CONVERGED SECURITY | RESEARCH COMPANIONS

PUBLIC SAMPLE EDITION

Privacy in Converged Systems

Data Flows, Protective Decisions and Assurance

Prof. Dr. Vladimir Bunic

Global Converged Security Board



Title and publication overview

Privacy in Converged Systems
Data Flows, Protective Decisions and Assurance
Public sample edition | Version 1.0 | 11 November 2026

Author: Prof. Dr. Vladimir Bunic
Owner and distributor: Global Converged Security Board

A secondary practical/reference companion to the primary article identified in the research bibliography, read alongside the issued GCSB standards, mandatory procedures and advisory playbooks.

Eight explanatory readings and three fictional reflection exercises develop questions of evidence, authority and practical judgement. Exact reading crosswalks connect the commentary to issued standards, mandatory procedures and advisory playbooks. This is not a course study guide, a complete training sequence or a research article.

Research method and limits. Conceptual four-layer privacy architecture; the article identifies empirical validation and privacy metrics as future research needs.

Publication chronology. The primary article's registered online publication date is 31 October 2026. The CSF standards cited here were issued 13 October 2026; procedures and playbooks followed on 19 October 2026. This companion was prepared for publication on 11 November 2026. Its crosswalk is a later educational comparison, not evidence that the article used these issued editions.

Copyright and reader information

Copyright © 2026 Global Converged Security Board.
All rights reserved.

Except as permitted by applicable law, reproduction, redistribution or adaptation of this companion requires prior written permission. Source articles retain their separate licences; the companion’s rights notice does not change them.

Applicable law and adopted issued standards govern requirements. Mandatory procedures implement parent requirements; playbooks are advisory. Implementation milestones use the starting event stated by the relevant parent standard. Record organisational adoption and certification commencement separately; the Main Standard uses documented adoption for a new adopter. Article publication, source issue and book publication dates do not start an organisation's implementation period.

All exercises are fictional. Use no personal or confidential workplace data and make no live operational changes. Full worked solutions, complete training scenarios and instructor guidance are excluded.

The companion itself has not been peer reviewed and is not a GCSB Journal article. Source articles retain their original authorship, institutional attribution and licences. No ISBN is assigned. Cover imagery is AI-generated illustration.

Suggested citation. Bunic, V. (2026). Privacy in Converged Systems: Data Flows, Protective Decisions and Assurance. Public sample edition (v1.0). Global Converged Security Board. https://doi.org/10.5281/zenodo.24129173

Contents

Privacy follows the data flow **4**

Interpreting the four-layer model **5**

Purpose, access and retention in connected operations **6**

Privacy incidents and evidence of improvement **7**

The CSF lens: privacy crosses the whole estate **8**

New inferences require a new processing question **9**

Retention is a lifecycle, not a deletion button **10**

Breach coordination without erasing legal roles **11**

Sample exercise 1: A new inference from old records **12**

Sample exercise 2: Deletion in only one system **13**

Sample exercise 3: An outage with uncertain data effects **14**

Research bibliography and evidence **15**

Reading crosswalk: explanations **16**

Reading crosswalk: sample exercises **17**

Issued-source bibliography **18**

Issued-source bibliography (continued) **19**

Privacy follows the data flow

The primary article considers personal-data flows across IT, OT and physical security. A camera, badge reader or location sensor can contribute to a wider information environment even when its procurement owner is outside the IT team.

A data-flow view examines collection, transformation, access, sharing, retention and disposal. Privacy exposure can change when records are combined: information innocuous in one context may become sensitive when linked to identity, location or behaviour.

The organisational purpose of processing matters. Data collected to admit a visitor should not be treated as automatically suitable for unrelated analytics simply because the technical integration is possible.

Original companion example: a facilities dashboard combines visitor entry times with camera events and workforce schedules. The integration may create a new inference about an individual that none of the original systems was designed to make.

Reading bridge. GCSB-GDL-DPP-001, Play 1, Discover and inventory data: include physical and converged sources, purposes, access and retention. No live personal records are needed for this reflection.

Interpreting the four-layer model

The article proposes four connected capabilities: privacy governance, operational privacy, technology and cryptographic controls, and assurance and compliance. They are an analytical architecture, not a substitute for the issued GCSB DPP standard or applicable law.

Governance clarifies responsibility and purpose. Operational privacy concerns how decisions are carried out in ordinary processes. Technical controls constrain access and exposure. Assurance asks whether claims are supported by evidence and whether problems lead to correction.

Technical protection alone cannot justify a processing purpose. Encryption may reduce exposure while leaving excessive collection, inappropriate linkage or unjustified retention untouched. Conversely, a sound policy without operating controls may offer little protection.

