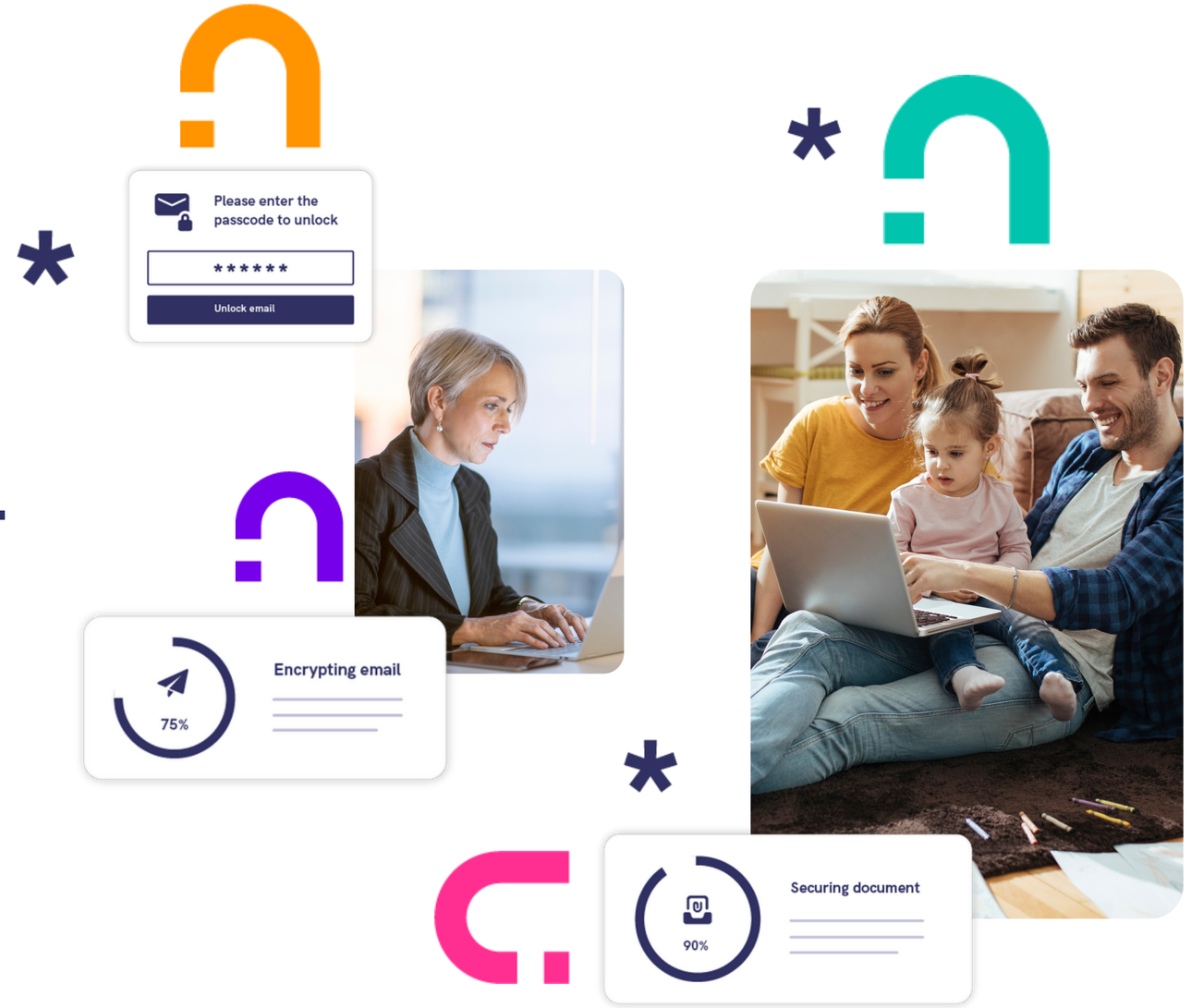
mailock

Personally Identifiable Data - Risks and Vulnerabilities



CYBER ESSENTIALS CERTIFIED PLUS

British Assessment Bureau UKAS MANAGEMENT SYSTEMS 0289 ISO 27001 INFORMATION SECURITY MANAGEMENT

Crown Commercial Service *Supplier*

PII DATA OVERVIEW

An introduction

To fully assess an organisation's risks and vulnerabilities in the management and handling of Personally Identifiable Data, a clear understanding of what constitutes this important clause of EU and now UK GDPR is essential.

