GRACE
CONNECT

# DPO Forum 2025

*From GDPR to Resilience*
*The Intertwinement of Privacy, Security, and Resilience Risks*

# INTRODUCTION: THE EXPANDING ROLE OF THE DPO

- The **role of DPOs has evolved beyond GDPR compliance**.
- With increasing regulatory convergence (GDPR, NIS 2, DORA), **DPOs** must **align privacy, security, and resilience strategies**

How can **DPOs** actively contribute to risk reduction beyond legal compliance?

GRACE
CONNECT

# WHY PRIVACY, SECURITY & RESILIENCE MUST BE CONNECTED?

**Data protection depends on security**

Without strong cybersecurity, privacy risks increase (e.g., breaches expose sensitive data).

**Regulatory requirements now demand operational resilience**

DORA/NIS 2 require continuity planning for cyber incidents.

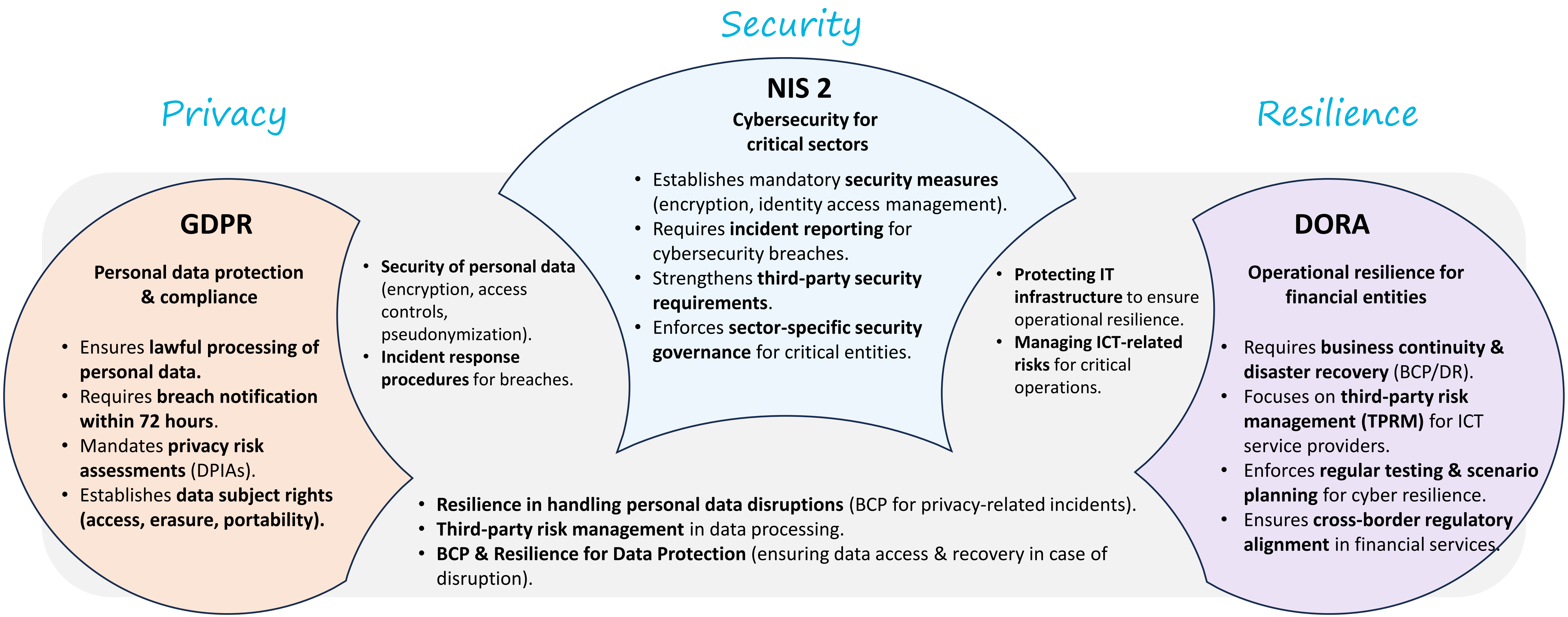
**Privacy, security, and resilience share the same business impact**

Data loss, reputational damage, regulatory fines.

**Control functions (DPO, CISO, BCM, Risk) must work together**

Silos create inefficiencies and gaps.

# REGULATORY FRAMEWORKS



## Security

## Privacy

## Resilience

### NIS 2

**Cybersecurity for critical sectors**

- Establishes mandatory **security measures** (encryption, identity access management).
- Requires **incident reporting** for cybersecurity breaches.
- Strengthens **third-party security requirements**.
- Enforces **sector-specific security governance** for critical entities.

### GDPR

**Personal data protection & compliance**

- Ensures **lawful processing of personal data.**
- Requires **breach notification within 72 hours**.
- Mandates **privacy risk assessments** (DPIAs).
- Establishes **data subject rights (access, erasure, portability).**

- **Security of personal data** (encryption, access controls, pseudonymization).
- **Incident response procedures** for breaches.

