

Data Protection and Privacy Standard

Version 2.0 · Issued 13 October 2026 · Global Converged Security Board (GCSB)

Document control

Field	Value
Identifier	GCSB-ST-CSF-DPP-001
Title	Data Protection and Privacy Standard
Document type	Standard
Version	2.0
Status	Issued
Issue date	13 October 2026
Effective date	13 October 2026
Next scheduled review	13 October 2027
Issuer	Global Converged Security Board (GCSB)

Author	Prof. Dr. Vladimir Bunic
Owners	Prof. Dr. Vladimir Bunic and Global Converged Security Board (GCSB)
Reviewed by	Certification and Standards Committee
Approved by	Governing Council; approved for issue by Prof. Dr. Vladimir Bunic, President & Chair, 13 October 2026
Classification	General Use
Registered office	GCSB UK, Office 10595, 321-323 High Road, Chadwell Heath, Essex, RM6 6AX, United Kingdom
Published at	https://gcsb.uk/standards/csf-dpp-001-data-protection

Contents

- 1. Foreword, status and intended use
- 2. Purpose, scope and applicability
- 3. Normative references and related documents
- 4. Terms and abbreviations
- 5. Roles, responsibilities and governance
- 6. Numbered data protection requirements
- 7. Implementation and transition
- 8. Evidence, monitoring and corrective action
- 9. Exceptions, escalation and review
- 10. Document control and revision history

I. Foreword, status and intended use

I.1 Intended use

This standard addresses lawful and accountable personal data processing across cybersecurity, physical security and operational technology (OT) within an adopter's documented scope. It links privacy governance, inventories, classification, impact assessment, architecture, rights, retention, suppliers, incident response and assurance to the Main Standard (GCSB-ST-CSF-001) and companion standards.

I.2 Issuer and adopter

GCSB issues standards and makes recognition decisions through separately authorised arrangements. The adopter implements controls through its governing body, controller or processor responsibilities, Chief Converged Security Officer (CCSO), business and domain owners and independent privacy advice.

GCSB is not represented as a training, consulting or audit provider. Adoption does not itself confer a qualification, Trustmark Award, accreditation, regulatory approval, ISO certification or product certification. Independent assessment access must be lawful and minimised, not a right to all personal data.

1.3 Drafting convention

"Shall" denotes a requirement, "should" a recommendation, "may" a permission and "can" a capability. This standard sets out outcome-based protection, DPO independence, proportionate architecture, corrected rights timing and role-specific breach handling.

2. Purpose, scope and applicability

2.1 Purpose

The purpose is demonstrable protection of individuals, lawful cross-domain processing and resilient controls with accountable decisions. Expected benefits are intended outcomes, not guarantees of full compliance, eliminated risk, regulatory recognition or commercial advantage.

2.2 Scope

The adopter shall document entities, purposes, processing activities, personal data, individuals, locations, systems, recipients, suppliers, flows and dependencies. Cyber, physical and OT processing shall be covered where present; an absent domain shall be explained, not invented. Non-personal operational data shall be distinguished from identifiable or inferential personal data.

Subsidiaries, joint ventures and partners shall be scoped by actual control, processing roles and lawful arrangements. Access to another entity's systems does not automatically grant control over that entity. Training, platform capability and adopter processing shall be distinguished from GCSB recognition and administration.

2.3 Binding obligations and precedence

The adopter shall maintain an applicability register by jurisdiction, entity, sector and activity. UK GDPR, the Data Protection Act 2018 and applicable amendments, EU GDPR and member-state provisions, PECR, NIS2 implementing measures, DORA and relevant other applicable laws are distinct. Law applies by virtue of its own scope, not because an internal framework table marks it as applicable.

Binding law takes priority over internal controls; lawful contractual and scheme duties shall be identified separately. Applicable legal duties shall be met from their binding dates, notwithstanding any internal transition, exception or consultation period adopted under this standard. The adopter shall address the 5 February 2026 commencement of UK data-subject rights timing and automated-decision reforms where applicable to it. No EU rule is assumed identical to the corresponding UK rule.

