GDPR: What could a breach mean for your business?

The GDPR came into force in May 2018 and introduces a duty on organisations to report certain types of personal data breaches to the regulator. Certain high risk breaches must also be notified to data subjects. As owners and processors of data, Treasurers should be aware of their obligations and have processes in place to detect, prevent, investigate and manage breaches.

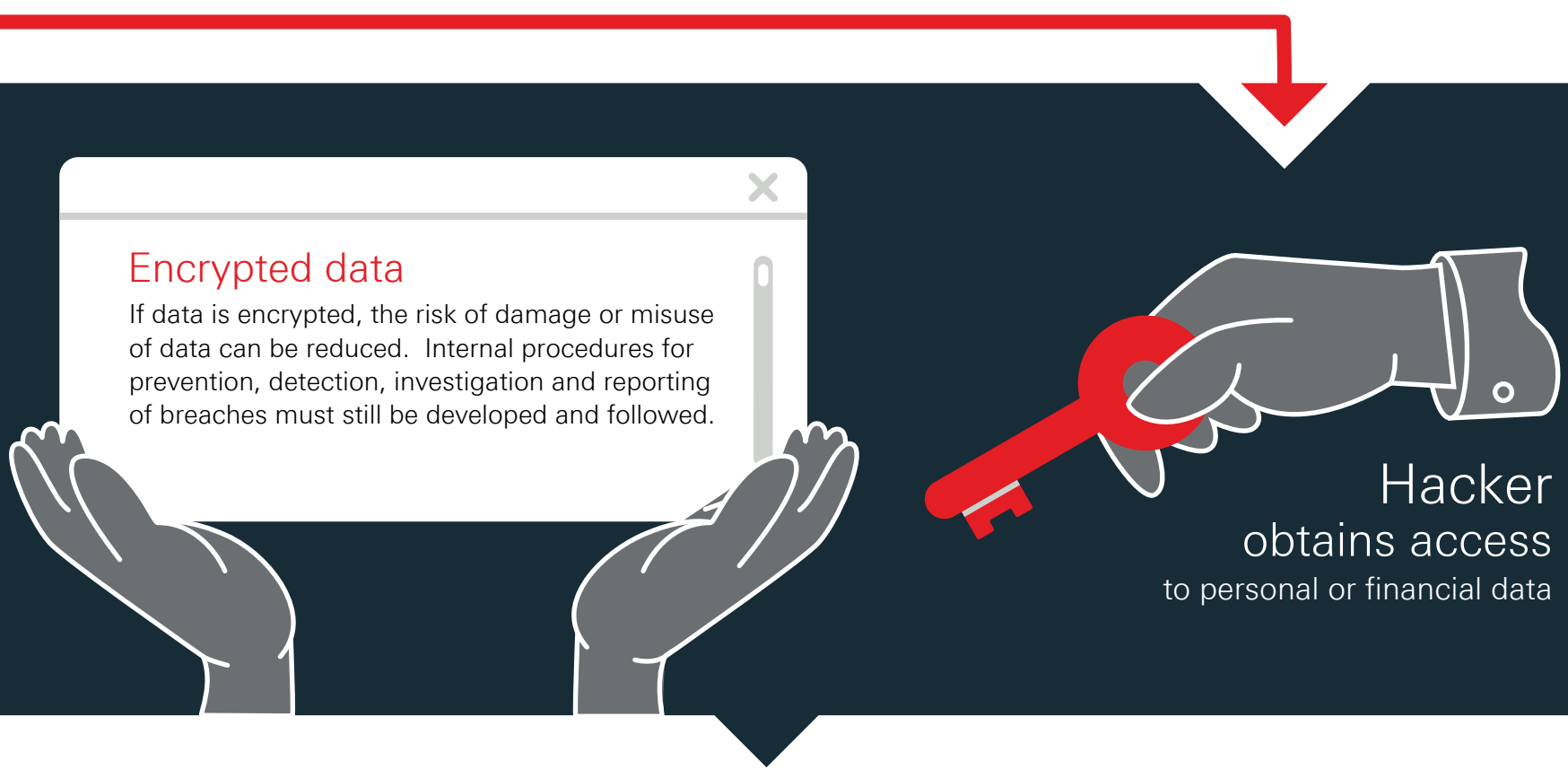
A personal data breach occurs where a breach of security leads to an an accidental or unlawful destruction, loss, alteration disclosure or unauthorised access to data.

