Integro & Naq
GDPR for *SMEs & Freelancers.*

Nadia Kadhim
CEO *Naq*

INTEGRO ACCOUNTING | naq.

CYBER ESSENTIALS CERTIFIED

Cyber Accelerator Alumni
in association with National Cyber Security Centre

naq. UKGDPR COMPLIANT

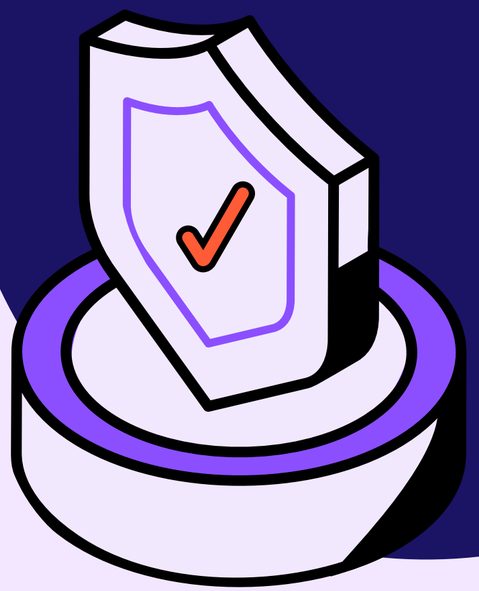
naq. EUGDPR COMPLIANT

Intro to *GDPR*

- Difference between UK GDPR & GDPR.
- Both pieces of legislation designed to protect individual's pers information & enhance privacy rights.
- Framework to how individual's data is collected, stored, processed, and shared by companies across the UK and the EU.
- All businesses handling personal information must abide by the UK GDPR/GDPR.

naq.

Why you should *care about GDPR.*



"Complying with the GDPR is not only necessary to protect yourself from fines and legal trouble, but will instil more trust in your users and ultimately improve your relationships and company image. This is important for businesses of all sizes."

naq.

Controller *v.* *Processor.*

- Controllers are responsible, accountable & liable.
- Processors process on behalf of the Controller.
- Protecting "personal" data:
  - Names, email addresses, addresses
  - Date of birth, gender
  - Video, photography

naq.

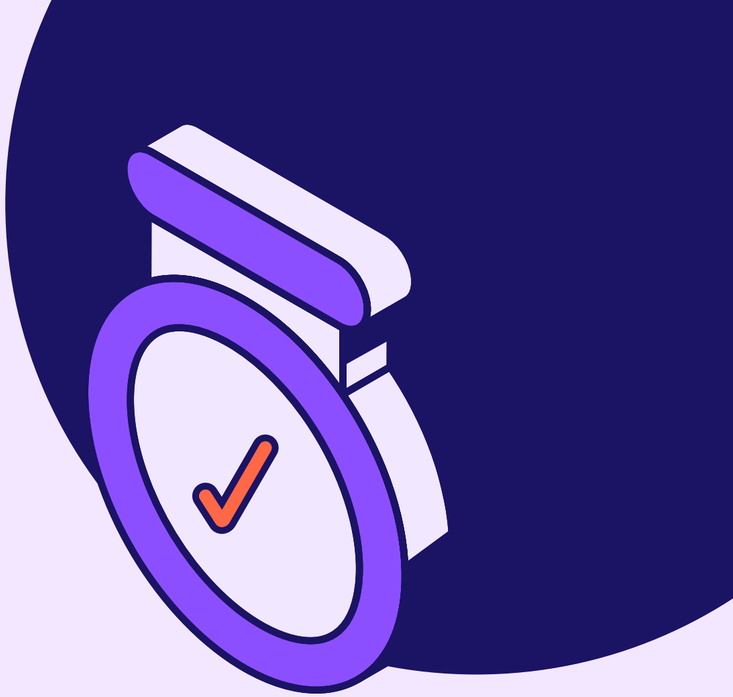
Basic principles of *GDPR*.

- Lawful basis
  - Legal obligation
  - Legitimate interest
  - Consent *
- Data Protection by Design and Default
- Fairness and Transparency

naq.

People.

How do you minimise human risk?



- Training (GDPR, phishing, account security)
- Processes laid down in documentation
- Testing processes
- Contractual obligations
- Contractual liability

naq.