3. Normative references and related documents

3.1 Related documents and references

Reference	Role
-----------	------

GCSB-ST-CSF-001 and GCSB-CSF-STRAT	Scope, baseline and strategy
GCSB-ST-CSF-GLA-001	Adopter oversight, delegation and reporting
GCSB-ST-CSF-RMA-001 and GCSB-ST-CSF-TIA-001	Privacy risk, architecture, coverage and recovery interfaces
GCSB-ST-CSF-IAM-001	Identity, access, biometrics, privacy, retention and recovery
GCSB-ST-CSF-IRBC-001, GCSB-ST-CSF-TRA-001 and GCSB-POL-CSF-CCSO-001	Response, competence and executive responsibilities
Associated guidance, where issued by GCSB	Terminology and implementation support material
UK and EU GDPR and applicable domestic data protection law	Binding duties within their legal scope
ISO/IEC 27001; Common Criteria; FIPS 140; NIST SP 800-88	Management, evaluation, cryptographic modules and sanitisation
TLS, IPsec, OAuth and relevant API specifications	Transport and integration mechanisms

3.2 Reference integrity

The adopter shall identify the current edition, specific provisions, normative or informative status and availability of each reference it relies on. GDPR Article 30 is a recordkeeping duty, not an interoperability protocol. ISO/IEC 27001 is not a cryptographic algorithm certification; Common Criteria evaluation assurance levels and FIPS module levels do not establish equivalent protection automatically. No cited document alone certifies the adopter.

4. Terms and abbreviations

Term	Meaning
Personal data / processing	As defined by applicable law; identifiability includes relevant indirect identification
Controller / processor / joint controllers	Determined by actual purposes-and-means, instructions, or joint determination, not by labels chosen to avoid duties
DPO	Statutory data protection officer where appointed under applicable law, providing independent advice and monitoring
Privacy executive	An operational privacy role, distinct from an independent DPO; this standard implies no GCSB appointment
CCSO	Chief Converged Security Officer or equivalent cross-domain executive under the Main Standard
PIA / DPIA	Internal privacy assessment / legally required data protection impact assessment; overlapping but not identical processes

Special-category data	The legal categories defined under applicable law, not synonymous with all internally "Restricted" data
Classification	Internal handling sensitivity; a "Public" label never removes personal-data duties
Personal data breach	A security breach affecting confidentiality, integrity or availability of personal data under applicable law
Risk / high risk	Risk to individuals' rights and freedoms for legal notification purposes, distinct from organisational incident severity
Hybrid / systemic / cascading	Risk or incident types, not automatically severity or notification categories
Retention / legal hold / disposal	Purpose- and law-based keeping / a bounded preservation obligation / verified deletion or sanitisation
Pseudonymisation / anonymisation	Re-identification controlled but possible / identifiability removed under a substantiated assessment; not interchangeable
Coverage / availability	Accepted integrations over defined eligible systems / service accessibility during a defined period
Exception	An authorised internal deviation within lawful bounds, never a statutory exemption or automatic recognition

5. Roles, responsibilities and governance

5.1 Issuer governance

Development and review of this standard sits with the Certification and Standards Committee. Institutional approval sits with the Governing Council. Recognition, concessions and appeals are administered through the relevant GCSB arrangements referenced in this standard.

5.2 Adopter and independent privacy advice

The controller or processor shall retain its actual legal obligations. The governing body and responsible executives shall approve processing and resources through documented delegation; the CCSO shall coordinate converged security controls and response. Domain owners implement controls and supply evidence. Legal, HR, safety and business owners retain their competent duties.

A data governance body shall coordinate policy consistency and report to the responsible executive and governing body.

A DPO, where appointed, shall advise and monitor independently, have timely involvement, appropriate access and resources, direct access to the highest management level and freedom from incompatible operational decisions. Controller decision accountability shall not be transferred to the DPO. Independent advice and challenge do not prevent urgent lawful action by authorised responders.

5.3 Changes and escalation

Approval, consultation, implementation, independent advice and escalation shall be distinguished. No veto or administrative delay may prevent legally required protection, and DPO independence shall not be displaced by voting or operational authority.

6. Numbered data protection requirements

6.1 Inventory, classification and accountable flows

6.1.1 The adopter shall maintain processing inventories and accountable data-flow maps covering collection, use, recipients, storage, aggregation, transfer, recovery and disposal across scoped domains. Processing records shall reflect actual controller/processor duties and be updated to reflect material changes.

6.1.2 Classification shall support consistent handling outcomes and preserve labels during transfer. Public personal data remains regulated; special-category status shall be separately identified, including applicable criminal-offence rules where relevant. The same classification label does not require technically identical controls across paper, physical, cyber and OT environments.

6.2 Lawfulness, transparency and purpose

6.2.1 The adopter shall record applicable lawful bases by purpose and activity, together with transparency, necessity, minimisation and accuracy measures. The same data may be processed for different purposes under different lawful bases. An Article 9 condition, where required, is additional to the Article 6 basis, not its substitute.