- **Protecting IT infrastructure** to ensure operational resilience.
- **Managing ICT-related risks** for critical operations.

### DORA

**Operational resilience for financial entities**

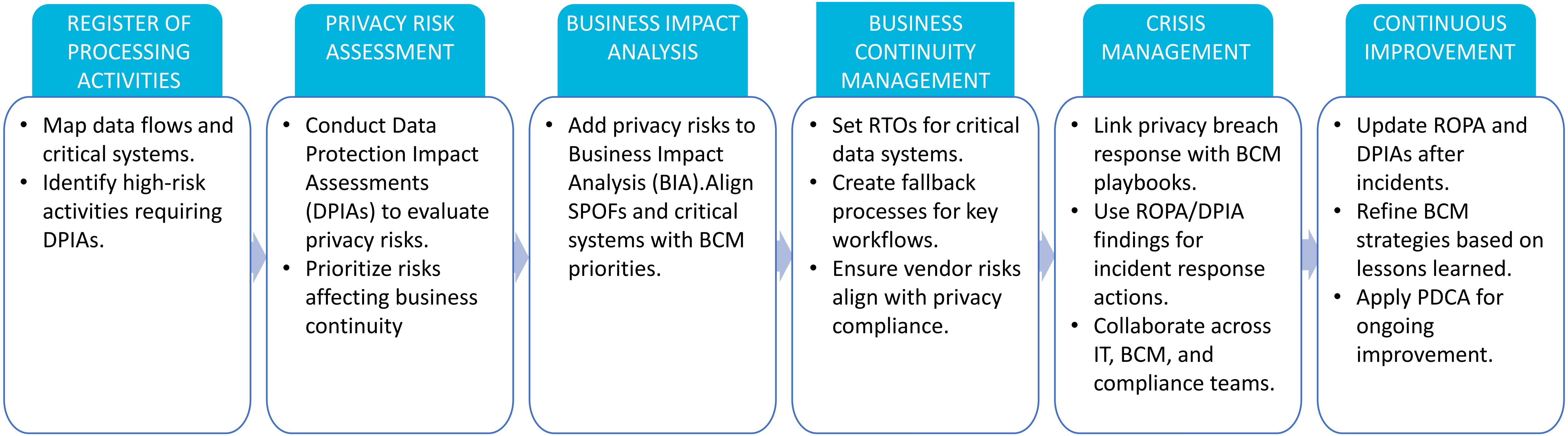
- Requires **business continuity & disaster recovery** (BCP/DR).
- Focuses on **third-party risk management (TPRM)** for ICT service providers.
- Enforces **regular testing & scenario planning** for cyber resilience.
- Ensures **cross-border regulatory alignment** in financial services.

- **Resilience in handling personal data disruptions** (BCP for privacy-related incidents).
- **Third-party risk management** in data processing.
- **BCP & Resilience for Data Protection** (ensuring data access & recovery in case of disruption).

**DPOs, CISOs, and Business Continuity Managers must collaborate** to ensure that privacy, security, and resilience efforts are **aligned rather than siloed**.

# BREAKING SILOS
# ALIGNING DATA PROTECTION WITH BUSINESS RESILIENCE

- DPOs must **integrate privacy risk assessments** into business continuity planning.
- **Third-party risks impact all areas**—A vendor breach can expose personal data **and** disrupt operations.
- **Cyber resilience requires privacy controls & vice versa**—Incident response should cover both **data breaches** and **business continuity failures**.



### REGISTER OF PROCESSING ACTIVITIES

- Map data flows and critical systems.
- Identify high-risk activities requiring DPIAs.

### PRIVACY RISK ASSESSMENT

- Conduct Data Protection Impact Assessments (DPIAs) to evaluate privacy risks.
- Prioritize risks affecting business continuity

### BUSINESS IMPACT ANALYSIS

- Add privacy risks to Business Impact Analysis (BIA).Align SPOFs and critical systems with BCM priorities.

### BUSINESS CONTINUITY MANAGEMENT

- Set RTOs for critical data systems.
- Create fallback processes for key workflows.
- Ensure vendor risks align with privacy compliance.

### CRISIS MANAGEMENT

- Link privacy breach response with BCM playbooks.
- Use ROPA/DPIA findings for incident response actions.
- Collaborate across IT, BCM, and compliance teams.

