

(RESEARCH ARTICLE)



A UNIFIED DATA PROTECTION AND PRIVACY ARCHITECTURE FOR CYBER-PHYSICAL SYSTEMS: MANAGING CROSS-DOMAIN, SYSTEMIC, AND CASCADING PRIVACY RISKS IN CONVERGED ENVIRONMENTS

Vladimir Bunic *

Converged Security Institute (CSI), Barcelona, Spain.

* Corresponding Author; Email: vladimir.bunic@convergedsecurity.es

ORCID Details

Vladimir Bunic: <https://orcid.org/0009-0006-6209-629X>

Global Journal of Engineering and Technology Advances, 2026, 29(01), 196–204

Publication history: Received on 29 August 2026; revised on 10 October 2026; accepted on 12 October 2026

Article DOI: <https://doi.org/10.30574/gjeta.2026.29.1.0285>

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

Cyber physical ecosystem combines information technology, operational technology and physical security infrastructures, forming multi personal data flow behind the scenes in a complicated environment. Many traditional privacy frameworks, while suitable for digital aspects, are insufficient for interactions across domains, systemic interactions and cascading disruptions that increase privacy exposure in converged systems. In this study, a Unified Data Protection and Privacy Architecture to deal with privacy risks between a cyber physical space is introduced. Built on four mutually dependent layers, or structural capabilities, to deal with data flows across domains, cross domain coordination of privacy incident response, and compliance with regulatory requirements, they are as follows: Privacy Governance, Operational Privacy, Technology and Cryptographic Controls, and Assurance and Compliance.

The model is aligned with the principles of GDPR, NIS2, DORA, ISO/IEC 27001, ISO/IEC 27701, ISO 31000 and ISO 22301, providing harmonised governance, clear use of the same operational principles across IT, OT and physical entities and interoperable technological controls.

The sector specific implications of the threats faced by critical infrastructure, financial services, industrial environments and public sector organisations are explored.

The findings demonstrate that unified privacy architectures enhance organisational resilience, reduce fragmentation, and support coordinated protection of personal data in cyber-physical systems. The proposed model provides a structural foundation for privacy resilience and offers a pathway for future research on empirical validation and privacy metrics for converged environments.

Keywords: Cyber-Physical Systems; Privacy Architecture; GDPR; NIS2; DORA; Cross-Domain Privacy Risks

1 INTRODUCTION

The Cyber-Physical ecosystems have become highly connected ecosystems that involve information systems, operational technology, and physical security infrastructures working together. This convergence has made privacy exposures deeper and more complex, resulting in crosscutting and multi-layered data flows, and risks that go beyond the traditional digitally-based approach to privacy. Organisations continue to include sensors, automation platforms, identity systems, and physical access technologies in their digital systems, and we have seen a growing amount of personal data migrating from one traditionally distinct system to another. The change raises privacy concerns that plateau through dependent systems and increases the risk for system failures, further making it much harder to remain regulatory compliant. The field of cyber-physical security research underscores the presence of emerging hybrid risks, integrating IT, OT, and physical aspects [1,2]. The risk of privacy exposure grows affects privacy when personal data is being generated or exchanged via sensors, automation platforms, access control and industrial control systems [3].

The characteristics of cyber- physical environments are not necessarily well understood by existing privacy and data protection frameworks such as GDPR [6], ISO/IEC 27701 [10] or ISO/IEC 27001 [9] that may provide strong foundations for the management of digital privacy risks. These frameworks make a number of assumptions, such as predictable data flows, well-defined system boundaries, and systems governance structures within a single domain.

Converged ecosystems, however, present open horizon privacy risks, as they stem from interactions with cross domains, as well as system interdependencies and cascading failures, which can be rooted in physical systems, passed along the operational technology systems and finally reaching digital platforms. Fragmented governance, poor system integrity controls and siloed operations add to these challenges, in turn reducing the impact of privacy protection efforts. There is a pressing need in privacy engineering literature for systems that would support privacy across complex ecosystems, integrating the various perspectives on privacy required for such a task [3-5].