6.2.2 Consent, where relied upon, shall be valid, evidenced, understandable and withdrawable without unnecessary friction. Withdrawal does not permit retrospectively inventing another basis to continue the same processing. Legitimate interests require an appropriate assessment and applicable objection handling, not a generic waiver of rights.

6.2.3 Biometric and monitoring deployments shall address actual purpose, lawful basis, special-category conditions when applicable, worker rights, access, proportionality and alternatives. Profiling and significant automated decisions require the operative jurisdiction-specific rules and safeguards.

6.3 Privacy impact assessment and design

6.3.1 Changes shall receive documented privacy screening before deployment. Where law requires a DPIA, the controller shall complete it, seek DPO advice where applicable and address prior consultation where residual legal high risk requires it.

6.3.2 Assessment shall address purposes, flows, aggregation and inference, necessity, proportionality, individual risks, mitigation, responsibility and rights. Competent security, physical, OT, safety, business, privacy and legal input shall be obtained as relevant.

6.3.3 Design and defaults shall minimise collection, access, sharing and retention. Pseudonymisation, masking and non-production controls shall preserve protection; pseudonymised data shall not automatically be treated as anonymous.

6.4 Architecture, encryption and keys

6.4.1 Architecture shall implement appropriate security, segregation, least privilege, authenticated interfaces, resilience and key lifecycle controls that are proportionate and vendor-neutral.

6.4.2 Cryptographic controls shall state purpose, profile, supported protocols, keys, owners, access, rotation, compromise response, escrow restrictions and sanitisation evidence. The adopter shall use current, valid cryptographic and sanitisation profiles and shall review them regularly, taking account of the transition of FIPS 140-2 validations to historical status and of NIST SP 800-88 Rev. 2. Changing an edition alone does not prove equivalent assurance.

6.4.3 Backup and recovery shall protect personal data and keys, address business impact and safety, and prevent erased or restricted data being silently restored into active processing. Encryption translation, centralisation and recovery escrow shall not expose all domains to uncontrolled shared compromise.

6.5 Monitoring, DLP and analytics

6.5.1 Monitoring shall be justified, transparent where required, minimised, access-restricted and testable. Logs shall not indiscriminately collect credentials, tokens or unrelated personal content.

6.5.2 Blocking and quarantine shall follow authorised rules, evidence and escalation, with OT safety, physical egress, critical-service continuity and safe fallback addressed. Automated action shall not authorise unsafe disconnection or suspension of legally required processing.

6.5.3 Analytics shall validate utility, limitations, error rates, drift, access and human authority; no universal prediction or legal-compliance guarantee is implied.

6.6 Retention, holds and disposal

6.6.1 Retention shall be set by actual purpose, category, law, necessity and evidence, with owners and periodic review.

6.6.2 Holds shall identify authority, scope, necessity, restricted access, review and expiry. DPO advice shall not replace controller or legal-owner accountability. Legitimate interests shall not be treated as an unlimited override of erasure or storage limitation.

6.6.3 Disposal shall coordinate active copies, recipients, caches, logs, archives and backups, with verification and restoration safeguards. Where operative law or guidance permits backup lifecycle arrangements, data shall be kept beyond use only with appropriate access restrictions and scheduled erasure; no blanket postponement or indefinite retention is authorised. Evidence of deletion shall itself be minimised and retained lawfully.

6.7 Individual rights and communications

6.7.1 The adopter shall provide a coordinated, accessible rights channel without requiring separate domain requests. Rights shall be assessed under applicable jurisdiction, conditions, exceptions and safeguards.

6.7.2 Timing shall follow operative law, with recorded receipt, identity verification, permitted information or clarification steps, any legal pauses, extensions and notices. Under EU GDPR the ordinary response period runs from receipt, with a necessary extension within the period set by applicable EU and Member State law. Under UK law, section 76 of the Data (Use and Access) Act 2025 inserts Article 12A: one month from the relevant time (the latest of receipt, permitted identity information and any permitted fee), with a necessary extension by two further months and notice within the first month, and a permitted Article 15 clarification pause where reasonably required. These UK provisions commenced on 5 February 2026 under S.I. 2026/82, subject to transitional savings.

6.7.3 Identity checks shall be necessary and proportionate. Portability shall distinguish entitlement to a structured, commonly used machine-readable copy from technically feasible direct controller-to-controller transmission. Rectification, objection and restriction shall address applicable tests and recipient communication, not a blanket entitlement or exclusion.

6.8 Suppliers and international transfers

6.8.1 Processors shall receive applicable written processing terms, instructions, confidentiality, security, subprocessor, assistance, audit evidence, incident and end-of-service obligations. Joint controllers and independent controllers shall have their own appropriate arrangements, not automatically processor terms.

