SHOOSMITHS

No.	Question	Is a response required (Yes/No)	Response to question (Yes/No)	Response to question (each less than 3,000 characters)
1	What is your name?	No	Alice Wallbank	
2.	What is your email address?	No	alice.wallbank@shoosmiths.com	
3.	Are you responding to this consultation on behalf of an organisation?	Yes	Yes	
4.	What is your organisation?	No	Shoosmiths LLP	
5.	Are you answering as: ○ An organisation seeking to use (or already using) encryption to protect personal information ○ An organisation that provides encryption technologies (e.g. software or hardware solutions) ○ An academic or researcher ○ An individual acting in a professional capacity ○ An individual acting in a private capacity (eg someone providing their views as a member of the public) ○ Other	Yes	An individual acting in a professional capacity	
6.	If you are an organisation, or you're responding on behalf of one, what's your size?	No	(I can sort this)	
7.	Do you currently use encryption?	Yes	Yes	As a law firm, Shoosmiths LLP handles highly sensitive information. In accordance with data protection law, professional conduct rules and applicable cybersecurity standards, it is the firm's policy that all information assets, including systems, applications, storage, data in transit (e.g., emails and file transfers), backups, computing devices,

				and removable media, must have Shoosmiths-approved encryption software installed and enabled where possible.
8.	Have you faced any particular challenges implementing encryption?	No	No	Most modern software already includes built-in encryption features and uses proven, standard algorithms and protocols that underpin encryption technologies.
9.	If you answered "yes", what challenges have you faced?	No		N/A
10.	Do you agree that this update provides greater clarity on our expectations for your use of encryption, as compared to the previous version?	Yes	Strongly agree Agree Disagree Strongly disagree Unsure / don't know	
11.	Does the section on encryption and data protection law give you a clear and useful understanding as to why encryption is important?	Yes	Yes	
12.	If you answered "no", please explain why.	No		We agree that the section on "encryption and data protection" provides a useful summary of the reasons for encrypting personal information in transit or that is otherwise stored on personal computing devices (such as PCs, laptops and smartphones) and removable media (such as USB flash drives, external hard drives and CDs). However, we suggest that this section could be amended to provide further clarification on the extent of the requirements under UK data protection laws.Uk What does UK data law say about encryption? Additional clarification could note that where a controller has implemented appropriate encryption measures to the extent that personal data the subject of a data breach is unintelligible to any person not authorised to access it, that controller will not be required to communicate the data breach to the relevant data subject(s)(Article 34(3)(a)). For example, if an encrypted laptop is stolen but protected with full-disk encryption and a strong password policy, notification under

				Article 34 may not be necessary—provided the device was locked and keys were not stored on the device. This is a potentially important incentive to use encryption effectively. In addition to protecting against external threats, encryption also supports the UK GDPR's data minimisation and purpose limitation principles. Does this mean we must encrypt personal information? It would be useful to note that, whilst it is not a prescriptive requirement under UK data protection laws to encrypt personal information held by an organisation, the ICO has previously taken enforcement action against entities which failed to implement adequate technical and organisational measures to protect personal information, including failing to encrypt the organisation's devices where it would have been appropriate to do so: for example, previous ICO enforcement action against Meta and Advanced Computer Systems. Does this mean we must encrypt personal information? We recommend adding an additional bullet point to clarify that for organisations that regularly handle sensitive personal data (e.g. health records, biometrics, children's data), failure to implement encryption could be interpreted as failing to meet appropriate security standards. It would be especially helpful if the ICO could signpost organisations to more industry-standard tools such as password managers, SSO solutions and trust authentication providers.
13.	Are the descriptions of the main uses of encryption - storage and transfer – sufficiently clear and actionable for you?	Yes	No	
14.	If you answered "no", please explain why.	No		We suggest that additional information in this section would promote clarity about how encryption can practically be used to protect personal information stored on computers and removable media.

				What is full-disk encryption? In the first example provided, additional clarification could mention that any storage solution used by the hospital (whether it be network attached storage or storage area networks) needs to be encrypted in addition to the terminal. How do we implement full disk encryption? We suggest that the example provided in this section might be clearer if additional information were provided about the circumstances surrounding the fine issued by the ICO to the Glasgow City Council, and practical suggestions for what should have been done, following best practice. What are the residual risks with encrypted data storage? In addition to the listed risks, we note the following risks: • lack of access control practices (i.e. even if the organisation encrypted files correctly, it should limit who has access to passwords and regularly rotate passwords and keys); • lack of compliance with the organisation's software security practices. This can be mitigated with regular employee training of the organisation's practices; and • use of out-of-date versions of software e.g. using out of date ciphers or versions of transport layer security. How can we test if our HTTPS implementation is effective? In addition, it might be noted that publicly available online testing services should be used in a safe testing environment that isn't connected to the real, live system or its data.
15.	Are the encryption scenarios relevant for the processing that you do?	Yes	Yes	While the details around encryption and associated scenarios provide a solid foundation for many organisations, we feel the

