Upholding information rights

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

[redacted]
Department for Digital, Culture, Media and Sport (DCMS)
[redacted]

By email only: [redacted]

8 April 2022

Dear [redacted],

I am writing to in respect of the consultation which discussed legislation to improve the UK's cyber resilience and recent discussions we have held in relation to this.

About the ICO

As you will know, the Information Commissioner has responsibility for promoting and enforcing the Network and Information Systems Regulations 2018 ('NIS Regulations'), the UK General Data Protection Regulation ('UKGDPR'), the Data Protection Act 2018 ('DPA'), the Freedom of Information Act 2000 ('FOIA'), the Environmental Information Regulations 2004 ('EIR') and the Privacy and Electronic Communications Regulations 2003 ('PECR'). The Commissioner 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 we can, and taking appropriate action where the law is broken.

Introduction

The ICO is designated as the competent authority in the United Kingdom for Relevant Digital Service Providers ('RDSPs') under NIS Regulations. RDSPs are online marketplaces, online search engines and cloud computing services that fall within scope of the regulations.

An RDSP is required under NIS Regulation 12(1) to identify and take appropriate and proportionate measures to manage the risks posed to the security of network and information systems.

In addition to NIS, the ICO also promotes the protection of personal data under the UKGDPR/DPA. Under UKGDPR, organisations are required to implement appropriate technical and organisational measures to ensure that their processing of personal data is secure. Organisations are required to ensure that personal data is processed in a manner that ensures it's appropriate security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures to achieve this.

Organisations are required to report to ICO within 72hrs where they suffer a breach of service (NIS) or security (UKGDPR) which poses a high risk to UK residents.

The ICO has a range of enforcement and sanctioning powers. Under both NIS Regulations and UKGDPR/DPA, these include powers to order corrective measures to be taken to bring an organisation into compliance. If appropriate monetary penalties can be imposed for the most serious and harmful contraventions.

Our perspective in response to this consultation is focused to one of a regulatory view. However, we remain cognisant of impact and cost to organisations regulated by competent authorities under NIS Regulations.

General Comments

Pillar I: Proposals to amend provisions relating to digital service providers.

Expanding the regulation of digital service providers.

The ICO agrees with the approach that managed service providers ('MSPs') are brought within scope of the NIS Regulations due to the role they play in UK society and economy. It should however be noted that some MSPs will already

fall within the regulatory reach of NIS through the cloud computing service they offer.

It is important that where MSPs fall within the scope of the NIS Regulations, a clear definition is provided on the face of the legislation and it is supported by relevant guidance. This will ensure that the correct organisations are captured effectively.

The inclusion of MSPs will increase the number of entities within the ICO's supervision. RDSP's in their nature will often be large, complex and multi-jurisdictional organisations, the addition of MSPs will add a further layer of complexity. This will therefore have an increased impact upon the supervisory functions the ICO has as the competent authority.

It is the view of the ICO that further consideration is required in the proposed modification to bring a number of small and micro businesses into the scope of NIS Regulations. We would be keen to continue to explore this area further with DCMS.

The supervisory regime for digital service providers.

The ICO supports the proposal to introduce a two-tier supervisory regime for RDSPs and can see the positive impact this will have. Particularly where RDSPs supply essential services it would be beneficial that they are subject to the same security requirements and regulatory approach as the Operators of Essential Services ('OES') they supply. This would provide a consistent regulatory approach.

To reliably and effectively capture the digital service providers that are most critical to the UK's resilience within the scope of NIS, consideration is required as to how this information will be supplied to the ICO as the competent authority for RDSPs. Placing a positive obligation on RDSPs to supply certain information on registration would enable the ICO to better identify and mitigate risks.

Pillar II: Proposals to future-proof the UK NIS Regulations.

Delegated power to update the NIS Regulations in the future & delegated power to amend the scope of NIS Regulations.

The ICO recognises the benefits of delegated powers to update and amend the scope of the NIS Regulations as this would future proof the regulations and the capabilities of competent authorities. There are clear advantages to having agile legislation that has the ability to keep pace with evolving and emerging technological developments, the cyber threat landscape and the risks posed to the OES' and RDSPs.

It is, however, essential that clear and appropriate safeguards are in place to ensure that such powers are used proportionately. This would assist in ensuring that there is no over extension in scope beyond the intentions of the NIS Regulations.

Measure to regulate critical sectoral dependencies in NIS.

The ICO acknowledges the benefits in the government being granted the power to designate critical dependencies.

However, it should be noted that protections in this area already exist within legislation. For example, there are organisations that provide critical dependencies that are currently out of scope of the NIS Regulations but under UKGDPR would be a data processor. Under Article 28 of the UKGDPR, where processing personal data, a data processor is required to provide sufficient guarantees as to the security of its systems which must be specified in a contract or other legal act.

In addition, consideration is required as to how information is obtained from organisations in order to identify and designate the critical sectoral dependencies.

Additional incident reporting duties beyond continuity of service.

The ICO notes the benefits detailed in the consultation to expand the incident reporting duties for the OES' and RDSPs. In particular this would provide a broader view of the risks that are posed to the regulated community in scope of NIS Regulations.

It is however important that clear guidance and thresholds are set in this area. Many organisations will deal with hundreds, if not thousands, of potential incidents each day (i.e. through their security operating centre). That threat, however, is often managed before an actual incident occurs. The requirement to report an incident beyond the continuity of the service will therefore need to be clearly defined to ensure consistent and correct levels of reporting. Furthermore, the definition of additional incident reporting may benefit from the continued inclusion of 'authenticity', as per Regulation 1(3)(g) NIS.

Full cost recovery of NIS functions.

The ICO notes the proposed changes in cost recovery. Whilst the proposed hybrid model may have some benefits in the recovery of reasonable costs there will need to be flexibility in the ability to adjust levels of costs in future. This will assist in the future proofing of the regulations and the funding of the functions of the competent authorities.

Through the regulation of the UKGDPR / DPA18, the ICO conduct a fee-based process and therefore the ICO has experience in this area. Consideration would be required regarding the amount of 'reasonable costs' that can be recovered and balanced against the costs to ensure the resilience of the functions of the competent authorities.

Conclusion

The ICO has identified that implementation of these measures would have a substantial impact upon our functions as competent authority for RDSPs. We consider that this impact would be upon our resourcing, capacity and costs in RDSP regulation under NIS.

The ICO is committed to meeting the challenges we would face with an increased number of RDSPs through the inclusion of MSPs, the inclusion of a two-tiered supervisory regime and other proposed amendments. It is our view, however, that for the ICO to be able to achieve its objectives and KPIs, the Government should provide the appropriate and commensurate funding necessary for us to be effective and do the best job we can.

We would welcome the opportunity to further engage with DCMS regarding these proposals and further understand the objectives in order to assist in ensuring that the UK continues to have a strong cyber resilience in critical national infrastructure.

Yours sincerely

[redacted]