To overcome these constraints, organisations need a common privacy architecture that could help them to seize control of data protection and privacy in cyber-physical spaces. The architecture must have an integrated governance model, operational processes, technology controls and assurance models that, together, create an effect that is in line with the challenges of convergent environments. It should be able to facilitate cross domain data flow management, allow coordinated privacy incident response and reduce systemic and cascading privacy risks. Moreover, it needs to comply with the requirements of GDPR [6] and the principles of NIS2 [7] and DORA [8] ensuring privacy resilience is seen as a capability of the organisation, not a set of activities in various domains.

To fulfil these requirements, this article proposes Unified Data Protection and Privacy Architecture. The model is grounded in four interdependent layers (Privacy Governance, Operational Privacy, Technology and Cryptographic Controls, and Assurance and Compliance) that create a complete model to address privacy risks in cyber-physical systems. The architecture embeds a range of global best practice codes of conduct [9-15] to enable cross-domain coordination, improving the resilience of an organisation to withstand hybrid, systemic and cascading privacy disruption. A series of sector specific implications are explored in regard to critical infrastructure, financial services, industrial organisations and public sector organisations to exemplify that the model has applicability and relevance within various operating contexts.

2 LITERATURE REVIEW

The challenges to privacy posed by cyber-physical ecosystems are different than the traditional digital environment. Recognizing these privacy risks in converged systems has become increasingly apparent in the literature, driven by an understanding that it is these interdependencies, between information technology and operational technology and between physical security and information security, that lead to privacy risks. In this section, the authors review the fundamental research and regulations that lead to the design of a single-architecture privacy system for cyber-physical systems.

2.1 Cyber-Physical Systems and Converged Risk Landscapes

Cyber physical systems (CPS) are integrated systems which combine computational and physical processes, where the digital and physical components exchange information continuously. The new security issues and threats appear in the form of hybrid risks, which are propagated through the different domains and involve both digital assets and physical processes, see for instance the CPS research [1,2]. It is noted in studies that increased privacy exposure occurs with the generation, processing, and transfer of personal information from sensors, automation platforms, access control and Industrial Control System (ICS) technologies [3]. Such environments are interconnected and interdependent, with effects of disruptions spreading systemically from one domain to another, thereby adding to the impact on privacy and increasing the difficulty of mitigation.

2.2 Privacy Engineering and Data Protection Standards

Privacy engineering frameworks offer a tool for incorporating privacy features into the design and working of systems. GDPR sets the basic ground rules for lawful processing, data minimisation, purpose limitation, and accountability, as well as Articles 25 and 32 which highlight the aspect of privacy-by-design and the security of the processing. ISO/IEC 27001 outlines the information security governance and control requirements [9] and ISO/IEC 27701 take those concepts to privacy with recommendations for roles, responsibility and operational controls [10]. The ISO 31000 offers a framework for managing risks, which can be applied to privacy risk assessment [11] and ISO 22301 lays down requirements for continuity to ensure that privacy operations continue during disruptions [12].

Combined, these standards constitute a strong framework but are rather geared towards the digital environment and do not explicitly provide a way to manage privacy risks that cross over domains within cyber-physical systems. This gap is further highlighted in the privacy engineering literature which stresses the need for holistic system-wide approaches based on privacy by design [3-5].

2.3 Regulatory Drivers for Privacy Resilience

Regulatory frameworks in Europe recognise the necessity for integrated privacy and safety measures throughout distributed conditions. The NIS2 Directive strengthens security and incident reporting duties for operators of essential services, with a special focus on cross-domain coordination and resilience [7].

Digital Operational Resilience Act (DORA) sets out a comprehensive framework for ICT risk management, third-party oversight, and operation continuity in the Financial Services industry, with some of these requirements applying directly to the privacy governance. ENISA offers cryptographic guidance for good encryption and key management practices [12], whilst EN 50131, EN 62676, and EN 60839 prescribe interoperability and security for physical security systems that are often working with personal data. Together these regulatory tools make an argument for common privacy architectures that can function within cyber physical spaces.

