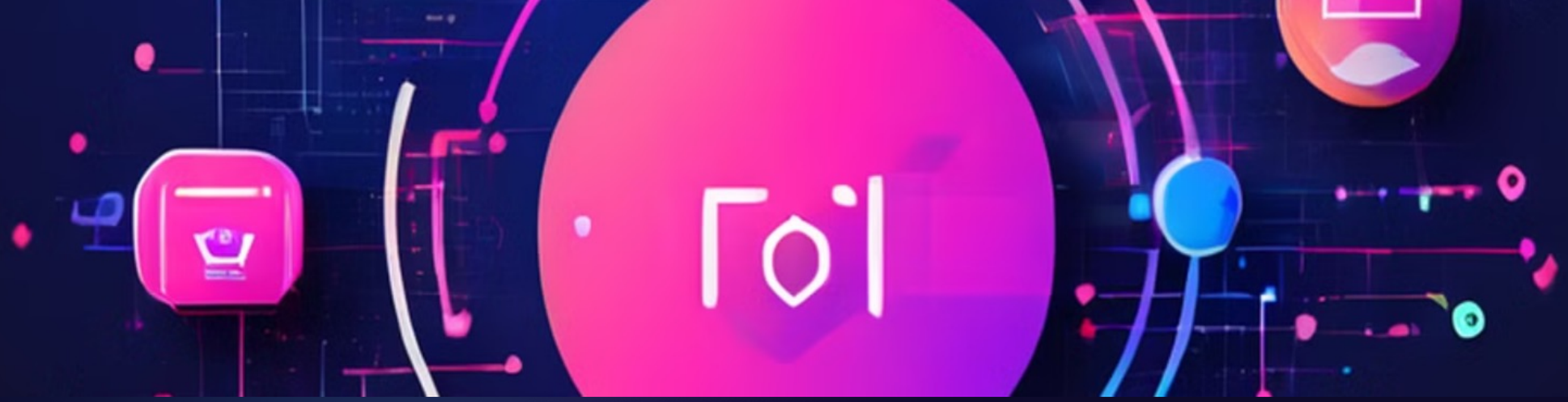
# NIS 2, DORA, and GDPR

An overview of the key EU cybersecurity and data protection regulations businesses must comply with.

**By Ntsapi, Mohamed, Glen & Benoit**



# Understanding NIS 2, DORA, and GDPR

## NIS 2

EU cybersecurity regulation, replacing NIS Directive

## DORA

EU digital operational resilience framework for finance

## GDPR

Comprehensive EU data protection regulation

# NIS 2 Overview

## Enhancing Cybersecurity Measures

NIS 2 aims to improve national cybersecurity capabilities across the EU.

## Fostering Collaboration

The directive promotes EU-wide cooperation to address cyber threats.

## Securing Essential Services

NIS 2 focuses on enhancing the security of vital societal and economic functions.