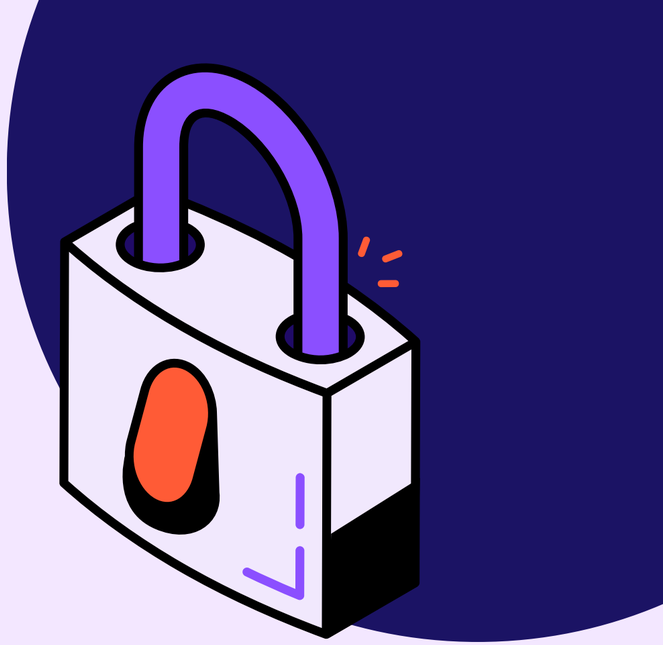
Processes.

- Establish and write down process for
  - Data retention
  - International data transfers
  - Supply-chain management
  - Data subject requests
  - Incident response and data breach notification

- Inform through privacy policy

naq.

Technology.

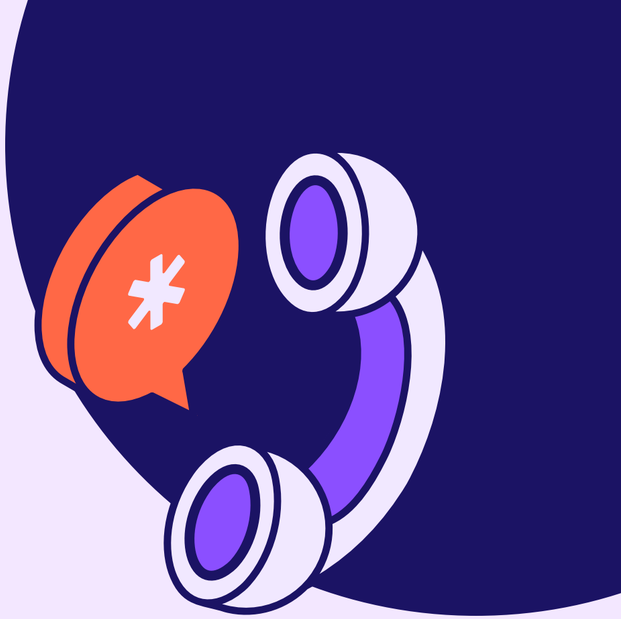


Security by design

- Devices
  - Antivirus, regular updates, admin account, encryption & firewall
- First &Third party cloud applications
  - Unique and secure passwords, MFA, encryption, access controls and monitoring
- Network equipment
  - Encryption, firewall, access controls and monitoring
- Office
  - Clear desk & clear screen, CCTV, access controls

naq.

Incident response
& Data Breach notification.



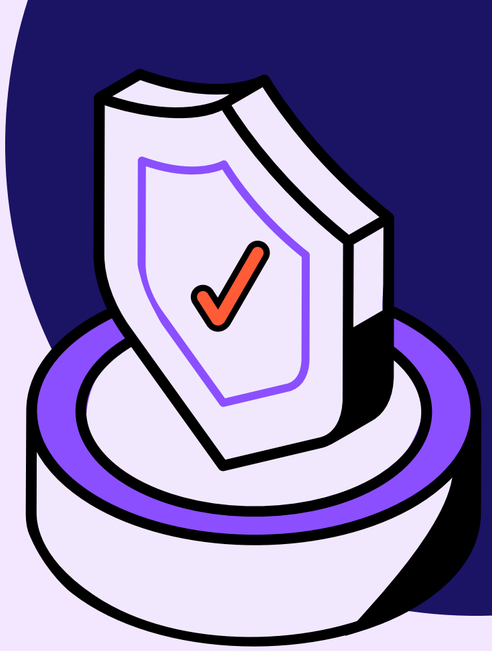
- Incident response plan: Prepare; Identify; Contain; Eradicate; Restore; Learn; Test and Repeat

- Not all incidents are data breaches

- Data breach
  - High risk: Report to ICO within 72 hours
  - Very high risk: Report to data subjects without delay

naq.

4 Common GDPR Compliance *Myths.*



1st Myth: GDPR only applies to big businesses

Reality: GDPR applies to all organizations, regardless of size, that process the personal data of UK/EU residents.

2nd Myth: GDPR only affects companies based in the UK/EU

Reality: GDPR applies to any organization that offers goods or services to EU residents or monitors their behaviour, regardless of its location.

naq.

4 Common GDPR Compliance *Myths.*

3rd Myth: GDPR compliance is a one-time task

Reality: GDPR compliance is a continuous effort and requires regular data assessments, updates to privacy policies, and employee training to ensure continued compliance.

4th Myth: GDPR compliance is only about avoiding fines

Reality: GDPR compliance goes beyond avoiding penalties. It helps small businesses build trust with customers, enhance data security practices and ensure the security measures are in place to keep everyone's data protected.

naq.

Take the *Complexity* out of your company's *Compliance.*

nadia@naqcyber.com

www.naqcyber.com

naq.