2.4 Privacy Risk Propagation in Converged Environments

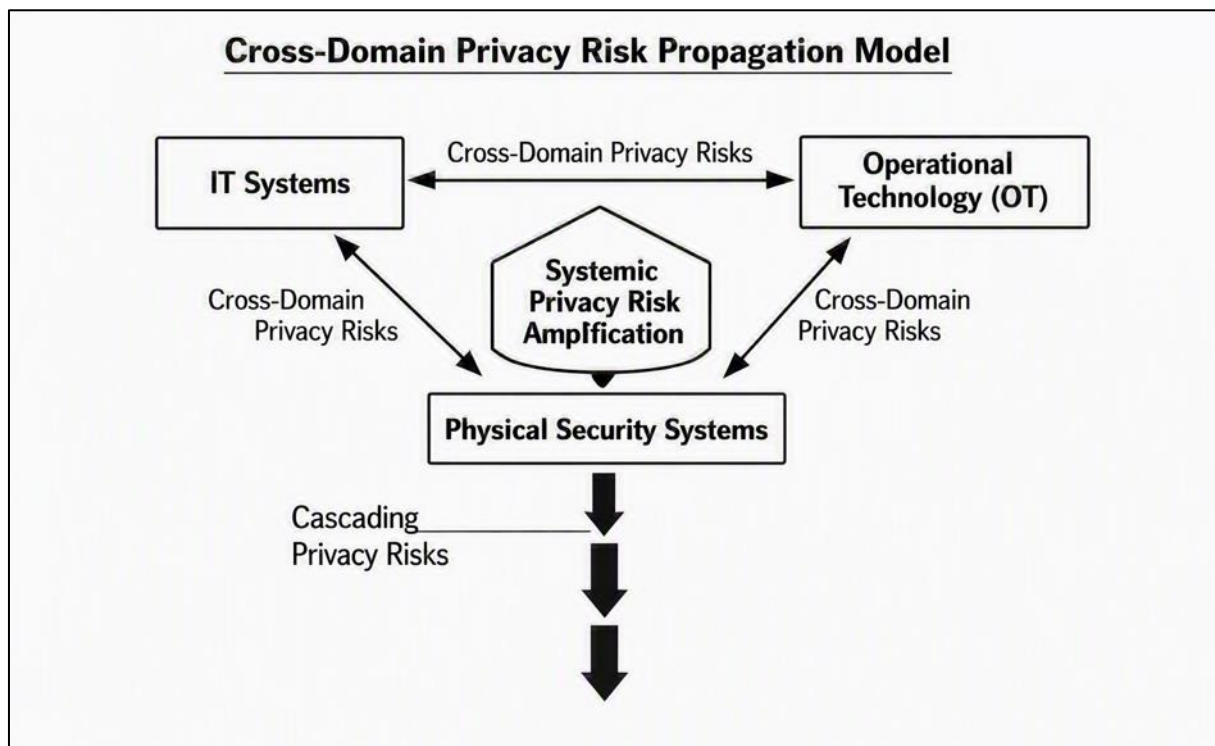


Figure 1: Cross-Domain Privacy Risk Propagation Model

Privacy risks in cyber-physical systems propagate through mechanisms that are different from traditional digital environments. Cross-domain privacy risks become more critical when personal data flows across IT, OT, and physical security systems, creating exposure points that require coordinated protection [1–3]. The process of systemic privacy failures occurs when impact of privacy failures has cascading effects through interconnected systems, via organisational dependencies [2]. Privacy is experiencing cascading threats when the first vulnerabilities lead to further cascading or

sequential vulnerability disclosures across different domains in the system, which can occur due to data aggregation or data correlation processes, or due to data inference allowing sensitive data to be extracted in an unintended way [3-5].

The literature highlights this multidisciplinary approach to governance, the need to provide integrated controls, and shared monitoring mechanisms, which elements are not necessarily captured by current privacy legislation but that would be crucial to being resilient in converged environments.

Table 1: Mapping Privacy Risk Types to Cyber-Physical Domains

Privacy Risk Type	IT Domain	OT Domain	Physical Security Domain	Propagation Characteristics
Cross-Domain Risks	API flows, identity systems	ICS/SCADA telemetry	Access control, CCTV	Bidirectional, triggered by data movement
Systemic Risks	Platform failures	Automation chain failures	Sensor network failures	Amplified through interdependencies
Cascading Risks	Data correlation, inference	Sequential OT disruptions	Physical-digital chain reactions	Sequential, multi-stage propagation

3 METHODOLOGY

The methodology for the development of the Unified Data Protection and Privacy Architecture is structured to guarantee a conceptual rigor, legal compliance with regulations, and integration of the elements in cyber-physical environments.