It would be fair to say that many organisations are likely to underestimate how much personal data they manage and the risks associated with this.

So what is personal data?
Personal data can be considered any piece of information that someone could use to identify a living person.

Any of the following can be considered personal data:

- Identity: This includes forename and surname, date of birth or birthday, signature, and gender.
- Contact Info: This includes personal or work address details, phone number, and email address.
- Personal: This includes bank and or credit card details, passport or driving licence.
- Professional: This includes details of job title, employment details, salary etc.
- IT: This includes an individual's IP address, browsing history, and cookie preferences.

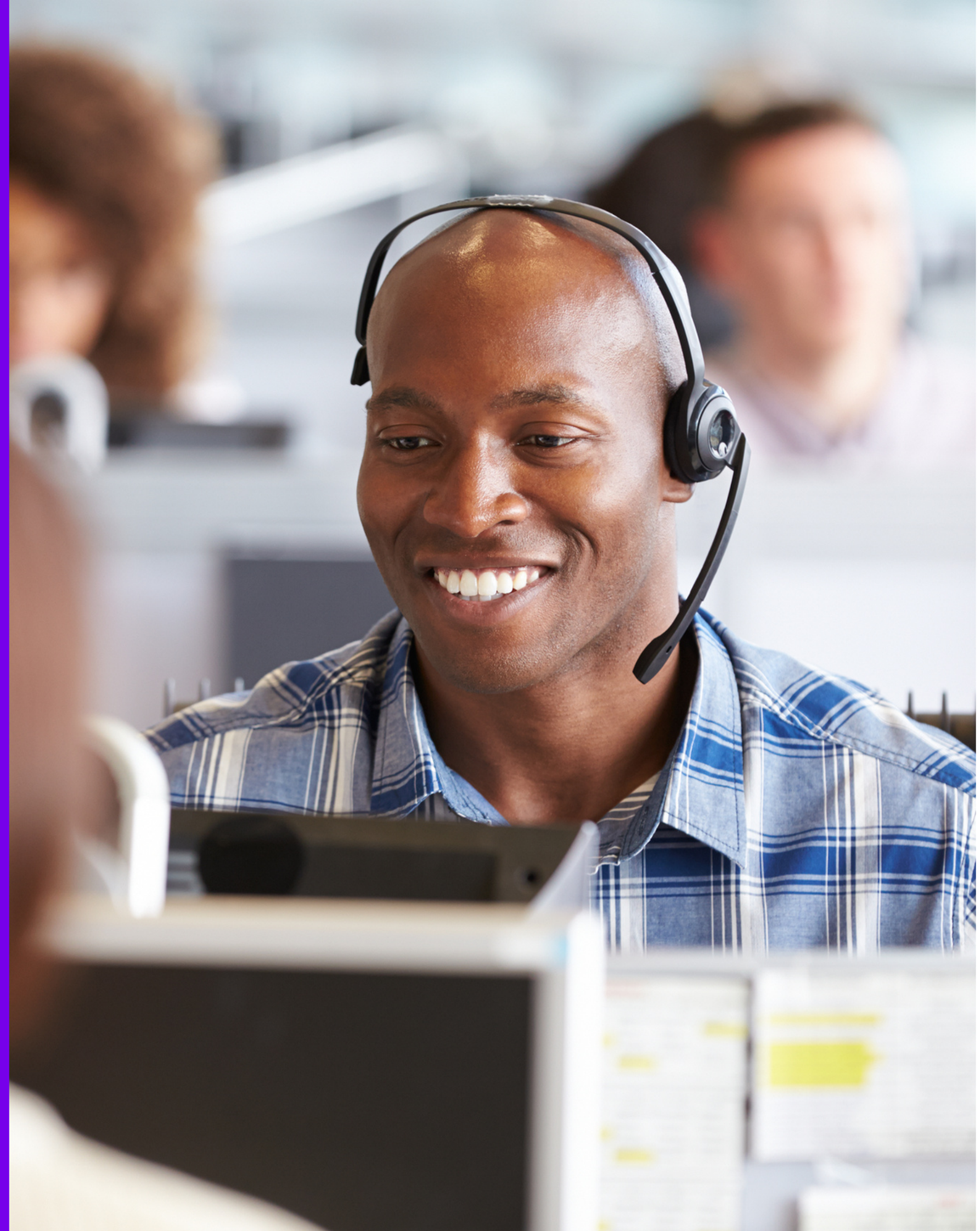
Personal data can also be physical such as a photo, a CCTV image, and fingerprints.