Cross-layer questions can reveal gaps. If a retention decision is approved, where is it implemented, who checks it and how are exceptions handled? Each question connects a decision to an observable consequence.

Reading bridge. GCSB-GDL-DPP-001, Play 3, Apply protection controls: verification should cover converged systems, not just conventional databases.

Purpose, access and retention in connected operations

Integration can widen access beyond the original operational need. A shared console should not make all personal records visible to every participant. Access decisions need defined purposes, accountable roles and proportionate evidence.

Retention is an operating decision, not only a schedule. Copies, exports, supplier systems and paper fallbacks can persist after a primary system deletes a record. A credible review examines where the information actually remains.

The article discusses GDPR alongside other security and resilience instruments. They do not confer interchangeable permissions or identical legal duties. Identify the relevant processing activity and jurisdiction, and obtain qualified advice for legal conclusions.

Data minimisation can also improve incident handling by reducing unnecessary exposure in shared records. It should not be misused to destroy evidence that must lawfully be preserved; resolve that tension through the authorised legal and incident decision routes.

Reading bridge. GCSB-GDL-DPP-001, Play 4, Retention, disposal and rights handling. This companion specifies no universal retention period or notification deadline.

Privacy incidents and evidence of improvement

A cyber-physical incident can affect confidentiality, integrity or availability of personal data while also disrupting a site or service. Privacy analysis should connect to incident coordination without assuming that every service outage is a notifiable personal-data breach.

Distinguish observed facts, potential exposure, affected people and unresolved questions. Notification decisions require applicable law, the actual circumstances and authorised judgement; a simplified research model cannot make that decision.

The article frames empirical validation and privacy metrics as future work. Its architectural proposal should therefore not be presented as proof of quantified privacy improvement or guaranteed compliance.

An improvement claim needs a clear comparison and defensible evidence. A reduction in collected records may be relevant, but it cannot alone show that all processing is lawful or that every risk is addressed.

Reading bridge. GCSB-GDL-DPP-001, Play 5, Incidents, review and evidence: retain reasoning and connect observations to programme review. No legal determination or worked response is supplied.

The CSF lens: privacy crosses the whole estate

GCSB-ST-CSF-001 v2.0 integrates cybersecurity, physical security and operational technology security; personal information, identity and personnel concerns cut across them. Privacy is not confined to conventional IT databases or added only after security integration.

Main Standard clause 6.10 connects classification, cross-domain privacy assessment, retention, encryption and data governance. Clauses 2.2-2.4 require lawful scope and jurisdiction-specific applicability. Security integration is not itself a lawful basis for every new use of personal data.

GCSB-PRC-CSF-001 Step 6 connects data controls to technology and identity. GCSB-PRC-DPP-001 Steps 1-2 identify actual processing purposes, recipients, aggregation and dependencies; a device owner and a legal controller are not necessarily the same party.

GCSB-GDL-CSF-001 Play 3 and GCSB-GDL-DPP-001 Play 1 provide advisory practical perspectives. The article's four-layer model is useful commentary, not a replacement for the issued DPP requirements or an article-level peer-review finding.

New inferences require a new processing question

GCSB-ST-CSF-DPP-001 clauses 6.1-6.3 distinguish accountable flows, lawful purposes and privacy impact assessment. Identifiable or inferential information can emerge when otherwise separate camera, access and scheduling records are linked.

GCSB-PRC-DPP-001 Steps 2-4 connect that change to updated flow records, purpose-specific lawful-basis evidence and pre-deployment screening. A DPIA is required when operative law requires it; this companion does not declare every integration automatically high risk.

GCSB-GDL-DPP-001 Plays 1-2 help examine discovery and classification. Pseudonymisation is not automatically anonymisation, and publicly accessible personal information does not cease to be regulated simply because it is visible.

The book's inference exercise asks what changed in purpose, recipients, access and effect on individuals. It gives no lawful-basis ruling. Where a DPO is appointed, independent advice and monitoring remain distinct from the controller's processing decisions and executive resource authority.

Retention is a lifecycle, not a deletion button

GCSB-ST-CSF-DPP-001 clauses 6.4 and 6.6 connect appropriate architecture, recovery safeguards, retention, holds and coordinated disposal. A primary-system deletion does not establish that exports, caches, backups or recipients have been dealt with.

GCSB-PRC-DPP-001 Steps 5 and 7 identify owners, restoration safeguards, hold authority, restricted access, review and disposal verification. A lawful hold needs a defined basis and scope; a generic desire to retain evidence indefinitely is not enough.