The method is a combination of comparative standards analysis, architectural synthesis and resilience-oriented validation criteria. This is based on the concept of converged ecosystems that rely on cross-ecosystem data movement and involved by multiple operational domains that demand coordinated operational processes, harmonized governance and consolidated technical controls throughout the data movement.

3.1 Analytical Framework

The analytical framework relies on comparative assessment of the resilience, privacy, security countermeasures in other countries. GDPR introduces general basic legal obligations for personal data processing, such as privacy-by-design (Article 25), security of processing (Article 32) and the need to conduct Privacy Impact Assessments (Article 35) [6]. The information security and information privacy management aspects of governance and information security operational control are relevant in the context of ISO/IEC 27001 and ISO/IEC 27701 [9,10].

All this is supported by several standards, such as ISO 31000 which carries a risk management framework that can be applied to cross-domain privacy risk assessment [11] and ISO 22301 that includes principles for continuity that are critical with regards to privacy operations during disturbances [12] NIS2 and DORA [7,8] bring cross-domain security and operational resilience requirements that impact the privacy governance profile of key industries. Integrated system wide approaches to privacy-by-design are also emphasized in the privacy engineering literature [3-5]. The standards and sources were examined to find gaps that may be cross-domain applicable, and to isolate the requirements that are needed for a general, cross-domain running privacy architecture.

3.2 Architectural Synthesis Approach

The architectural synthesis process demanded mapping requirements for privacy to structural properties of cyber-physical systems. Through this mapping, the requirement for a layered architecture to incorporate assurance, governance, operational processes and technological controls, was identified. The synthesis approach highlighted resiliency to systemic and cascading risks of privacy, cross domain coordination and interoperability. Building blocks that will be used in architectural components were based on known privacy engineering principles [3-5] including regulations [6-8] and cyber physical security research [1,2].

The model that emerges from this process discusses the four distinct layers: Privacy Governance, Operational Privacy, Technology and Cryptographic Controls, as well as Assurance and Compliance, that each address specific needs for privacy risks in converged environments. The architecture was designed in a way that would help ensure consistency across domains, manage data flow in a consistent way and coordinate the way privacy incidents are handled.

3.3 Validation Criteria

Criteria based on regulatory compliance, cross-domain applicability and resilience effectiveness were used for the situation the proposed architecture was validated. To evaluate architecture for regulatory alignment, the GDPR principles along with those outlined in NIS2, DORA, ISO/IEC 27001, ISO/IEC 27701, ISO 31000, and ISO 22301 [6-12] were used. The cross-domain applicability has been covered by evaluating the architecture to support a unified governance, harmonised operation processes, and interoperable technological controls in IT, OT, and physical security domains. The effectiveness of resilience was assessed based on the ability to reduce cross-domain, systemic, and cascading threats to privacy [1–3] and facilitate coordinated response efforts and ensure privacy operations continuity in case of disruptions. For the evaluation of technological controls, the principles of Zero Trust (NIST SP 800-207) [13] and cryptographic guidance provided by ENISA were taken into consideration. These criteria are used to validate the concept of the architecture and its viability for the organisation that operates in a cyber-physical ecosystem.

4 RESULTS: UNIFIED DATA PROTECTION AND PRIVACY ARCHITECTURE

The Unified Data Protection and Privacy Architecture offers a structured model to address privacy risks in cyber-physical environments. It brings governance, operational processes, technology and assurance measures together in one cohesive system that will be able to manage cross-domain, systemic and cascading privacy risks. It's designed to be consistent across IT, OT and physical security scenarios, and harmonised with the protection of personal data as well as the regulatory demands outlined in the GDPR, NIS2 and DORA [6–8].

The layers highlight interdependencies characteristic of converged ecosystems and enable a coordinated approach to privacy management across organisations. The fundamental studies in cyber-physical security and privacy engineering further underscore their importance of interconnected architectures [1–5].