Huw Thomas

Compliance & Quality Manager

The traditional perception of data and identity theft as an act committed by a lone individual rummaging through trash for personal information is outdated and underestimates the modern reality of the situation.

Today, a highly organised criminal infrastructure exists that only needs a small piece of information, like a non-shredded envelope, to add to information obtained from other sources in order to reveal an individual's identity. Each piece of data can be thought of as a puzzle piece, and when multiple pieces are combined, they can be used to construct a complete picture of a person's identity. The expertise of the hacker or criminal has shifted from obtaining information to piecing it together.



PERSONALLY IDENTIFIABLE INFORMATION (PII)

Multiple data points and vulnerability

Many organisations will often collect, use, share and store single pieces of information unprotected, which could easily, with the right tools, and with information from other sources, be put together to identify an individual customer or employee.

For such an organisation, Personally Identifiable Information (PII) leakage should be considered a significant information security vulnerability. This vulnerability could be considered critical if any of the information could be used to track, identify or contact a particular individual. This could be any combination or component of the above list.

There is also a sub-category of personal data termed “sensitive data”, this being data requiring greater protection and includes data on an individual’s ethnicity, sexual orientation, medical history etc.

There is often confusion that non-sensitive PII does not need to be secured. As can be seen from the description above, any non-sensitive data could be linked to information from other sources or databases to reveal much more than intended.