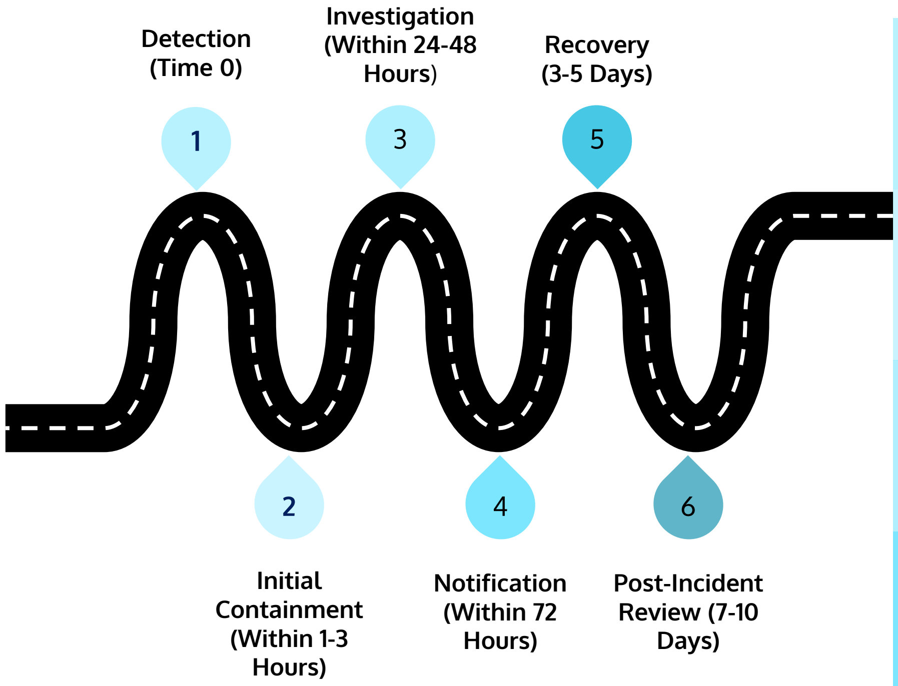
### CONTINUOUS IMPROVEMENT

- Update ROPA and DPIAs after incidents.
- Refine BCM strategies based on lessons learned.
- Apply PDCA for ongoing improvement.

GRACE CONNECT

# Case Study: when a Privacy Breach becomes a Resilience Crisis

- **Incident:** a cloud provider storing and processing customer data suffers a ransomware attack, leading to data exposure **and** business downtime.
- **Regulatory Impact:** GDPR breach notification + DORA mandatory reporting.



1 Detection (Time 0)

2 Initial Containment (Within 1-3 Hours)

3 Investigation (Within 24-48 Hours)

4 Notification (Within 72 Hours)

5 Recovery (3-5 Days)

6 Post-Incident Review (7-10 Days)

Actions

| | SECURITY | PRIVACY | RESILIENCE |
|---|---|---|---|
| **DETECTION** | • Triggered by monitoring systems, intrusion detection, or anomaly alerts.<br>• Security team identifies the incident and classifies its severity | • Initial assessment of personal data involved.<br>• Determine if there is a potential privacy violation (e.g., data breach). | • Activate crisis management plan for operational continuity.<br>• Contain the threat to prevent further disruption. |
| **INITIAL CONTAINMENT** | • Isolate affected systems (e.g., shut down compromised servers).<br>• Implement temporary fixes to halt the breach | • Verify impacted data records and affected data subjects.<br>• Begin drafting data breach notifications if required. | • Ensure business-critical functions continue through alternative workflows.<br>• Update leadership and stakeholders about the operational impact. |
| **INVESTIGATIONS** | • Conduct forensic analysis to identify attack vectors and scope.<br>• Collaborate with IT to ensure no further vulnerabilities exist. | • Confirm compliance with GDPR or other regulatory reporting timelines.<br>• Collect all necessary evidence for regulatory filings. | • Assess damage to operational continuity and prepare recovery strategies.<br>• Coordinate third-party checks if a vendor caused the breach. |
| **NOTIFICATION** | • Deliver a comprehensive report to internal and external stakeholders. | • Submit required notifications to regulatory authorities (e.g., GDPR 72-hour rule).<br>• Notify affected individuals if their data was compromised. | • Execute communication plans to inform customers and partners of any operational impacts. |
| **RECOVERY** | • Patch vulnerabilities and restore system functionality.<br>• Re-evaluate security controls to prevent similar incidents. | • Document lessons learned in privacy policies and risk assessments.<br>• Update the register of processing activities and data protection impact assessments as needed. | • Resume normal business operations and finalize business continuity tasks.<br>• Conduct a review of crisis management effectiveness. |
| **POST INCIDENT REVIEW** | • Analyze root causes and identify areas for improvement. | • Reassess data protection measures based on findings | • Update business continuity plan and incident response playbooks based on lessons learned. |

**Lessons Learned:** organizations need **privacy-aware incident response plans** that align security, compliance, and resilience teams.

# MAIN TAKE AWAYS
# HOW DPOS CAN DRIVE BOTH COMPLIANCE & RESILIENCE

- Embed **privacy risk assessments** into Business Continuity & Cyber Resilience frameworks.
- Ensure **third-party security assessments** also evaluate data protection risks.
- Align **incident response playbooks** between DPOs, CISOs, and BCM leaders.
- Establish **joint training & simulations** for cyber/privacy crises.
- Use **PDCA (Plan-Do-Check-Act)** methodology to **continuously improve resilience strategies**.

*Resilience is more than just recovery.*
*It starts with strong data governance and proactive risk management.*
*Are DPOs ready to lead the next evolution of compliance?*

Download Grace Connect
DPO Check list