CLYDE&CO

Countdown to Dora

The lull before the storm

Nick Gibbons, Legal Director

SUMMARY

- DORA part of a suite of new EU legislation governing cyber security, ICT resilience and artificial intelligence
- Will impact most UK financial institutions and insurers and their insureds
- Unlike GDPR covers all types of data
- Much tougher and more comprehensive security requirements than GDPR, or FCA
- Governs business and ICT service providers
- Cyber Essentials and ISO 27001 certification will not satisfy DORA requirements

BACKGROUND

- Interconnectivity of financial sector and increasing number of cyber attacks
- Prior to DORA 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

Main Provisions

- ICT Risk Management of attack surface and estimation of potential impact of an outage
- Voluntary risk reporting
- Mandatory risk reporting
- Digital Operational Resiliency testing including threat led penetration testing
- Information and intelligence sharing
- Managing ICT third party risk by covered entities
- DORA authorises the European Supervisory authority to establish arrangements with regulators in non EU countries

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

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/DPA ,NIS, FCA and DORA

DORA is complementary to rather than a replacement for existing EU laws governing information security such as:

- GDPR
- the Network and Information Security Directive
- DORA is also part of a raft of new EU legislation to combat cybercrime and create stronger cyber resiliency including the EU AI Act
- Much more rigorous than FCA guidance

GDPR Security : Article 32

Security of processing

Considering the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood ***and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:***

the pseudonymisation and encryption of personal data;

2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

4. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.

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

FCA guidance much weaker

FCA guidance describes customer data as personal data;

Unspecific/un-prescriptive guidance:

- Appropriate systems n place
- Making sure staff understand their obligation
- Good passwords
- Secure back up
- Due diligence on service providers

Cyber essentials and ISO 27001

DORA is more rigorous than:

- Cyber essentials
- ISO27001

Certification will not be sufficient – DORA requires constant vigilance and oversight – many cyber incidents caused by poor internal communication and inadequately maintained/patched systems

Cyber essentials and ISO 27001

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 DORA’s comprehensive requirements

Similar legislation

EU AI Act:

- comprehensive set of rules for providers and users of AI systems, which details transparency and reporting obligations
- expected to *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**.**

Similar Legislation

Network and Information Security (NIS) Directive to be replaced

- 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.

Impact on insurers

- Cyber insurance has been principally concerned with privacy and personal data. New legislation including DORA concerns all types of online data
- Insurers and their poicyholders will need to comply
- Policy wordings will need to change to accommodate a new yardstick which will be recognised andenforced by the courts
- 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
- Board and management must be closely involved

ANY QUESTIONS?