4.1 Overview of the Architecture

The architecture comprises four interdependent layers:

- Privacy Governance Layer
- Operational Privacy Layer
- Technology and Cryptographic Controls Layer
- Assurance and Compliance Layer

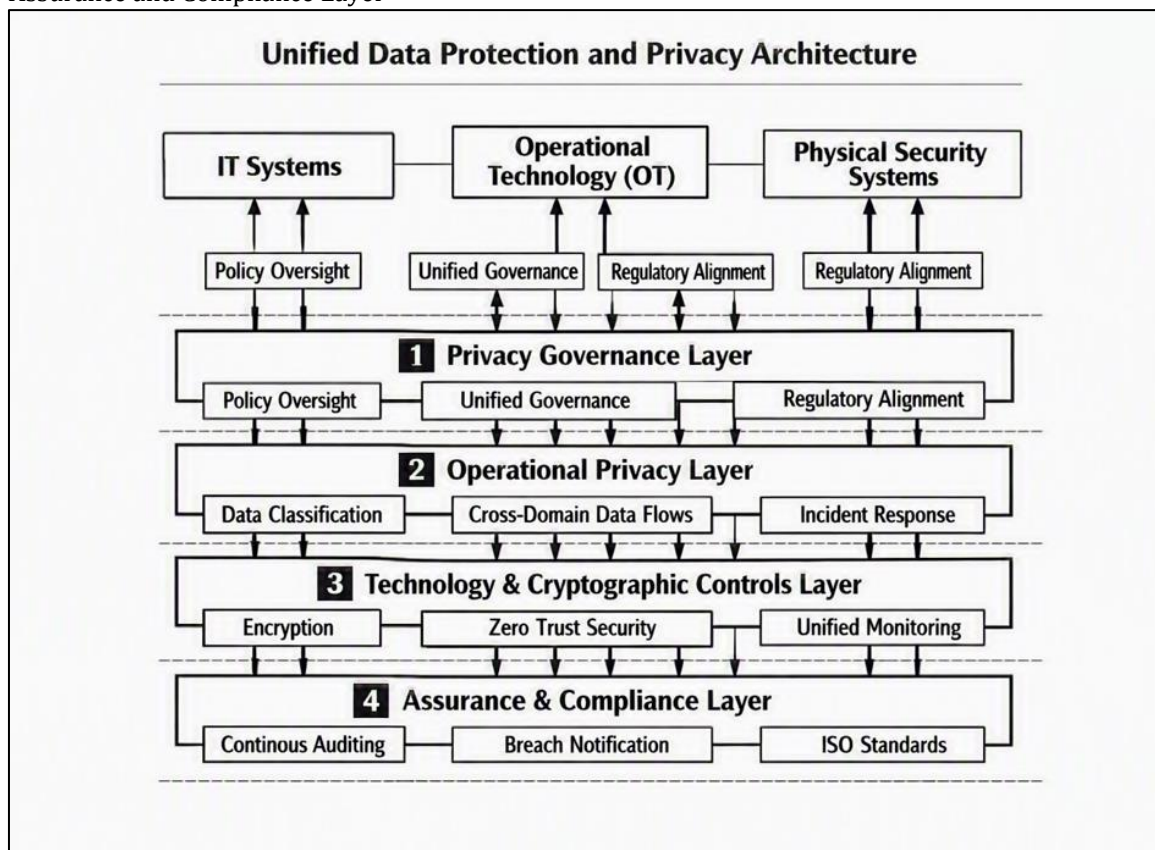


Figure 2: Unified Data Protection and Privacy Architecture (Four-Layer Model)

Table 2: Unified Architecture Layers and Regulatory Alignment

Architecture Layer	Primary Functions	Regulatory Alignment
Privacy Governance	Policies, roles, oversight	GDPR, NIS2, DORA
Operational Privacy	Data flows, DPIAs, incident response	GDPR Art. 25, 32, 35
Technology & Cryptographic Controls	Encryption, monitoring, Zero Trust	ENISA, NIST SP 800-207
Assurance & Compliance	Audits, breach notification, continuity	ISO 27001, 27701, 31000, 22301