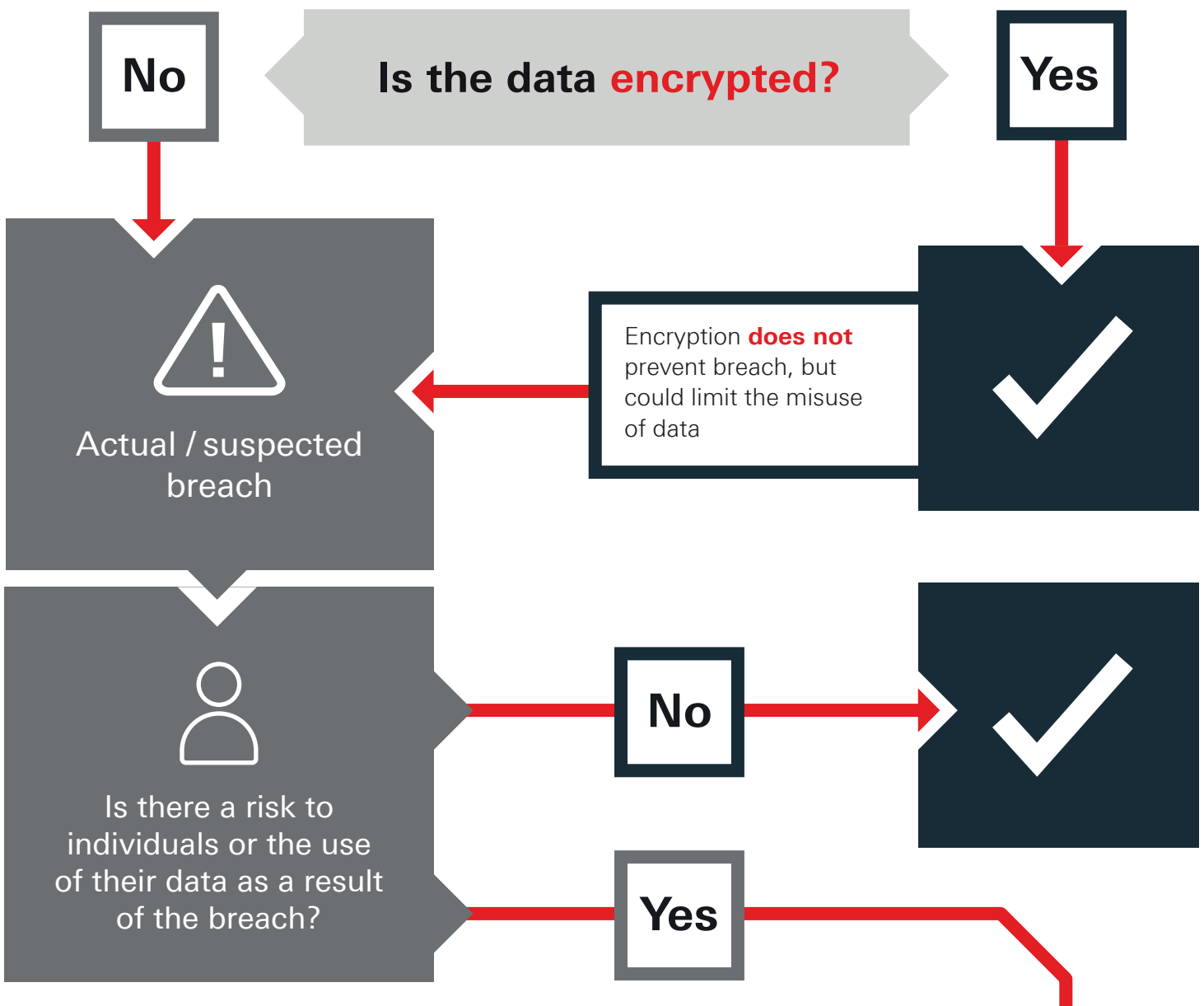
A personal data breach can happen for a variety of reasons. Data encryption is an important way of tackling a potential breach. Technology for storing and processing data correctly and securely is also essential, but must be backed with effective policies, processes and staff training.

Some examples of data breaches:

- Unauthorised access to unsecured facility or system
- User accesses phishing website or clicks on phishing website
- Breach of third party processor within / outside EU

Companies outsourcing to third party processors do not lose their legal liability in case of breach at or by the third party

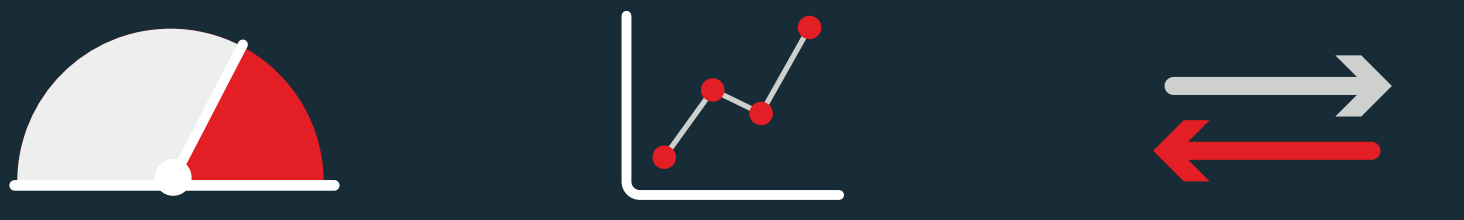




Certain breaches must be reported to the ICO within 72 hours and certain types of breaches must also be notified to data subjects. More information can be found on www.ico.org/uk

Failure to report to the ICO within 72 hours could result in an additional fine. Companies can report a suspected breach and then provide updates as the situation becomes clearer. Processes need to be in place for rapid notification.

1 Has your organisation given notice of breach **within 72 hours?**



gbm.hsbc.com