GCSB-GDL-DPP-001 Play 4 offers advisory lifecycle questions. The companion's spreadsheet example directs attention to remaining copies and evidence of coordination, rather than a universal retention period or an instruction to destroy records.

Recovery should not silently return erased or restricted information to ordinary processing. The important assurance question is how the organisation carries the original purpose, restrictions and authorised hold decisions through backup and recovery, while preserving information lawfully required as evidence.

Breach coordination without erasing legal roles

GCSB-ST-CSF-DPP-001 clause 6.9 separates security suspicion, legal awareness, personal-data assessment, operational command and notification. Incident type, operational severity and risk to individuals are different questions and should not share an unexplained label.

GCSB-PRC-DPP-001 Step 10 distinguishes controller regulator notification, processor-to-controller reporting and affected-person communication. Internal escalation never postpones applicable statutory duties. The issued source, operative law and authorised advice determine each duty, not this sample exercise.

GCSB-GDL-DPP-001 Play 5 connects incident evidence and review. Clause 6.10 and Procedure Step 11 also distinguish independent assurance from control operation and GCSB recognition; assurance access should be lawful and minimised.

The source article's empirical validation and privacy metrics remain future-work questions. Its complete PDF and publication history were checked for this edition. Its four-layer model is interpreted alongside the issued DPP standard; the publisher's CC BY 4.0 notice conflicts with Crossref's CC BY-SA metadata and is disclosed in the bibliography.

Sample exercise 1: A new inference from old records

Fictional situation. A site proposes combining visitor logs, camera events and staff rosters to predict unusual behaviour. Each system was originally justified for a different purpose.

Reflection prompts. What new data flow or inference is created? Which purpose, access and legal-applicability questions need examination before a decision?

Your output. A fictional data-flow sketch and a question list; use no real personal data.

Further reading. GCSB-GDL-DPP-001, Play 1. No lawful-basis conclusion is provided.

Sample exercise 2: Deletion in only one system

Fictional situation. A controller’s main access-log system deletes old records. A monthly spreadsheet export and supplier backup keep the same information indefinitely.

Reflection prompts. What does the deletion claim establish? Which owners and evidence are needed to assess the remaining copies?

Your output. An assurance question set, not a universal retention schedule.

Further reading. GCSB-GDL-DPP-001, Play 4. No full solution is included.

Sample exercise 3: An outage with uncertain data effects

Fictional situation. A building-access outage interrupts operations. A supplier also reports that visitor-record integrity may have been affected, but the scope is unknown.

Reflection prompts. Separate operational disruption from personal-data questions. What facts are missing, and which authorised decision routes need to be coordinated?

Your output. A statement of known facts and uncertainty; do not make a notification decision.

Further reading. GCSB-GDL-DPP-001, Play 5. No legal ruling or answer key is included.

Research bibliography and evidence

Primary article. Bunic, V. (2026). A UNIFIED DATA PROTECTION AND PRIVACY ARCHITECTURE FOR CYBER-PHYSICAL SYSTEMS: MANAGING CROSS-DOMAIN, SYSTEMIC, AND CASCADING PRIVACY RISKS IN CONVERGED ENVIRONMENTS. Global Journal of Engineering and Technology Advances, 29(1), 196-204. https://doi.org/10.30574/gjeta.2026.29.1.0285

Article history. Received 29 August 2026; revised 10 October 2026; accepted 12 October 2026. Online publication: 31 October 2026 (Crossref published-online field; not DOI creation or deposit date).

Source identity. Vladimir Bunic; Converged Security Institute (CSI), Barcelona, Spain.. Publisher article | Original article PDF. Sources checked 11 November 2026.

Declared journal review policy. Read the publisher policy. Public policy describes the journal’s stated process, not an independent audit of the article’s confidential reports.

Scope of this companion. Conceptual four-layer privacy architecture; the article identifies empirical validation and privacy metrics as future research needs. No quantitative benefit, causal effect or universal compliance outcome is inferred.

Source rights. Publisher page and original PDF state CC BY 4.0. Crossref records CC BY-SA 4.0, a conflicting metadata licence; the discrepancy is disclosed rather than silently reconciled. No original article text, figures or tables are reproduced. New companion commentary retains its separate reserved-rights notice.

Related primary families. DPP, IAM, IRBC, TIA. The following bibliography links the full issued framework; only the indicated families are central to this volume.

Reading crosswalk: explanations

Standards v2.0 set adopted requirements; procedures v1.0 set mandatory steps; playbooks v1.0 offer advisory methods. The following is an interpretive reading crosswalk, not an operational checklist or a new requirement.

Privacy follows the data flow
GCSB-ST-CSF-DPP-001 §6.1 | GCSB-PRC-DPP-001 Step 2 | GCSB-GDL-DPP-001 Play 1
Identify collection, combination and accountable data flows.