While each layer is focused on addressing particular privacy, threat management is in operation across cyber–physical systems, they are taken together to create a cohesive model that enables coordination across multiple domains, regulatory requirements, and organisational resilience. The architecture promotes interoperability, uniform data protection policies, and built-in incident responses, enabling privacy no matter the Hybrid or Systemic challenges. [1–12]

4.2 Privacy Governance Layer

The Privacy Governance Layer provides the framework, policies, and monitoring and supervision capabilities in place to govern privacy in cyber–physical environments. It introduces unified governance principles applicable to IT, OT and physical locations which applies consistently throughout the environment to ensure personal data is processed according to GDPR, ISO/IEC 27001 and ISO/IEC 27701 [6,9,10]. The emphasis of privacy governance literature is to have well-defined roles such as Data Protection Officers with cross-domain authority [5].

To achieve unified governance, there needs to be consistency in data handling policies, uniformity in cross domain data flow protocols, and uniformity in the principles of privacy by design, as set forth in [3–5]. Governance structures should facilitate coordinated decision-making, articulation of escalation processes, and the integration of reporting processes linking to GDPR, NIS2 and DORA [6–8]. It works by making it easy to clarify the requirements for privacy, to provide a consistent environment to work with the domain admin and to establish a unified ownership of the cross-domain privacy issues.

4.3 Operational Privacy Layer

The process and procedure to handle privacy risks in cyber-physical environments. It features the same data classification principles, cross domain data flow management, coordinated privacy incident response and the mandatory Privacy Impact Assessments (PIA) per GDPR Article 35 for activities using cross domain processing or new technologies [6].

It guarantees uniform protection for personal information, no matter the application or field of use. Cross domain data flow management sets the ground rules for the transfer of personal data from the IT-, OT- and physical security space, minimising data fragmentation and ensuring compliance with the GDPR principles of purpose limitation and data minimisation [6]. Privacy incident response processes must be regularized in different domains so that they can be coordinated for detection, escalation, and mitigation of privacy incidents [7,8].

This layer also adds training and simulation exercises that are mapped to the NFPA 1600 and the ISO 22301 standards to ensure everyone across all these domains is familiar with their duties (privacy) and would react appropriately in a privacy incident involving a cross-domain event.

4.4 Technology and Cryptographic Controls Layer

The Technology and Cryptographic Controls Layer delivers the technology behind personal data security for cyber-physical systems. It provides unified monitoring, robust security and encryption capabilities, secure keys management, enforcement of Zero Trust principles and inter-operability with the physical security standards.

Access to encryption is to be based upon AES-256 or EINSTAIN approved equivalents, and key management to be in accordance with FIPS 140-2 and Common Criteria EAL4+ [12]. Unified monitoring correlates the digital and physical telemetry, which allows identifying anomalies when there are possible privacy risks across domains [1–3]. The Zero Trust principles of the NIST Special Publication 800-207 guarantee that access to personal data is continually verified anywhere [13].

Interoperability of physical security systems (including video security, access control, and intrusion detection) can be integrated seamlessly with digital security platforms to use the same procedural and privacy-level security, via

compliance with EN 50131, EN 62676 and EN 60839 [13]. An automated anomaly detection and predictive analytics system further improve the identification of cascading and systemic privacy threats to prevent them from getting worse [2–4].

4.5 Assurance and Compliance Layer

The Assurance and Compliance Layer provides ongoing monitoring and auditability, and regulatory compliance, connecting cyber-physical systems. It provides mechanisms for verifying compliance with GDPR, NIS2, DORA, ISO/IEC 27001, ISO/IEC 27701, ISO 31000, and ISO 22301 [6–12]. This is to benefit the coordinated exercise of data subject rights under Article 15 - Articles 22 of GDPR, where clients can make requests for access to their information, rectification, erasure and portability in a unified manner [6].

A unified process for breaches allows GDPR's 72-hour deadline to report on breaches to be fulfilled and facilitates messaging to affected data subjects and to supervisory authority bodies. In addition to compliance status monitoring, continuous systems monitor compliance within specific domains, and post-incident analysis and improvement cycles ensure that lessons learned from privacy incidents are fed into governance, operational processes, and technology to reduce risks and support continuous improvement. [11,12]

5 DISCUSSION: SECTOR IMPLICATIONS

Unified Data Protection and Privacy Architecture provides the structural solidity for handling privacy risks throughout cyber physical environments. It's relevant in a variety of industries where multi-sector converged systems, cross-domain data movements and privacy regulatory requirements present complex exposure.