				guidance would be enhanced with content about incoming or state of the art technologies. Given the potentially wide audience including those advising entities in regulated industries, or who handle high volumes of high-risk data, we would suggest that both homomorphic encryption and quantum-resistant encryption are explicitly highlighted, with a link to more detailed guidance. A high level explanation, definitions in the glossary, and links provided to appropriate external resources and technical guidance, such as those maintained by NIST and the NCSC, would also be useful. This additional context will help the ICO ensure that its guidance remains up-to-date with international standards.
16.	If you answered "no", please explain why.			N/A
17.	Are there any encryption use cases or scenarios in the current draft that you think are no longer relevant?		No	
18.	If you answered "yes", please tell us which ones and why:			
19.	Are there other encryption use cases or scenarios that you think we should include in the final version of the guidance?		Yes	The draft guidance offers a welcome and pragmatic resource, particularly for legal, privacy, and compliance professionals who are increasingly required to engage in informed dialogue with information security and IT assurance teams. Given the growing overlap between data protection and cyber regulation (such as NISR, the expansion of CNI designation, the Telecommunications (Security) Act, and the anticipated Cyber Security and Resilience Bill), there is a greater demand on legal and compliance professionals to meaningfully engage with their information security colleagues on encryption. As these individuals become more involved in the selection and implementation of security controls, the ability to understand and challenge assumptions around encryption technologies becomes

				critical. The guidance should ideally aim to equip users with sufficient context to interrogate whether a particular encryption approach meets the ‘state of the art’ threshold within the specific operational and threat landscape of their organisation. The section addressing residual risks would benefit from the addition of common threat scenarios where encryption may offer limited protection, such as Active Directory-based attacks, man-in-the-middle exploits, and administrative account compromises. These remain prevalent attack vectors where encryption alone is insufficient as a mitigating control and should be understood in the broader context of layered defence strategies. Furthermore, it would be helpful for the guidance to briefly distinguish between encryption at different layers, particularly application and database-level encryption, and to summarise their advantages relative to full-disk or file-level encryption.
20.	If you answered "yes", please tell us.			
21.	Are there any areas of this draft guidance that you found unclear, or that you think require further detail?			The ICO guidance will provide welcome clarity on what organisations should consider when assessing the appropriateness of the technical and organisation measures used by their organisations to protect personal data. Generally the draft guidance is clearly set out and contains useful diagrams (particularly Figures 1 and 2 in the section titled “What is encryption?”), and useful encryption scenarios. Noting that a balance must be struck between practicality and accessibility, we make the following suggestions for additional clarifications which may help bridge the gap between technical and non-technical readers. What is encryption? The ICO may wish to consider adding a more technical, definition of encryption:

				Encryption is a cryptographic process that transforms readable data (plaintext) into an unreadable format (ciphertext) using an algorithm and an encryption key. It is a core component of data security strategies for ensuring confidentiality, integrity, and authenticity of personal data, particularly under Article 32 of the UK GDPR, which mandates “appropriate technical and organisational measures to ensure a level of security appropriate to the risk”. It would be useful to note that symmetric encryption is suitable for at-rest encryption and is typically used for encrypting large volumes of data, whereas asymmetric encryption is more appropriate for securing small datasets and data in transit. Additionally, hybrid models (which combine both) are also widely used in secure communications protocols. Encryption is one method of cryptography that can be used to protect personal information, but not the only method. Other methods including hashing, salting and digital signatures, although we note that alternative methods of cryptographic encryption are outside the scope of the guidance. <ins>General comments</ins> Useful additions would include a sample encryption policy covering areas such as roles and responsibilities, key management, use of encryption tools and standards and training for employees and contractors. The ICO may also wish to include a short practical checklist covering what organisations should consider when reviewing their compliance with the UK GDPR’s security principle, including checking whether the organisation uses NCSC-approved encryption standards, has a documented key management policy and undertakes regular testing and validation of encryption tools and staff training on handling encrypted data.

				Sector-specific guidance would be welcome for future versions especially in regulated sectors.
22.	The ICO would like your permission to publish your consultation response. Please indicate your publishing preference: ○ Publish response ○ Publish response anonymously (this will remove all personal data, eg name) ○ Do not publish response		Publish response	