# NIS 2 Key Differences

## Risk Management

Shift from general assessments to specific threat focus

## Incident Reporting

Stricter timelines and mandatory breach notifications

## Business Continuity

Regularly updated disaster recovery and crisis response plans

## Supply Chain Security

Comprehensive assessments of third-party risks and dependencies

# NIS 2 Transition Action Plan

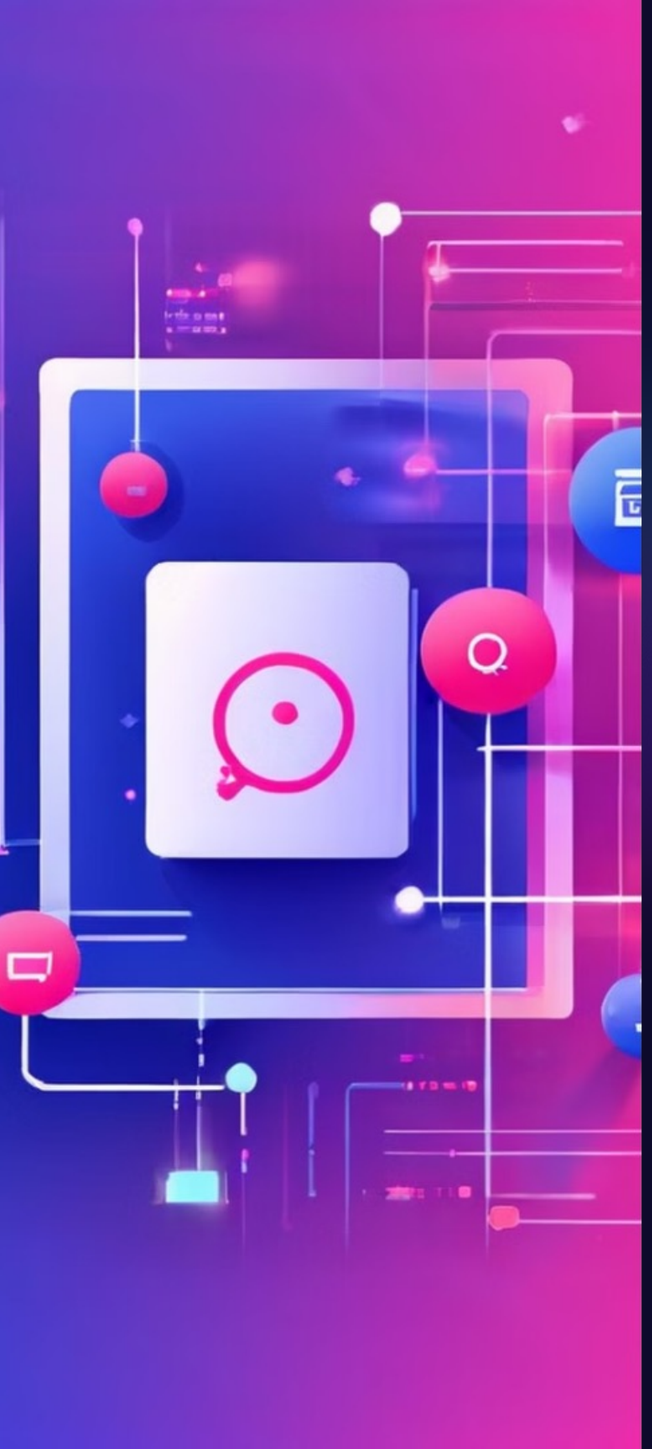
# DORA (Digital Operational Resilience Act)

## Purpose

Ensures resilience of financial entities against cyber threats

## Key Focus Areas

- IT infrastructure management
- Cyber resilience testing
- Incident reporting and response
- Third-party risk assessments



# GDPR (General Data Protection Regulation)

## Purpose

Protect personal data and privacy of EU citizens

## Broad Scope

Applies to any organization processing EU residents' data

## Comprehensive Regulation

Covers data controllers, processors, and cross-border data transfers

# GDPR Key Principles

## Fairness, Transparency

Treat data fairly, be transparent on usage

## Data Minimization

Collect only necessary personal data

## Storage Limitation

Retain data only as long as needed

## Accountability

Demonstrate compliance, respect data subject rights

# GDPR Compliance Action Plan

1

## Identify

Comprehensive data inventory, assess data accuracy

2

## Protect

Implement measures for data integrity, secure consent

3

## Detect

Deploy monitoring tools, conduct regular audits

4

## Respond

Develop breach response plan, train staff on procedures

5

## Recover

Establish recovery processes, review effectiveness of response

To achieve GDPR compliance, organizations must take a comprehensive approach that addresses each stage of the data lifecycle. This action plan outlines the key steps to identify personal data, protect its accuracy and security, detect potential breaches, respond effectively to incidents, and establish robust recovery procedures.

# Questions and Discussion

Addressing your queries and concerns