The Information Commissioner's response to Ofcom's Call for Inputs about updating Ofcom's guidance on network security

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"). He 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 he can, and taking appropriate action where the law is broken.

We understand that this Call for Inputs concerns Ofcom's 'Guidance on security requirements in the revised Communications Act 2003' (which implements the revised European framework for the regulation of the communications services sector) and the areas of the guidance that would benefit from revision. We note that the main focus of this guidance is the security and availability of communications services and the networks that support them.

In the current climate we feel this is a timely consultation, bearing in mind recent concerns about confidentiality of communications and particularly communications sent across international borders.

We cannot comment on specific technical aspects of compliance with the Communications Act 2003 (CA2003) and Ofcom's proposals to revise the accompanying guidance as to do so is outside our area of expertise, however we would still like to respond to this consultation in more general terms.

Whilst the DPA and PECR are not directly at issue here, it is our view that there is to some extent an overlap between the security obligations set by that legislation and those set by the CA2003.

Our focus is on security issues that could impact on the security of individuals' personal data and compliance with the DPA and PECR, and consequently our response focuses only on those issues where there may be overlap in these areas.

Principle seven of the DPA requires that "*Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*." We interpret this to mean that an organisation should design and organise its security to fit the nature of the personal data held and the harm that may result from a security breach. PECR echoes this obligation and requires that a provider of a public electronic communications service ("the service provider") shall take appropriate technical and organisational measures to safeguard the security of that service.

We would support a move to ensure that guidance for security of services is as clear as possible about the responsibilities and obligations of communications providers (CPs). In our view it is important that security is built in from infrastructure upwards, due to the potential for failures in those services to have a consequential, detrimental effect on the security of personal data and compliance with the DPA and PECR.

We recognise that future concerns cannot be predicted with absolute certainty and understand Ofcom's desire to future-proof any guidance. It is our view that any guidance produced should, to some extent, anticipate future possibilities without being unduly restrictive or prescriptive. This could for example be achieved by setting out minimum standards and placing an onus on CPs to plan carefully, carry out impact assessments, undertake rigorous testing and to continually review the security and resilience of their services and networks.

The consultation highlights several areas of risk, including supply chain risk, the use of third party data centres and the needs and obligations of smaller CPs that are currently not addressed by Ofcom's guidance. If these areas have been recognised to be missing from existing guidance then we would support their inclusion in the revised guidance in the interests of clarity.

If areas of vulnerability around supply chains and the use of third party data centres have been identified, it would be helpful for the guidance to address these. The DPA's approach to this issue is to describe the steps that must be taken to ensure that delegation of duties are acknowledged, roles are clearly delineated and responsibility assigned (the relationship between the organisation which determines the purposes for/manner in which data are processed (data controller) and the data processor who acts purely under their instruction). This is particularly important where a supply chain involves multiple parties, to ensure all involved know who is ultimately responsible and to consider whether the customer is aware of what is happening with their information.

We note the proposals to improve consistency of information made available to individuals, and the potential for there to be a standardised approach. We would support an approach with greater transparency where more information is provided to consumers so they are able to make informed choices about a CP's services, network availability and interconnections. We do however recognise that it can be challenging to provide information that is accurate and meaningful to a consumer. A key aspect of the DPA is the requirement under principle 1 that individuals be informed about what their data will be used for. This is to enable individuals to make an informed decision about whether to interact with an organisation. There is also a requirement under PECR, whereby if service providers take appropriate measures but there is still a significant risk to the security of the service, they must inform the subscribers concerned of the nature of the risk, any appropriate measures the subscriber may take to safeguard against the risk and the likely costs to the subscriber involved in taking such measures.

We note the similarities between the reporting obligations set by Ofcom in respect of significant security incidents, and those set by PECR (where service providers have a specific obligation to notify the Information Commissioner's Office about a personal data breach within 24 hours of detection). In our view it is important that Ofcom's guidance about reporting is clear as to who needs to report what. It is also difficult to see why security reporting should be restricted (by thresholds) to solely capture the activities of larger CPs when there are also inherent risks for security incidents experienced by smaller CPs as well. We therefore agree with the stance of relative thresholds to replace the absolute thresholds that may only pick up on incidents affecting those with a larger customer base. Similarly if it has been noted that in practice most reporting is solely based on the quantitative thresholds and not qualitative criteria then we feel it may be important to give more weight to these also so that important and significant incidents are not missed from the reporting requirements.