PSD2 – eIDAS – NIS

An innovative cybersecurity legal framework

INNOVATION LAW FIRM

Giuseppe Vaciago
g.vaciago@42lf.it
https://www.linkedin.com/in/vaciago/

INTRODUCTION.

PSD2

Payment Service Directive

eIDAS

Electronic Identification, Authentication and trust Services Directive

NIS

Network and Information Security Directive

INTRODUCTION.

What is the common core of the regulatory approach to cybersecurity in Europe?

- 🔎 Risk assessment and security measures
- 🔎 Data protection by design and by default
- 🔎 Notifications, reporting obligations, and mitigation measures (data breaches)
- 🔎 Business Continuity, Disaster Recovery, and Resilience
- 🔎 Certification process
- 🔎 Annual report to the European Authority

MAIN INTERCONNECTION BETWEEN GDPR PSD2 EIDAS AND NIS

Rules and principles	GDPR	PSD2	eIDAS	NIS
Data protection by design and by default **("security by design")**	Recital 78 and Article 25	Recital 89	Art. 12.3 c	
	Organisational measures Adoption of specific security requirements and procedures from the early stages of the development lifecycle Procedures to integrate data protection safeguards into processing activities **Technical measures** Special technologies to support privacy and data protection (PETs) (i.e. tools that encourage data minimisation, anonymisation or limitation of use, amongst other things)	**Technical measures** Secure technologies by design and by default should find solutions to common critical points (connectivity into banks, security fraud and liability, poor user authentication experiences, granting permissions)	**Technical measures** Software development has inspired the use of a catalogue of precise design patterns to develop solutions to known security problems Risk management frameworks and engineering objectives highlight a privacy risk model and three privacy system objectives (on top of the classic security objectives represented by confidentiality, integrity and availability): predictability, manageability and disassociability (US NIST)	N/A

MAIN INTERCONNECTION BETWEEN GDPR PSD2 EIDAS AND NIS

Rules and principles	GDPR	PSD2	eIDAS	NIS
Notifications, reporting obligations, and mitigation measures	Recitals 85, 86, 87 and Articles 33, 34	Recital 89	Recitals 31, 38, 39 and Article 19.2	Article 9. 4, 14.3, 14.4, 16.3 and 16.4
	Organisational measures Procedures to immediately detect whether a personal data breach has taken place Incident response plan **Technical measures** Data flow and log analysers Tokenisation, encryption, etc.	**Organisational measures** Appropriate processes and organisational structures to ensure the consistent and integrated monitoring, handling and follow-up of operational or security incidents Reporting procedures **Technical measures** Early warning indicators that should serve as an alert to enable early detection of operational or security incidents	**Organisational measures** Notification can be of the user or by publishing the required information on the provider's website depending on the nature of the breach, using applications or software to provide a document or fill in a form to notify providers of any incidents	**Organisational measures** Providers and operators must immediately report significant disruptions to the National Agency and the reporting obligations must have no adverse effect on correcting the disruption. **Technical measures** Technologies supporting notification and reporting obligations must: (i) adopt alerting systems; (ii) gather information on incidents; (iii) provide automated completion of notifications using pre-established NIS elements

MAIN INTERCONNECTION BETWEEN GDPR PSD2 EIDAS AND NIS

Rules and principles	GDPR	PSD2	eIDAS	NIS
Business Continuity, Disaster Recovery, and Resilience	Article 32.1.b, 32.1.c	Article 5.1.h	Article 10.3 Article 24.2.h and 24.2.i	Recitals 69, Article 14.2 and Article 16.1.c
	Organisational measures Business continuity plan Data restore procedures Adoption of an effective cyber-resilience approach Disaster recovery plan **Technical measures** Backup techniques Business continuity technologies (e.g. redundancy techniques)	**Organisational measures** Develop response and recovery plans, which should: • Focus on the impact on the operation of critical functions, processes, systems, transactions and interdependencies • Be documented and made available to the business • Be updated in line with lessons learned from the tests, new risks identified and threats and changed recovery objectives and priorities	**Organisational measures** Business impact analysis and a threat analysis Following threat identification, a risk assessment must be performed to determine the impact of the threat on the business, likelihood of occurrence, and recovery time necessary for essential business applications and processes	**Organisational measures** Operators and providers must ensure cyber-resilience, implementing business continuity management measures such as: Cyber risk and vulnerability management Incident response team Alternative resources in the event of crisis Backup systems