The implications of the architecture for critical infrastructure, financial services, industrial and manufacturing environments and public sector organisations are examined. Because the sector-specific characteristics shape different aspects of privacy risk propagation, the analysis offers insights into how resilient resilience is in the face of privacy disruption across different domains, different levels of the system, and different impacts of disruption in the system.

5.1 Critical Infrastructure

Sectors like energy, transportation, water, and healthcare share very interconnected systems, where all three arenas (IT, OT and physical security) are in constant interaction. In these settings, such as access control systems, sensor networks, operational telemetry and digital service platforms, large volume of personal data is produced. [1-3] There are various aspects of cross domains in critical infrastructure systems that can present risks to privacy. Cross domains are the functional and physical interdependencies, disruptions in one domain can impact another domain and vice versa, through which privacy risks can be transmitted [2].

By offering unified governance frameworks and processes consistent with the NIS2 requirements, harmonised operational procedures for the management of cross-site data flows and robust technological controls, encompassing encryption, monitoring and Zero Trust premises, it will provide architecture solutions to guide the implementation of critical infrastructure resilience. Systematically, unified mechanisms for incident responses enable a coordinated detection and mitigation of privacy incidents across domains, minimizing the risk of systemic or cascading privacy failures [6–8] Performing a continuous and comprehensive risk analysis of privacy risks would be an effective pre-emptive measure to minimize such failures. Risks of privacy incidents could be reduced with a continuous and comprehensive risk analysis of privacy risks, done as a pre-emptive measure. Complementing and supporting interoperability with EN physical security standards further enhances privacy protection in cases where physical systems are also integral to data processing.

5.2 Financial Services

The financial services organisations have a high velocity data flow, rich third-party dependency and tight regulatory requirements under GDPR and DORA [6,8] that make up their complex digital ecosystems. Cross- and multi-layered connectivity among ICT systems, automatic decision-making processes, and interactions among digital platforms, branches and operational technologies [3–5] is a source of risks for privacy in this sector. Failure in one financial services system could cascade to another, resulting in disruptions that have a negative effect on customer data, transaction integrity, and regulatory reporting [2]

The architecture contributes to the financial sector's resilience, unified governance in line with DORA's ICT risk management needs, harmonised architecture for managing the cross-domain data flow, and robust technological controls which includes encryption, monitoring, and secure key management [8,13,14].

The coordinating incident response mechanisms are relevant for complying with GDPR's notification obligations of a breach within 72 hours, as well as reporting to the supervisory authorities. This architecture's assurance layer adds accountability and auditability to the intricate nature of financial ecosystems, making privacy resilience a structural organisational capability [11, 12].

5.3 Industrial and Manufacturing Environments

Often, data identifies an employee, client or employee ID number, benefit number or any other personal identifying information, especially in the context of industrial and manufacturing settings which depend on OT, automation platforms, and physical security systems. Common areas of concern regarding privacy risks include interactions between production systems, digital platforms, and work of physical access in cross domains, sensor networks, and vulnerabilities for information technology (IT) and operational technology (OT) systems [1–3]. System failures can happen at any time on OT systems and cascades through digital systems, resulting in systemic privacy failures and revealing personal data [2].

The architectures enable industrial resilience by offering a single governance framework that combines OT privacy with digital privacy practices [9,10], seamless operational procedures for cross-domain data custody, and robust technological safeguards for homogeneous encryption, monitoring, and access control protocols [13,14].

Interoperability with EN physical security standards guarantees harmonized privacy control over physical systems regardless of specification and ensures seamless integration with digital-privacy management platforms [13]. Further benefits of predictive analytics and automated anomaly detection are that they are able to detect cascading and systemic privacy risks before they become too serious of a problem [2–4].

5.4 Public Sector and Emergency Services

The processing of personal data in the public sector or in emergency services is based on multi-domain environments involving the processing of personal data on digital platforms, operational systems and the physical infrastructure. Cross-domain interaction, high volume of data flow, and the demand of real-time information exchange in emergency response activities are common sources of privacy risks in these settings [1–3]. For example, a failure in one system can give rise to cascading failures in other systems, which can jeopardize privacy protections across systems [2].

