



# Changing Cyber Regulations: What This Means for Your Company

*Presenters:*

Lynn Parker Dupree

Nicholas Godlove

May 21, 2025

# Your Presenters



## Lynn Parker Dupree is a partner in our DC office

Lynn Parker Dupree, leader of the firm's privacy practice, focuses on privacy compliance, governance, and counseling for clients navigating the dynamic legal and regulatory privacy landscape. Her years of privacy experience provide her with the sharp ability to provide actionable privacy advice and guidance, and a keen understanding of the ways technology can be used to protect individual privacy.





**Contact Lynn:**  
+1 202 408 4462  
[lynn.parkerdupree@finnegan.com](mailto:lynn.parkerdupree@finnegan.com)



## Nick Godlove is the Legal Director for AI and Global Data Privacy at Yum! Brands

Nicholas Godlove is an attorney who specializes in privacy, cybersecurity, and AI applications. He has spoken widely on artificial intelligence, web browser and app privacy, and international data laws before bar associations, trade groups, and other organizations. He has also served on committees for the advancement of the field and taught as an adjunct professor. He currently manages the privacy program for Yum! Brands, which operates KFC, Pizza Hut, Taco Bell, and the Habit Burger Grill.

# Agenda

-  The NIS2 Directive
-  Digital Operational Resilience Act (DORA)
-  HIPAA Security Rule Updates
-  Draft CCPA Regulations

## NIS2 Background

- Replaces the NIS directive adopted in 2016
  - Basis for EU-wide cybersecurity legal requirements
- Key changes
  - Expands the list of sectors subject to cybersecurity obligations.
  - New classification of covered entities: essential entities and important entities.
  - Elaborated risk management measures
  - Incident reporting changes
  - Supervision of entities
  - Coordinated vulnerability disclosure
  - Whois database

# NIS2 Directive – Background

- Applicability
  - Medium and large entities identified in Annex I and II of the Directive
  - Any entity that:
    - provides services by public electronic communications networks, publicly available electronic communications services, trust service providers, or top-level domain name registries and domain name system service providers
    - is the sole provider of a service in a member state that is essential for the maintenance of critical societal or economic activities
    - could have an impact on public safety, security, or health if its services are disrupted
    - could induce a significant systemic risk if disrupted, particularly for sectors that could have a cross-border impact
    - is a critical entity because of its importance at the regional or national level for its sector or type of service
    - is a public administration entity

# NIS2 Directive – Are you in Scope?



Critical service  
with impact on  
public safety  
or economic  
stability



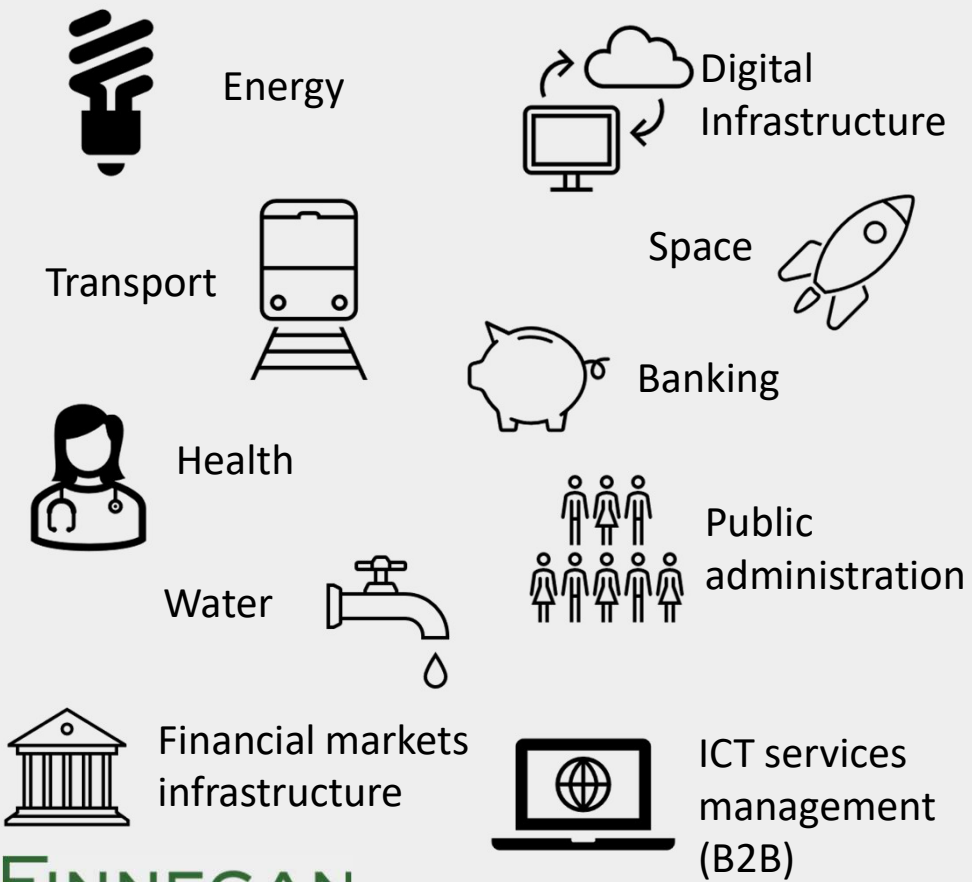
Operating in a  
sector covered  
by the NIS2