MAIN INTERCONNECTION BETWEEN GDPR PSD2 EIDAS AND NIS

Rules and principles	GDPR	PSD2	eIDAS	NIS
Certification Process	Article 43	Article 95.3	Recitals 44 Recital 55	
	Organisational measures Voluntary certifications issued by certification or by the competent Supervisory Authority. Article 48.2 of the Cybersecurity Act, ENISA has set up an Ad Hoc Working Group to support the preparation of a candidate EU cybersecurity certification scheme as a successor to the existing schemes operating under the SOG-IS MRA	**Organisational measures** The Guidelines do not specify the requirements in relation to certification processes, or industry standards such as ISO 27001/22301; as such, no national authority requires such certification processes at present;	**Organisational measures** Assessment of Standards related to eIDAS: ENISA sets out aspects of qualified electronic signature creation devices (QSCD certification) and qualified trust services providers (QTSP supervision) showing how to combine the respective elements in line with the eIDAS requirements **Technical measures** ENISA seeks to support standards CEN EN 419 241-2 and CEN EN 419 221-5:2018 so that they could be referenced in an amended version of CID (EU) 2016/650	. N/A

PSD2 - GOALS & PILLARS.

PILLARS

🔎 The possibility to transfer consumers’ personal data

🔎 Cybersecurity requirements => obligations for the different entities of the payment market environment

ART. 5 - AUTHORIZATION.

Payment institutions should meet specific requirements to be granted an authorization to operate:

- 🔎 **procedures** to monitor, handle and follow up a security incident and security related customer complaints, including an incident reporting mechanism which takes account of the notification obligations of the payment institution laid down in Article 96
- 🔎 **business continuity arrangements** including a clear identification of the critical operations, effective contingency plans and a procedure to regularly test and review the adequacy and efficiency of such plans

CYBERSECURITY TECHNICAL STANDARDS.

🔗 RISK MANAGEMENT

🔗 SECURITY READINESS

🔗 INCIDENT RESPONSE

- 📎 Corporate governance structure;
- 📎 Security and incident policies/toolkits;
- 📎 Arrangements to share information with agencies and industry centers;
- 📎 Third-party vendor contracts and management;
- 📎 Insider threat programs;
- 📎 Employee trainee program.

INCIDENT RESPONSE ACTIVITIES.

In case of cyber incidents and major security emergencies:

- 🔎 conducting internal investigations
- 🔎 engaging with law enforcement and agencies
- 🔎 ensuring compliance with individual notification requirements and government reporting obligations
- 🔎 managing public relations, employee communications and investor relations (aka: reputation)
- 🔎 managing legislative inquires and preparing executives and managers for hearings
- 🔎 handling class actions, enforcement actions and ADR

NOTIFICATION OF INCIDENTS.

TO THE NATIONAL AUTHORITY:

A **major operational or security incident** must be notified, without undue delay, by payment service providers to the competent authority in the home Member State of the payment service provider (Article 96).

TO THE USERS:

If the incident has or may have an **impact on the financial interests** of its payment service users, the provider must inform its payment service users about the incident and the mitigation measures, without undue delay.

eIDAS – GOALS & PILLARS.

Regulation (EU) No 910/2014 (eIDAS Regulation) concerns authentication, signature seals, registered delivery services and time stamps.

MAIN GOAL

🔎 To provide consistency across all EU member states in the way that Document Signing is carried out

INFORM & REMEDY.

If either the electronic identification scheme notified is **breached or partly compromised** in a manner that affects the reliability of the cross-border authentication:

- the notifying Member State shall, without delay, **suspend or revoke that cross-border authentication** or the compromised parts concerned, and shall inform other Member States and the Commission
- when the breach is remedied, the notifying Member State shall **re- establish the cross-border authentication** and shall inform other Member States and the Commission without undue delay
- if the breach is **not remedied within 3 months of the suspension or revocation**, the notifying Member State shall notify other Member States and the Commission the withdrawal of the electronic identification scheme

TECHNICAL AND ORGANIZATIONAL MEASURES.

