11. The Commissioner is also conscious that a series of shorter incidents, in relatively quick succession, might be just as disruptive, and possibly more disruptive than one longer incident. Additionally, 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.

12. She would further suggest that a substantial impact on provision may not solely relate to the *unavailability* of a service; 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 referred to above.

13. As to the percentage of services disrupted, and definitions of 'core services' which may be adopted, it is probably fair 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. 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 threshold for notification was not met (ie in percentage terms) even though the services affected were those which were most business-critical for most users.

14. Perhaps rather than 'core' services, an idea 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.

15. Notwithstanding the Commissioner's views on the use of numeric parameters in paragraph 10 above, if numeric values for thresholds are to be considered, the Commissioner recommends that these values are set by relation to the number of 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 would have done so.

Key challenges

16. The Commissioner notes that GDPR will apply to the DSPs her office may also be called upon to regulate under the NIS Directive, and that her regulatory role under GDPR is different. Clarity on the parameters for reporting incidents under NIS Directive will be important especially where the parameters for reporting data breaches under GDPR may be different. It will be important to avoid confusion by DSPs as to whether the threshold for reporting an incident under the NIS Directive implies that an associated data breach need not be reported to the ICO under GDPR. The requirements of each piece of legislation should be complied with on its own terms.

17. It will be necessary to establish appropriate gateways for data sharing between competent authorities, as well as between NCSC and competent authorities, especially where there is likely to be overlap between competent authorities in terms of their areas of competence. Where, for example, an incident is reported by NCSC to one of the other competent authorities under the NIS Directive, if there is a data protection dimension to the incident, the Commissioner would expect to be informed of this so that she can carry out her regulatory role in respect of that matter, under GDPR or domestic data protection legislation.

Powers

18. Clarity will be required on the extent and provision of any specific powers the ICO will be given under the NIS Directive, particularly in relation to powers of investigation and enforcement, for example powers to demand information about a breach, powers of access and entry to premises, seizure of documents and equipment, etc. The Commissioner also notes that her office's powers under the NIS Directive are restricted to regulation after an incident (eg she has no powers of audit). Clarity will therefore be necessary where her office has certain powers under GDPR, but not under the NIS Directive, so that the limits and extent of her office's powers are clearly defined and understood.

19. Ensuring that DSPs are clear about their obligations through guidance and support will be important. If the Commissioner's remit is intended to extend to that activity, this should be clear and funded accordingly.

Penalty regime

20. The Commissioner concurs with the intent of the government to align the NIS penalty regime, including processes and procedures, with that of the GDPR. She notes that the consultation presently proposes having two 'bands', one of 2% of turnover or €10m for 'lesser offences' (including failure to co-operate with the competent authority and failure to report an incident) and 4% of turnover or €20m for 'failure to implement appropriate and proportionate security measures'.

21. The Commissioner believes that further clarity is required on this alignment. This is because under the GDPR, failure to comply with the obligations of Article 32 – in other words, to implement appropriate technical and organisational measures to protect personal data being processed – is subject to a fine of 2% of turnover or €10 million, not the higher level of 4%. However, where the incident is not a personal data breach, and is therefore dealt with under the NIS Directive by the respective competent authority, it may result in a penalty of 4% or €20 million. This does not achieve the stated goal of alignment with the GDPR penalty regime.

22. If alignment with the GDPR penalty regime is the desired outcome the Commissioner also urges the UK government to take into account the guidelines on administrative fines being published by the Article 29 Working Party towards the end of 2017.

Information Commissioner

29 September 2017