CLYDE&CO

Data (use and Access) Bill , DORA, EU AI Directive and NIS2 : low profile changes creating significant challenges for business data managers and insurers in 2025

Nick Gibbons, Legal Director

The new legislation

New EU and UK legislation will make data processing compliance and insurance much more complicated:

- Data (Use and Access) Bill
- Digital Operations Resilience Act (“DORA”)
- EU Artificial Intelligence Act
- Network and Information Security Directive 2

Data (Use and Access) Bill

- First reading in House of Lords on 23 October 2024
- broader access to consumer data for the improvement of public services and consumer convenience and choice
- Financial penalties for companies that fail to comply with data access regulations
o

Data (Use and Access) Bill

- Replaces Information Commissioner with
- “Information Commission “
- Permits sharing of personal data within the public sector to improve
- Service delivery and enhance research . E.g within NHS
- Smart data – allows customers and businesses to ask for their data to
- be shared directly with them and authorised third parties
- in order to receive tailored comparisons

Data (Use and Access) Bill

Data protection and privacy:

- New rules for lawful data processing in compliance with GDPR
- Businesses must be clear about when AI is used to make relevant decisions, giving customers the option to request a human perspective.
- Enhanced right sto request access, restrictions, corrections, or deletions.

Data (Use and Access) Bill

Framework for online digital verification:

- Explicit confirmation for users to understand how their data is being used and shared, when applicable
- Not “profiling” users for third-party marketing
- Not creating large data sets that risk exposing sensitive information about users
- Verified providers that adhere to this framework will receive certification and a “trust mark

Digital Operations Resilience Act (DORA)

Motivation for DORA:

- Interconnectivity of financial sector and increasing number of cyber attacks

A mish mash of national regulations in finance sector

- EU has therefore created a framework of principles to identify and mitigate ICT risks by requiring financial sector to adhere to common resiliency standards

Provisions

- Mandatory risk reporting

- Digital Operational Resiliency testing including threat led penetration testing
- Information and intelligence sharing

- Managing ICT third party risk

- European Supervisory authority to establish arrangements with regulators in non EU countries

DORA FOOTPRINT

DORA applies to over 21,000 EU financial institutions including
Banks , credit companies, investment funds, insurers and
ICT service providers

Financial institutions outside of EU must also comply if they
Provide critical ICT processing to EU financial entities.

UK Insurers and many of their policyholders will therefore need to comply

DORA Sanctions

- Financial institutions and ICT Suppliers must perform resiliency testing to demonstrate compliance
- Regulators have power to perform audits on financial entities and ICT service suppliers
- It is not necessary to suffer an outage or cyber attack to be fined
- Non compliance with DORA will carry significant penalties and potentially criminal prosecution
- fine equivalent to 1%of an entity's annual turnover for a period of
- up to 6 months
- Likely to become a benchmark for the courts

Differences between GDPR and DORA

- GDPR only concerns personal data: DORA covers every type of data every type of data : commercial information, trade secrets,IP , confidential information
- GDPR requires a data controller to enter into an agreement with a data processor: it says nothing specific about ICT service providers
- GDPR technical security guidance is unspecific:DORA is much more detailed and specific
- GDPR generally only bites after an incident has been reported to the ICO: DORA includes auditing provisions
- GDPR fines are infrequently imposed:It appears that
- DORA will entail much more rigorous sanctions

Network and Information Security (NIS) Directive 2

- Clear and precise rules
- All types of data – not just personal data
- More entities and sectors will have to take measures to protect themselves:
- “Essential sectors” such as the energy, transport, banking, health, digital infrastructure, public administration and space sectors will be covered by the new security provisions.
- companies, governmental and public bodies
- The new rules will also protect so-called “important sectors” such as postal services, waste management, chemicals, food, manufacturing of medical devices, electronics, machinery, motor vehicles and digital providers.
- All medium-sized and large companies in selected sectors will fall under legislation.

EU Artificial Intelligence Act

Comprehensive set of rules for providers and users of AI systems, which details transparency and reporting obligations

- expected to affect *all AI systems impacting people in the EU*, including any company placing an AI system on the EU market or companies whose system outputs are being used within the EU (regardless of where systems are developed or deployed).
- Large fines :

  Up to 7% of global annual turnover or €35m for prohibited AI violations.

  Up to 3% of global annual turnover or €15m for most other violations.

  Up to 1.5% of global annual turnover or €7.5m for supplying incorrect info Caps on fines for SMEs and startups**.**

Existing security certification inadequate

Cyber essentials:

Basic technical security requirements

No focus on staff training

No teeth

Out dated

No reference to third party service providers

ISO 27001:

No reference to third party service providers

No auditing

Will not of itself satisfy new requirements

Impact on Insurers

An opportunity to

- Sell new forms of cover
- Use education as a marketing tool
- Attract new insureds
- Become first movers

Impact on insurers

- Cyber insurance has been principally concerned with privacy and personal data. New legislation much more complex and concerns all types of online data
- Insurers and their policyholders will need to comply
- Policy wordings will need to change to accommodate changes including
- new security yardstick which will be recognised and enforced by the courts
- Insurers and brokers will need to get their heads round hew risks abd cover
- Policy wordings will need to cover every type of data not just personal data Group companies and ICT service providers will need to be checked and contracts amended
- Compliance will be costly
- Ambulance chasing solicitors will have many more opportunities

Impact on SMEs

- Some New opportunites but.. just as they were beginning to get to grips with GDPR
- New set of complex laws and regulations
- Compliance: training, documentation , bureaucracy
- New fines

ANY QUESTIONS?