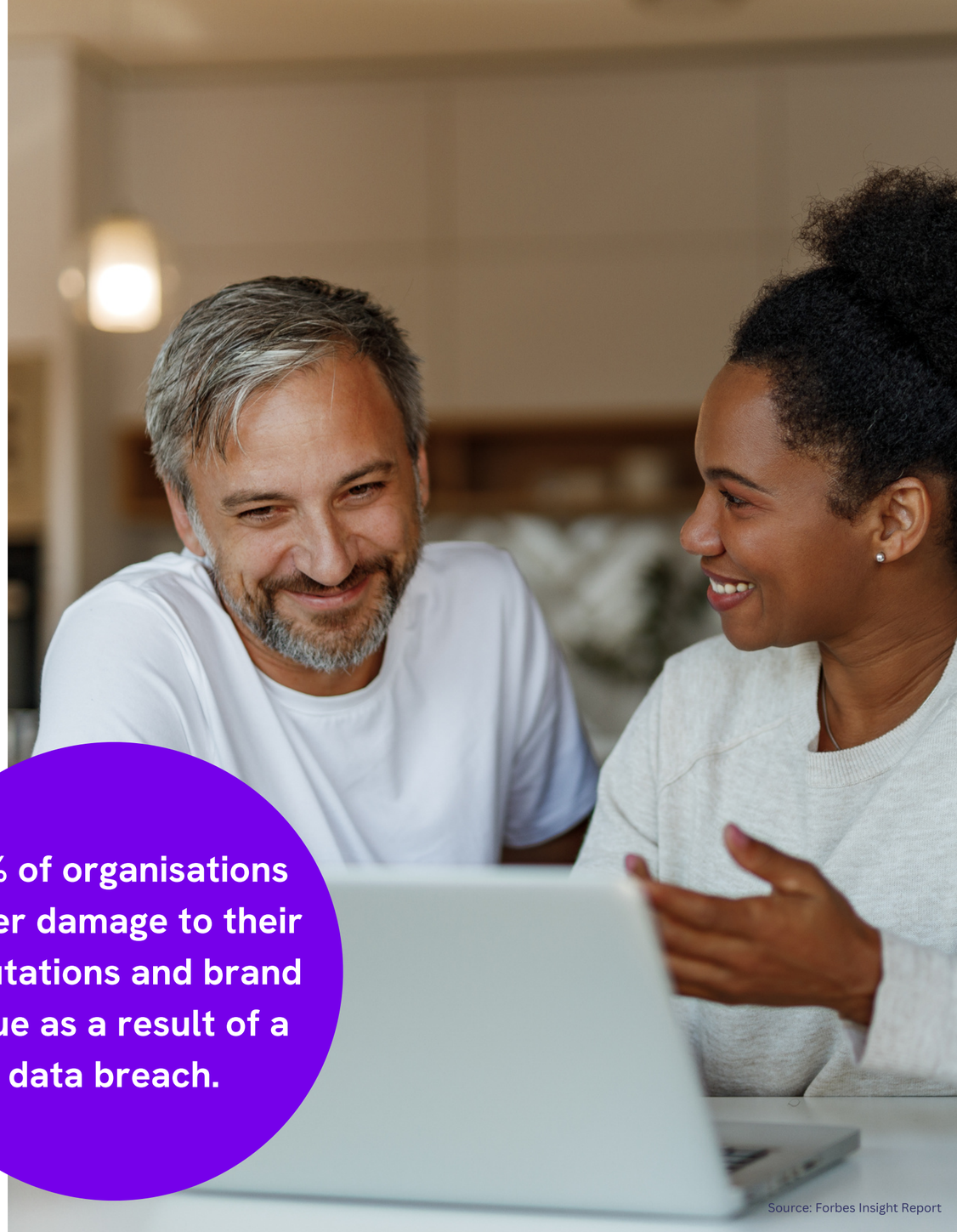
PERSONALLY IDENTIFIABLE INFORMATION (PII)

Multiple data points and vulnerability

Any organisation which processes Personally Identifiable data must consider the risks of doing so and must have a good understanding of the risks that arise when failing to keep all aspects of PII secure.

As well as the potential financial implications from regulatory bodies, such as the Information Commissioner's Office (ICO), for not securing PII for their customers in breach of GDPR, the reputational damage could be far more damaging to any organisation.

It is therefore essential to consider what security measures are in place, particularly in the sending and delivery of such information, to ensure they maintain the confidentiality, integrity and availability of the data they are processing. Protecting this data from hackers and cybercriminals should be integral to any organisation’s customer data and information security management.



46% of organisations suffer damage to their reputations and brand value as a result of a data breach.