6 CONCLUSION

Cyber-physical ecosystems have transformed the nature of privacy risk, creating environments where personal data flows across digital platforms, operational technologies, and physical security systems. Traditional privacy frameworks, while comprehensive within digital environments, are not sufficient for converged environments where cross-domain interactions, system interdependencies, and cascading disruptions can intensify privacy impacts. This article presents the Unified Data Protection and Privacy Architecture, which offers a structural solution to these challenges, encompassing governance, operational processes, technological controls and assurance mechanisms in a unified framework that can span IT, OT, and Physical domains.

The four-layered architecture provides a foundation for unified governance aligned with GDPR, NIS2, and DORA, harmonised operational procedures for cross-domain data flow management and incident response, robust technological controls incorporating encryption, monitoring, and Zero Trust principles, and assurance mechanisms that support accountability, auditability, and continuous compliance.

These elements collectively contribute to a comprehensive and flexible approach to privacy resilience, helping organizations tackle the cyber-physical threats they face.

Case studies in key sectors illustrate the architecture's application in critical infrastructure, financial services, industrial and public sector organizations. Each sector presents distinctive privacy challenges arising from cross-domain interactions and demonstrates how the proposed architecture can reduce systemic and cascading disruptions. The architecture echoes the concept that privacy resilience isn't something an organisation chooses to do on an "operational as a preference" basis but rather a structural requirement.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Acknowledgments

The author acknowledges the support of the Converged Security Institute (CSI) of Barcelona (Spain) where the development of this integrated dimension of privacy relies on the commitment to the advancement of cyber physical

resilience research. The author wishes to also thank additional colleagues who provided feedback on the ideas of privacy engineering, cyber physical security and regulatory compliance during the conceptual work on this.

Disclosure of Conflict of Interest

The author declares that there is no conflict of interest regarding the publication of this article.

Statement of Ethical Approval

This study is based on literature review, conceptual analysis, and architectural modelling. It did not involve human participants, animal subjects, clinical trials, or the collection of personal data. Ethical approval was therefore not required.

REFERENCES

- [1] Smith R, Brooks D. Security Science: The Theory and Practice of Security. Butterworth-Heinemann; 2013.
- [2] Kott A, Linkov I. Cyber-Physical Security: Protecting Critical Infrastructure. Springer; 2021.
- [3] Wagner I, Wuyts K. Engineering Privacy: A Practical Guide to Data Protection by Design. Oxford University Press; 2023.
- [4] European Parliament and Council of the European Union. Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88; 2016.
- [5] European Parliament and Council of the European Union. Directive (EU) 2022/2555 of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive). Official Journal of the European Union, L333, 80-152; 2022.
- [6] European Parliament and Council of the European Union. Regulation (EU) 2022/2554 of 14 December 2022 on Digital Operational Resilience for the Financial Sector (Digital Operational Resilience Act, DORA). Official Journal of the European Union, L333, 1-79; 2022.
- [7] ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. International Organization for Standardization, Geneva, Switzerland; 2022.
- [8] ISO/IEC 27701:2019. Security Techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management - Requirements and Guidelines. International Organization for Standardization, Geneva, Switzerland; 2019.
- [9] ISO 31000:2018. Risk Management - Guidelines. International Organization for Standardization, Geneva, Switzerland; 2018.
- [10] ISO 22301:2019. Security and Resilience - Business Continuity Management Systems - Requirements. International Organization for Standardization, Geneva, Switzerland; 2019.
- [11] Rose S, Borchert O, Mitchell S, Connelly S. NIST Special Publication 800-207: Zero Trust Architecture. National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA; 2020.
- [12] European Union Agency for Cybersecurity (ENISA). Good Practices for Security of Personal Data Processing. ENISA, Heraklion, Greece.
- [13] European Committee for Standardization (CEN/CENELEC). EN 50131 (Intrusion and Hold-up Alarm Systems), EN 62676 (Video Surveillance Systems for Use in Security Applications), and EN 60839 (Alarm and Electronic Security Systems). Brussels, Belgium.