Interpreting the four-layer model
GCSB-ST-CSF-DPP-001 §6.3-6.4 | GCSB-PRC-DPP-001 Step 4-5 | GCSB-GDL-DPP-001 Play 3
Connect governance decisions to design and operating controls.

Purpose, access and retention in connected operations
GCSB-ST-CSF-DPP-001 §6.2 and 6.6 | GCSB-PRC-DPP-001 Step 3 and 7 | GCSB-GDL-DPP-001 Play 4
Separate purpose, access, retention and lawful holds.

Privacy incidents and evidence of improvement
GCSB-ST-CSF-DPP-001 §6.9-6.10 | GCSB-PRC-DPP-001 Step 10-11 | GCSB-GDL-DPP-001 Play 5
Coordinate incident evidence while preserving legal roles.

Reading crosswalk: sample exercises

Standards v2.0 set adopted requirements; procedures v1.0 set mandatory steps; playbooks v1.0 offer advisory methods. The following is an interpretive reading crosswalk, not an operational checklist or a new requirement.

Sample exercise 1: A new inference from old records
GCSB-ST-CSF-DPP-001 §6.1-6.3 | GCSB-PRC-DPP-001 Step 2-4 | GCSB-GDL-DPP-001 Play 1
Question new inference without making a lawful-basis finding.

Sample exercise 2: Deletion in only one system
GCSB-ST-CSF-DPP-001 §6.6 | GCSB-PRC-DPP-001 Step 7 | GCSB-GDL-DPP-001 Play 4
Examine remaining copies and disposal verification.

Sample exercise 3: An outage with uncertain data effects
GCSB-ST-CSF-DPP-001 §6.9 | GCSB-PRC-DPP-001 Step 10 | GCSB-GDL-DPP-001 Play 5
Separate operational outage from personal-data breach assessment.

Issued-source bibliography

Primary standards and CCSO Policy: v2.0, issued 13 October 2026. Mandatory procedures and advisory playbooks: v1.0, issued 19 October 2026. Verify the current controlled edition and applicable provisions before use.

GCSB-CSF-STRAT | Converged Security Framework: Strategic Standards for Unified Risk Management and Organisational Resilience
Read issued primary source | GCSB-PRC-STRAT-001 | GCSB-GDL-STRAT-001

GCSB-ST-CSF-001 | Converged Security Framework Main Standard
Read issued primary source | GCSB-PRC-CSF-001 | GCSB-GDL-CSF-001

GCSB-ST-CSF-TRA-001 | Training and Awareness
Read issued primary source | GCSB-PRC-TRA-001 | GCSB-GDL-TRA-001

GCSB-ST-CSF-GLA-001 | Governance and Leadership Framework
Read issued primary source | GCSB-PRC-GLA-001 | GCSB-GDL-GLA-001

GCSB-ST-CSF-TIA-001 | Technology Integration and Architecture
Read issued primary source | GCSB-PRC-TIA-001 | GCSB-GDL-TIA-001

Issued-source bibliography (continued)

Primary standards and CCSO Policy: v2.0, issued 13 October 2026. Mandatory procedures and advisory playbooks: v1.0, issued 19 October 2026. Verify the current controlled edition and applicable provisions before use.

GCSB-ST-CSF-IRBC-001 | Incident Response and Business Continuity Framework
Read issued primary source | GCSB-PRC-IRBC-001 | GCSB-GDL-IRBC-001

GCSB-ST-CSF-IAM-001 | Identity and Access Management Standard
Read issued primary source | GCSB-PRC-IAM-001 | GCSB-GDL-IAM-001

GCSB-ST-CSF-DPP-001 | Data Protection and Privacy Standard
Read issued primary source | GCSB-PRC-DPP-001 | GCSB-GDL-DPP-001

GCSB-ST-CSF-RMA-001 | Converged Security Risk Management and Assessment Standard
Read issued primary source | GCSB-PRC-RMA-001 | GCSB-GDL-RMA-001

GCSB-POL-CSF-CCSO-001 | Chief Converged Security Officer (CCSO) Policy
Read issued primary source | GCSB-PRC-CCSO-001 | GCSB-GDL-CCSO-001

RESEARCH COMPANIONS | PUBLIC SAMPLE

Privacy in Converged Systems

Data Flows, Protective Decisions and Assurance

From research ideas to better questions: eight explanatory readings, three fictional exercises and exact issued-source crosswalks. A separate educational companion, not a standard or peer-reviewed research article.

Prof. Dr. Vladimir Bunic
Global Converged Security Board
Owner and distributor | All rights reserved