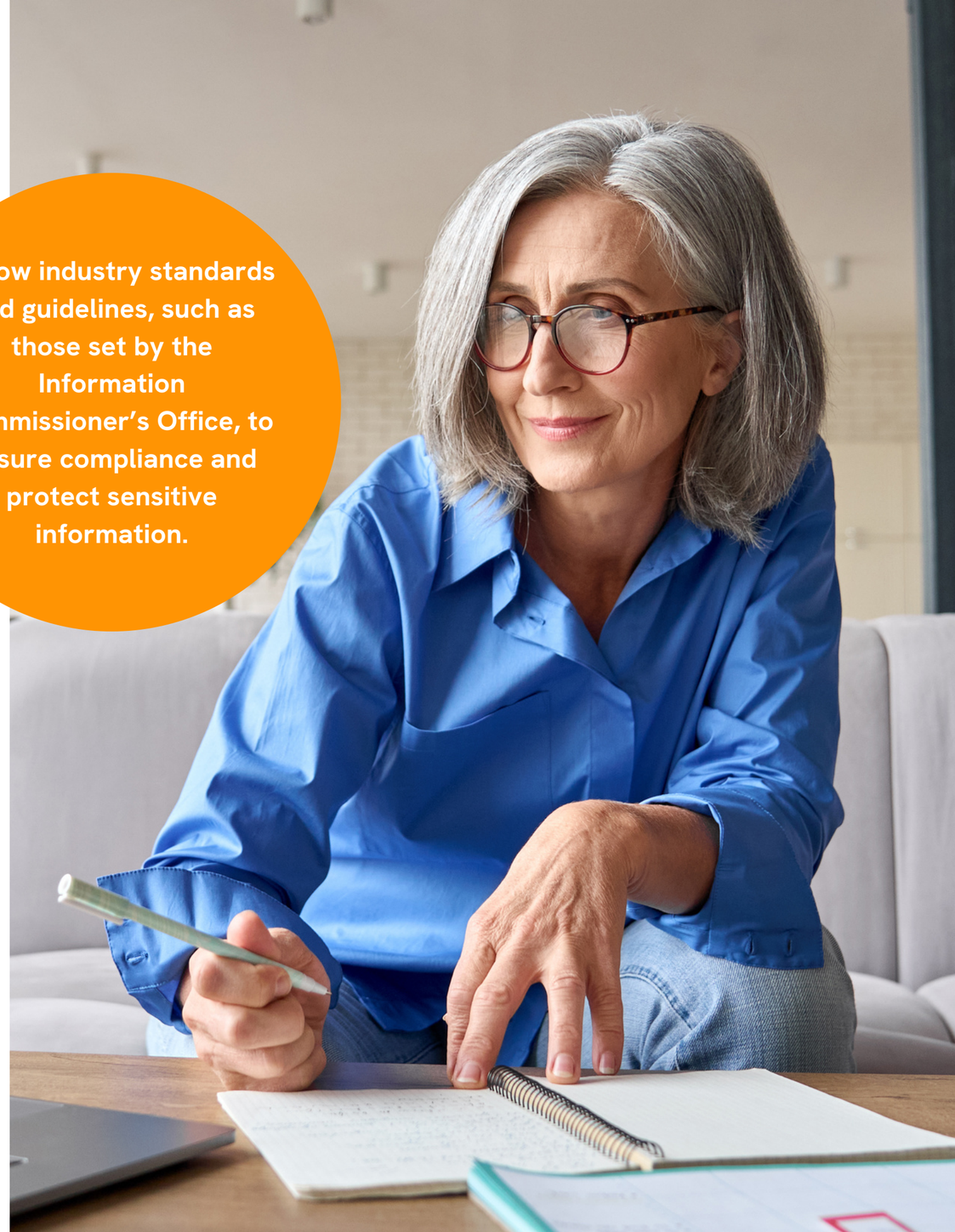
Source: Forbes Insight Report

WHAT YOU CAN DO

Mitigating the Risk

- Optimise your data storage and retention strategy by regularly reviewing and purging unnecessary information.
- If you need to handle PII within your organisation, it is safest to treat all information as actual or potential sensitive data, ensuring it is secured in transit and at rest.
- Implement strict protocols for handling sensitive data, including secure transmission and end-to-end encryption capabilities. Remember - only one piece of information in the hands of a sophisticated hacker can be dangerous.
- Data is particularly vulnerable during transmission - The ICO recommends recipient identification, such as two-factor authentication, as a minimum standard benchmark before you permit access to a secured email.

Follow industry standards and guidelines, such as those set by the Information Commissioner's Office, to ensure compliance and protect sensitive information.