- 🔍 Qualified and non-qualified trust service providers shall take **appropriate technical and organizational measures** to manage the risks posed to the security of the trust services

- 🔍 Having regard to the latest technological developments, those measures shall ensure that the **level of security is commensurate to the degree of risk**, in order to prevent and minimize the impact of security incidents and inform stakeholders of the adverse effects of incidents

NOTIFICATION DUTIES.

- Qualified and non-qualified trust service providers must, without undue delay but in any event within 24 hours after having become aware of it, **notify the supervisory body**
- **Other relevant bodies** (e.g. the competent national body for information security or the data protection authority) are notified of breaches of security or loss of integrity that has a significant impact on the trust service provider or on personal data
- If the breach of security or loss of integrity is likely to adversely **affect a natural or legal person**, the trust service provider also notifies the natural or legal person without undue delay
- The notified supervisory body must **inform the public or require the trust service provider** to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest

ENISA ROLE.

🔎 If **a breach of security or loss of integrity concerns, two or more Member States** the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA

🔎 Once a year, the supervisory body shall provide ENISA with a **summary of notifications of breach of security and loss of integrity** (i.e. https://youtu.be/ViRIoAimLnA) received from trust service providers.

TAKEAWAYS

STANDARDS

- Appropriate technical and organizational measures to manage risks and the notifications
- Appropriate technical and organizational measures to prevent and respond to incidents

REPORT

- Summary of notification to ENISA
- ...in order to rise and monitor the awareness on specific risks

COOPERATION

- Description of electronic identification procedures in each Member State
- Notifications between authorities,, even international, (ENISA)

TIMING

- Undue delay, 24 hour for breacher, 3 months at least for remediation - in order to avoid possible endemic lack of cybersecurity

NIS DIRECTIVE – SUBJECTS.

Directive (EU) 2016/1148 concerning measures for a high common level of security of Network and Information Systems across the Union applies to

- 🔎 **Essential services sector**, which includes companies and organizations identified as either operators of essential services (OES) or Competent Authorities (CAs)

- 🔎 **Network and information systems** which are all electronic communications, any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data or digital data stored, processed, retrieved or transmitted by elements covered for the purposes of their operation, use, protection and maintenance

GOALS & PURPOSES.

MAIN GOALS

🔎 managing security risk
🔎 protecting against cyber-attack
🔎 detecting cyber security events
🔎 minimizing the impact of cyber security incidents.

NATIONAL STRATEGY.

The national strategy addresses the following **issues**:

- **objectives and priorities** of the national strategy on the security of network and information systems
- a **governance framework** to achieve the objectives and priorities of the security of network and information systems
- **roles and responsibilities of the government bodies** and the other relevant actors
- the identification of **measures** for preparedness, response and recovery, including cooperation between public and private sectors
- indications of the **education**, awareness-raising and training programs relating to the national strategy
- indications of **the research and development plans** relating to the national strategy
- a **risk assessment plan** to identify risks
- a list of **actors involved** in the implementation of the national strategy on the security of network and information systems.

CSIRTs ROLE.

- Computer security incident response teams (CSIRTs) have to be designed by each Member State in order to have adequate resources to effectively carry out its tasks and access to an appropriate, secure, and resilient communication and information infrastructure at national level.

- Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network and they may request the assistance of ENISA in developing national CSIRTs.