Offering  
critical  
services within  
the EU

# NIS2 Directive – Sectors

## Annex I - High criticality sectors



## Annex II - Other critical sectors



# NIS2 Directive – Entities



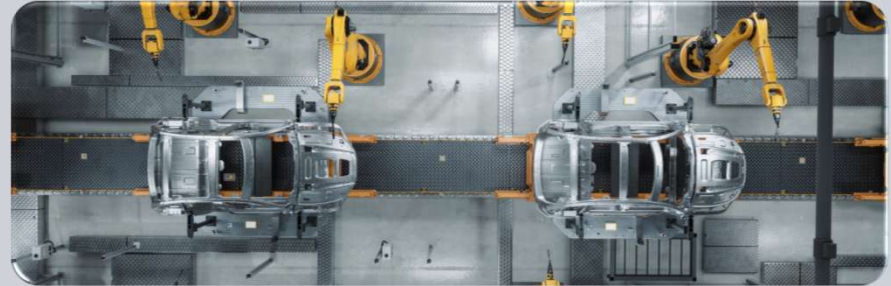
## Essential entities

Highly critical sectors, large enterprises  
(>€50m annual revenue; 250+ employees)

Qualified trust service providers, TLD name registries, DNS service providers

Public administration entities

Operators of essential services



## Important entities

Highly critical sectors, medium enterprises (>€10m annual revenue; 50+ employees)

Other critical sectors, medium & large enterprises



## NIS2 Directive – Risk Management Measures

- Policies on risk analysis and information system security
- Incident handling
- Business continuity and Crisis management
- Supply Chain Security
- Security in systems acquisition, development and maintenance
- Policies to assess the effectiveness of measures
- Basic cyber hygiene practices and training
- Cryptography and encryption
- Human resources security, Access control policies and asset management
- Use of multi-factor authentication and secured communications

# NIS2 Directive – Incident Reporting

**Early warning = within 24 hours of becoming aware of  
SIGNIFICANT INCIDENT**



**Incident notification = within 72 hours of becoming aware**



**An intermediate report on relevant status updates upon the request of the CSIRT**



**Progress report or a final report no later than one month after incident notification**

# NIS2 Directive – Enforcement

## Enforcement

- Fines
  - Essential entities: higher of (i) up to 10 million euros or (ii) 2% of the company's total annual worldwide turnover.
  - Important entities: higher of (i) up to 7 million euros or (ii) 1.4% of the company's total annual worldwide turnover
- Sanctions
  - Suspending certifications and authorizations for services
  - Temporarily banning any individual responsible for the breach from management positions

## EU Digital Operational Resilience Act (DORA)

Governs IT security systems for financial institutions and services and is meant to harmonize rules for financial entities and information and communication technology third party service providers.

Became applicable on January 17, 2025.