6.8.2 Controller choice of return or deletion, applicable legal storage requirements, backup safeguards and processor cooperation shall be scoped under operative law. Supplier verification must not expose unrestricted unrelated personal data.

6.8.3 Transfers shall be identified by actual exporting regime, recipient, access, location and mechanism. UK and EU adequacy, the International Data Transfer Agreement and Addendum, standard contractual clauses, binding corporate rules and limited derogations shall not be treated as identical or universally available. Destination-specific assessment and supplementary measures shall be used where required.

6.8.4 Use of a data transfer framework is not evidence of GCSB participation, recipient certification or actual lawful transfer. Current framework status and eligible recipients shall be verified at the time of use; ordinary intra-EEA flows are not automatically third-country transfers.

6.9 Incidents, notification and recovery

6.9.1 Response shall distinguish security suspicion or detection, actual legal awareness, personal-data breach assessment, internal command and statutory notifications. Internal deadlines shall not postpone legal notifications.

6.9.2 An authorised operational incident lead shall coordinate domain response and continuity with privacy and legal advice. Hybrid, systemic and cascading incident types, operational severity, and individual risk or high risk are different classifications.

6.9.3 Under applicable GDPR provisions, controller regulator notice is without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to result in risk; processors notify controllers without undue delay. High-risk affected-person communication is without undue delay, subject to legal conditions. Notifications shall include required information, contact, assessment and supplementary details.

6.9.4 Disproportionate effort is not automatic silence: applicable law requires public or similarly effective communication instead. Encryption exceptions depend on whether actual protection renders the data unintelligible; encryption alone never proves that condition. Recovery and testing shall align with the Incident Response and Business Continuity, Risk Management and Identity and Access Management standards.

6.10 Competence, records and assurance

6.10.1 Personnel competence shall cover role-relevant law, classification, rights, handling, incidents, technology and privacy risks, with initial and refresher training appropriate to role.

- 6.10.2 Evidence shall cover applicability, flows, lawful bases, transparency, impact assessment, architecture, access, monitoring, rights, retention, suppliers, transfers, incidents, training, exceptions and corrective actions.
- 6.10.3 Independent assurance shall be distinguished from control operation and from GCSB recognition. Reviews shall verify outcomes and corrective closure through lawful, minimised access.

7. Implementation and transition

Full implementation shall take place within 12 months of certification commencement, with a 6-month gap assessment of existing systems against this standard. Existing lawful controls and binding legal obligations continue throughout transition; deferring privacy impact assessments, retention arrangements or individual rights handling until a later phase does not justify unlawful interim processing. Substantive changes to approved implementation dependencies require renewed approval.

8. Evidence, monitoring and corrective action

Metrics shall define eligible population, purpose, calculation, period, source, owner, exclusions, target and escalation. Where cost or benefit figures are used for planning, they are illustrative examples, not commitments or guarantees.

Corrective actions shall identify risk, owner, urgent protection measures, due date, authority, evidence and closure. Employment rights, safety and legal obligations are not waived by any corrective or disciplinary process.

Certification and enforcement decisions may be appealed within 30 days of notification to the Appeals body established under the GCSB Governance Charter. Assessment and decision clocks are set by the GCSB certification procedure.

9. Exceptions, escalation and review

The CCSO may approve temporary exceptions up to 12 months. Longer exceptions require approval by the Board Risk Committee on recommendation of the Enterprise Risk Management Committee. All exceptions are reviewed quarterly. Executive privacy delegation stays separate from independent DPO advice, and no exception approval authority transfers to the DPO.

Each deviation shall document requirement, scope, necessity, applicable law, risk, compensating controls, authority, duration, review, remediation and closure. Compensating controls shall not justify unmitigated unlawful processing.

Any GCSB recognition concession is granted only under the recognition scheme reviewed by the Certification and Standards Committee and approved by the Governing Council. No concession overrides legal duties or creates automatic recognition.

10. Document control and revision history

Version	Date	Change	By
---------	------	--------	----

2.0	13 October 2026	Version 2.0: consolidated, aligned suite edition (identifiers, approval route, law and disputes, exceptions, implementation timetable, appeals)	GCSB
Transfer edition	10 October 2026	Issuing authority, ownership, copyright and jurisdiction transferred from CSI to GCSB (UK); content unchanged; not a separate version	GCSB
1.0	2025	First edition, issued by the Converged Security Institute (CSI)	Prof. Dr. Vladimir Bunic

Superseded edition: the 10 October 2026 transfer edition.

© 2026 Prof. Dr. Vladimir Bunic and Global Converged Security Board (GCSB). All rights reserved.