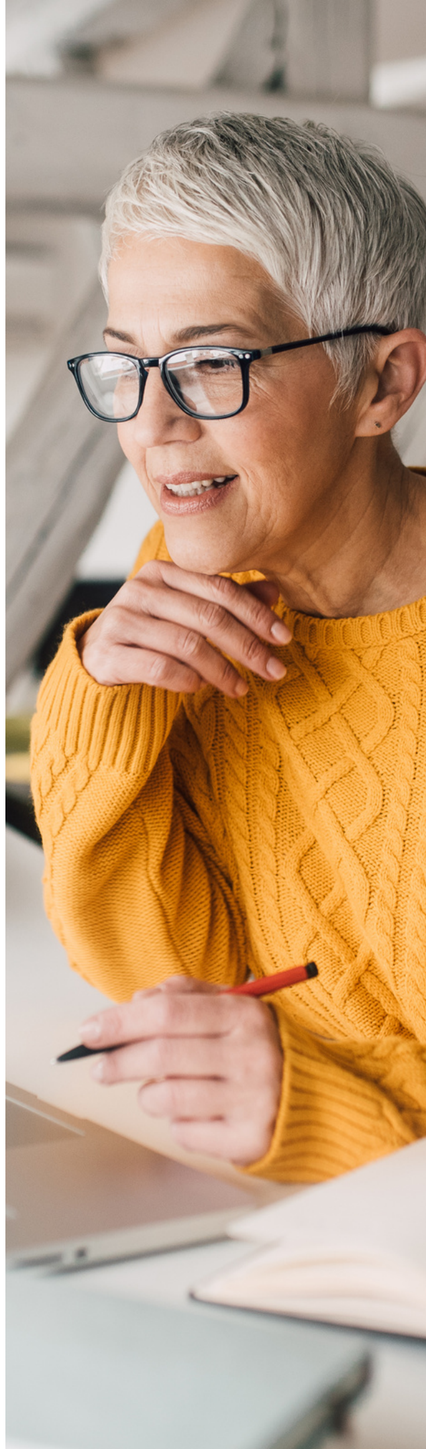


COMPLIANCE

Summary

While UK GDPR and ICO guidelines are important, they are not the only pieces of legislation that need to be adhered to within your business:

GDPR	Allows data transfer whilst providing safeguards to protect personal data. Empowers the Information Commissioner to levy fines of up to £17m or 4% of global turnover for serious breaches.
ICO (Information Commissioner's Office)	The ICO is explicit in its warning – 'Without additional encryption methods in place, the email body and any attachments will also be accessible to any unintended recipient or third party who intercepts the communication.' It goes on to provide significant 'best practice' guidance on encryption - 'A common type of personal data disclosure occurs when an email is sent to an incorrect recipient. Data controllers should be aware that encryption will only provide protection to personal data sent by email if the incorrect recipient does not have the means to decrypt the data [e.g., does not have the decryption key]'.
SMCR (Senior Managers & Certification Regime)	Aims to drive personal accountability by promoting improved corporate culture, governance and transparency. Makes senior managers personally accountable for any form of misconduct.
FCA (Financial Conduct Authority)	Uses SMCR and personal accountability of senior management to ensure a code of conduct for all staff in financial services firms [big and small].
NCSC (National Cyber Security Centre)	As part of GCHQ, the NCSC publishes advice on the latest vulnerabilities and risks as well as advice on what security professionals should be doing to protect their organisations & customers.



v1

mailock

Beyond Encryption

Huw Thomas

Compliance & Quality Manager

Implementing protection measures not only helps in saving costs and reducing anxiety, but also often results in savings that surpass the cost of the protection itself.

Additionally, these measures often have a positive impact on environmental, social, and governance (ESG) factors, making them an ideal addition to a company's Net Zero goals or corporate social responsibility strategy and messaging.

NEED MORE INFORMATION?

Contact us:

info@beyondencryption.com

AEGON SimplyBiz Group ORIGO PARAGON Customer Communications ROYAL LONDON HSBC