## Outlines requirements related to:

- Information and communication technology (ICT) risk management
  - Major incident reporting and voluntary notification of significant cyber threats
  - Reporting of major operational or security payment related incidents
  - Digital operational resilience testing
  - Information and intelligence sharing related to cyber threats and vulnerabilities
  - Contractual requirements for internet and communication service providers and financial entities
  - Oversight framework for critical third-party service providers providing services to financial entities
  - Cooperation among competent authorities and rules on supervision and enforcement

# ICT Risk Management Framework – Digital Operational Resilience Strategy



Requires a comprehensive, well-documented risk management framework, part of which includes a digital operational resilience strategy

- explain how the framework supports the financial entities' business strategy and objectives
- establish risk tolerance level in accordance with the risk appetite of the financial entity and analyze the impact tolerance for disruption
- Establish clear information security objectives that include key performance indicators and key risk metrics
- explain the reference architecture and any changes needed
- outline mechanisms put in place to detect incidents and prevent their impact
- Provide evidence for the current digital operational resilience based on the number of ICT related incidents reported and the effectiveness of the preventative measures
- implement digital operational resilience testing
- establish a communication strategy in the event of an ICT related incident that requires disclosure

# Key Contractual Provisions

- Contracts for the use of ICT services must include:
  - a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider;
  - the locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed;
  - provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data;
  - provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the event of the insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the event of the termination of the contractual arrangements;
  - service level descriptions, including updates and revisions;
  - the obligation of the ICT third-party service provider to provide incident response assistance to the financial entity at no additional cost, or at a cost that is determined ex-ante;
  - the obligation of the ICT third-party service provider to fully cooperate with the competent authorities and the resolution authorities of the financial entity;
  - termination rights and related minimum notice periods for the termination of the contractual arrangements;
  - the conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programmes and digital operational resilience training.

# Key Contractual Provisions

- Provisions for ICT service supporting critical or important functions must include all previous terms, plus:
  - full-service level descriptions
  - notice periods and reporting obligations of the ICT third-party service provider to the financial entity
  - requirements for the ICT third-party service provider to implement and test business contingency plans
  - the obligation of the ICT third-party service provider to participate and fully cooperate in the financial entity's threat led penetration testing
  - the right to monitor, on an ongoing basis, the ICT third-party service provider's performance, which entails the following:
    - unrestricted rights of access, inspection and audit by the financial entity, or an appointed third party, and by the competent authority,
    - the right to agree on alternative assurance levels if other clients' rights are affected;
    - the obligation of the ICT third-party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, financial entity or an appointed third party; and
    - the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits;
  - exit strategies, in particular the establishment of a mandatory adequate transition period:
    - during which the ICT third-party service provider will continue providing the respective functions, or ICT services, with a view to reducing the risk of disruption at the financial entity or to ensure its effective resolution and restructuring;
    - allowing the financial entity to migrate to another ICT third-party service provider or change to in-house solutions consistent with the complexity of the service provided.



# Enforcement and Penalties

- Penalties for critical ICT third-party service providers for failure to comply with oversight requests by the Lead Overseer: periodic penalty payment up to 1% of average daily worldwide turnover of the preceding business year.
- Violations of the Regulation can result in:
  - Cease and desist orders to a legal or natural person regarding conduct that violates the law
  - Requirement to temporarily or permanently cease conduct contrary to the Regulation
  - Adoption of measures, including pecuniary, that incentivize compliance
  - Require the production of data traffic from a telecommunication operator where legally permissible, when there is reasonable suspicion of a violation of the Regulation.
  - Public notices that identify the nature of the violation and the legal or natural person responsible.
- Where Member States impose criminal penalties, authorities may liaise with judicial, prosecuting, or criminal justice authorities.

# HIPAA Security Rule Updates

## Notice of Public Rulemaking to Strengthen Cybersecurity Protections for ePHI

- NPRM released on December 27, 2024
- Comment period ended March 7, 2025
- Rule changes designed to address:
  - Changes in the environment in which health care is provided significant increases in breaches and cyberattacks
  - Common deficiencies observed in investigations into Security Rule compliance
  - Other cybersecurity guidelines, best practices, methodologies, procedures, and processes
  - Court decisions that affect enforcement of the Security Rule

## Notable Technical Requirements

Encryption at Rest and in Transit

Multi-factor authentication

Vulnerability Scans and Penetration Testing Frequency

Network Segmentation

## Notable Impacts to Business Associates

- New requirement for regulated entities to verify that business associates have deployed technical safeguards, and not just addressed them in policies and procedures.
  - Must obtain written verification regarding technical safeguard deployment from business associates once every 12 months.
  - Verification must include a written analysis of the business associate's electronic information systems and include a certification that the analysis was performed and is accurate.
- Compliance: Business associates permitted to continue to operate under existing business associate agreements until the earlier of:
  - the date of contract renewal on or after the compliance date of the final rule; or
  - one year after the effective date of the final rule

