

NIS2 DIRECTIVE

One of several regulations to improve Cyber Resilience in the EU.

OPPORTUNITIES

- To promote more responsibility regarding cybersecurity.
- To promote information sharing in the event of breaches, so that the EU can learn and improve cybersecurity responses.



MAIN POINTS

- Entities are classified as essential and important as we operate in the health sector we are classified as essential.
- Security Controls:
 - » Risk management and information security policies
 - » Incident handling
 - » Business continuity and crisis management
 - » Cryptography and encryption, multi-factor authentication
 - » People, awareness and training



PENALTIES

- For essential entities: administrative fines of up to €10M or at least 2% of the total annual worldwide turnover.
 - » Applied through local laws, e.g. in Germany KRITIS - §8a BSIG