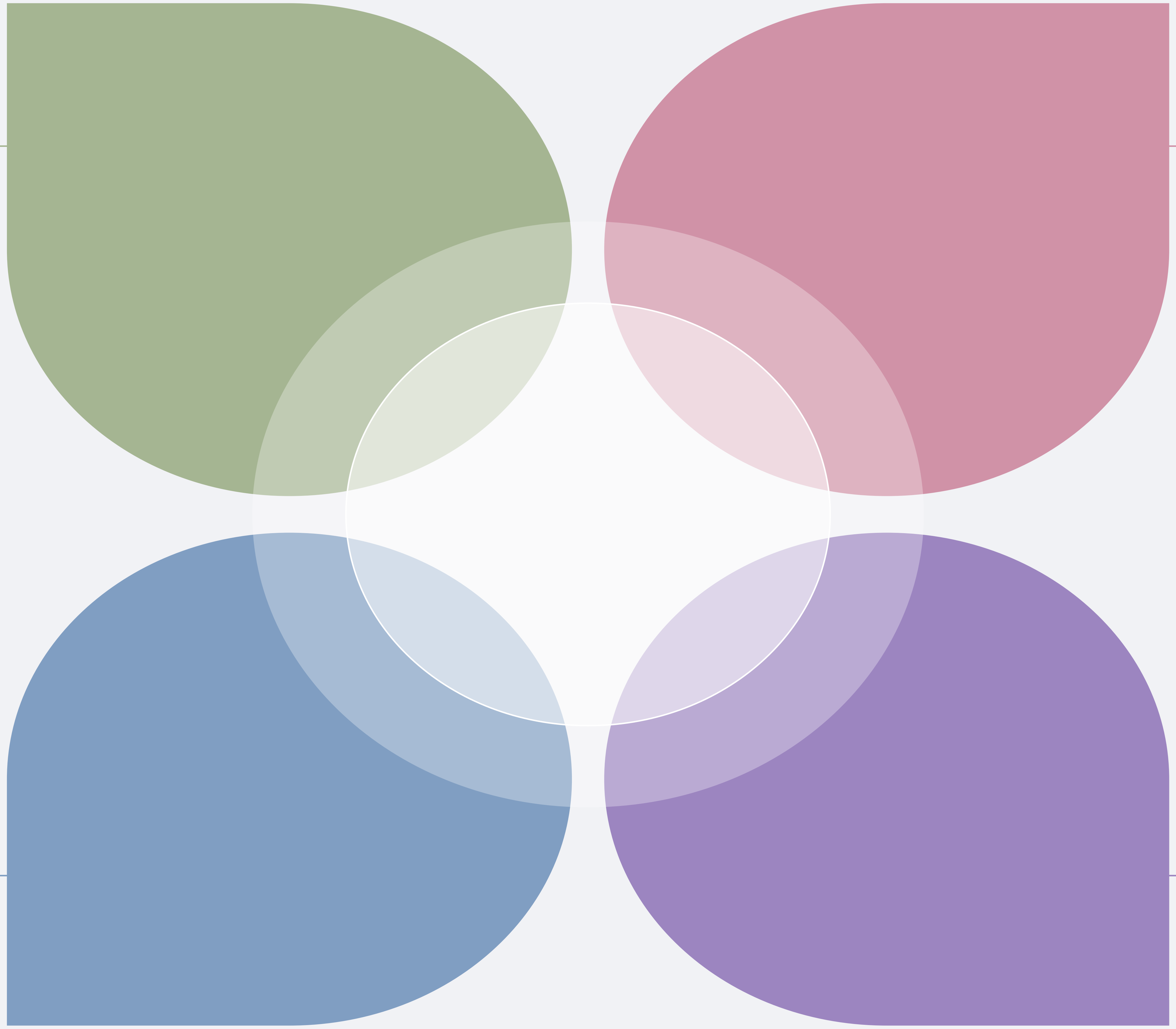
NOTIFICATION OF INCIDENTS
…for Operators of Essential Services.

TO THE COMPETENT AUTHORITY or CSIRT:

Member States must ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide.

- 🔗 Notifications must include infos on determining any **cross-border impact** of the incident, this won’t increase liability
- 🔗 the **criteria** in order to determine the significance of the impact are users, duration and geographical spread.

TAKEAWAYS



STANDARDS

- 🔍 Appropriate technical and organizational measures to manage risks and the notifications
- 🔍 criteria and standards to determine the significance of the impact of incidents

REPORT

- 📌 Notification to the competent authority or CSIRT
- 📌 Infos on determining any cross-border impact of the incident

COOPERATION

- 🔎 CSIRT, Cooperation Group and ENISA
- 🔎 Notifications between authorities, even international

TIMING

- 📌 Undue delay for notification - in order to avoid possible endemic lack of cybersecurity