# CPPA Draft cybersecurity regulations

Revised draft approved for a second round of public consultation on May 1, 2025

Applicability - business whose processing of personal information presents a significant risk to consumers security, which means the company

- Derives 50% or more of its annual revenue from selling or sharing consumers personal information or
- Meets financial threshold in 1798.140(d)(1)(A) *and* processed the personal information of 250,000 consumers in the preceding calendar year or processed the sensitive personal information 50,000 consumers in the preceding calendar year

# Cybersecurity Audits

Audits must assess how the cyber security program protects personal information, and the establishment, implementation, and maintenance of its program - including the written documentation.

# Program Components to be Assessed

---

Authentication

---

Encryption

---

Account Management and Access Controls

---

Inventory and Management of Personal Information and Information Systems

---

Hardware and Software Configuration

---

Internal and External Vulnerability Scans, Penetration Testing, and Vulnerability Disclosure and Reporting

---

## Components to be Assessed

---

Audit Log Management

---

Network Monitoring and Defenses

---

Antivirus and Anti-Malware Protection

---

Information System Segmentation

---

Limitation and Control on Ports, Services, and Protocols

---

Cybersecurity Awareness



## Components to be Assessed

---

Cybersecurity Education and Training

---

Secure Development and Coding

---

Oversight of External Parties

---

Retention Schedules and Information Disposal

---

Incident Response Management

---

Business Continuity and Disaster Recovery Plans

---



# Audit Report Requirements

Articulate the processes, activities, and components of the program that were assessed and the criteria used for the cyber security audit; evidence examined to make decisions and assessments

Identify the applicable program components and describe how the business implements and enforces compliance; explain the effectiveness of the components

Identify gaps and weaknesses

Remediation plan and time frame for resolution

Identify any corrections or amendments to prior cyber security audits

Responsible individuals - titles of up to three qualified individuals responsible for the cyber security program

Auditor's name, affiliation, and relevant qualifications as well as a statement signed and dated by the highest-ranking auditor certifying an independent review.

Date audit was presented to executives

# FINNEGAN

Questions?

# Your Presenters



## Lynn Parker Dupree is a partner in our DC office

Lynn Parker Dupree, leader of the firm's privacy practice, focuses on privacy compliance, governance, and counseling for clients navigating the dynamic legal and regulatory privacy landscape. Her years of privacy experience provide her with the sharp ability to provide actionable privacy advice and guidance, and a keen understanding of the ways technology can be used to protect individual privacy.

**Contact Lynn:**  
+1 202 408 4462  
[lynn.parkerdupree@finnegan.com](mailto:lynn.parkerdupree@finnegan.com)



## Nick Godlove is the Legal Director for AI and Global Data Privacy at Yum! Brands

Nicholas Godlove is an attorney who specializes in privacy, cybersecurity, and AI applications. He has spoken widely on artificial intelligence, web browser and app privacy, and international data laws before bar associations, trade groups, and other organizations. He has also served on committees for the advancement of the field and taught as an adjunct professor. He currently manages the privacy program for Yum! Brands, which operates KFC, Pizza Hut, Taco Bell, and the Habit Burger Grill.

## Our Disclaimer

These materials have been prepared solely for educational and informational purposes to contribute to the understanding of U.S. intellectual property law. These materials do not constitute legal advice and are not intended to suggest or establish any form of attorney-client relationship with the authors or Finnegan, Henderson, Farabow, Garrett & Dunner, LLP (including Finnegan Europe LLP, and Fei Han Foreign Legal Affairs Law Firm) (“Finnegan”). Rather, these materials reflect only the personal opinions of the authors, and those views are not necessarily appropriate for every situation they refer to or describe. These materials do not reflect the opinions or views of any of the authors’ clients or law firms (including Finnegan) or the opinions or views of any other individual. Specifically, neither Finnegan nor the authors may be bound either philosophically or as representatives of their various present and future clients to the opinions expressed in these materials. While every attempt was made to ensure that these materials are accurate, errors or omissions may be contained therein, for which any liability is disclaimed. All references in this disclaimer to ‘authors’ refer to Finnegan (including Finnegan personnel) and any other authors, presenters, or law firms contributing to these materials.