



EUROPEAN CENTRAL BANK

EUROSYSTEM

Privacy-by-Design in Data Governance

From confidentiality protection to trusted
analytical use of data

*Session 1: Foundations of data privacy:
concepts, trade-offs and governance
frameworks*

IFC – BdP Workshop
14-15/09/2026

Rita Choudhury, Rosemarie Dember & Gianluca Damiani
European Central Bank, Directorate-General Statistics



Narrative

- 1 Why privacy-aware governance matters now
- 2 How ECB data governance evolved
- 3 What Privacy-by-Design means in practice
- 4 How ECB operationalises Privacy-by-Design
- 5 Extending Privacy-by-Design to AI / ML
- 6 How Privacy-by-Design supports transparency and controlled access
- 7 Practitioner takeaways: trade-offs and considerations
- 8 Conclusion: broadly applicable lessons

To show how Privacy-by-Design can be embedded into data governance through roles, processes, technical controls and accountability mechanisms, using ECB examples.

1. Why privacy-aware governance matters now

Privacy-by-Design Framework

This was developed by Ann Cavoukian in 1995 stating **privacy should not be an afterthought** but a core component of system engineering and organisational practices.

Our work uses the **concept** of **Privacy by Design** as an **analytical framework** to explore **how privacy can be systematically integrated** into workflows, technologies and governance structures.

Covers sensitive, confidential and personal data

Context

Rapid growth in data & analytics

Increased use of AI / ML

Regulatory expectations

Opportunities: new analytical capabilities

Risks: increased privacy, confidentiality & trust challenges

Privacy-by-Design

Addresses this by **embedding safeguards** early

Supports analysis / **Protects** data / **Maintains** public trust

Privacy-by-Design turns privacy from a downstream compliance check into an upstream governance principle

2. How ECB data governance evolved

Key evolution

1990s

Confidentiality & Harmonisation

Established statistical standards & safeguards for secure data collection, transmission & confidentiality across the Eurosystem



Protect Data



2000s

Infrastructure & Data Sharing

Expanded data governance to support central bank functions; More focus on data quality, databases & data exchange



Manage Data



Today

Strategic & Privacy-Aware Governance

Data as a strategic asset, governed via Privacy-by-Design, compliance, metadata, access control & accountability



Govern Data

Drivers of change

Granular, high-value data | Increased data sharing | Advanced analytics & automation |
Metadata & Traceability | Responsible data use

The transition is from protecting data after collection to designing privacy into the full data lifecycle

3. What Privacy-by-Design means in practice

Turning Privacy-by-Design Principles into Operational Controls

Principle	Control	ECB illustration
Privacy built-in	Assess risks before design is finalised	Digital Euro - privacy is a core design objective, with privacy-enhancing technologies built into the architecture.
Controlled access	Align access with role, purpose and sensitivity	Analytical Credit Dataset - role-based access limits visibility and pseudonymisation prevents re-identification, with continuous monitoring for anomalies.
Traceability by design	Embed ownership, metadata and lineage	ECB Data Catalogue - centralised platform integrating metadata, lineage and access controls for trusted data use.
Lifecycle protection	Apply safeguards from collection to retention	Household Finance & Consumption Survey (HFCS) - anonymisation and aggregation protect respondent identity, with GDPR compliance enforced through data-sharing agreements.
Continuous assurance	Monitor and review controls over time	TARGET Instant Payment Settlement (TIPS) - regular DPIAs identify risks in cross-border payments, with encryption and automated validation securing transactions in real time.

Privacy-by-Design embeds privacy into systems and processes from the outset

4. How ECB operationalises Privacy-by-Design

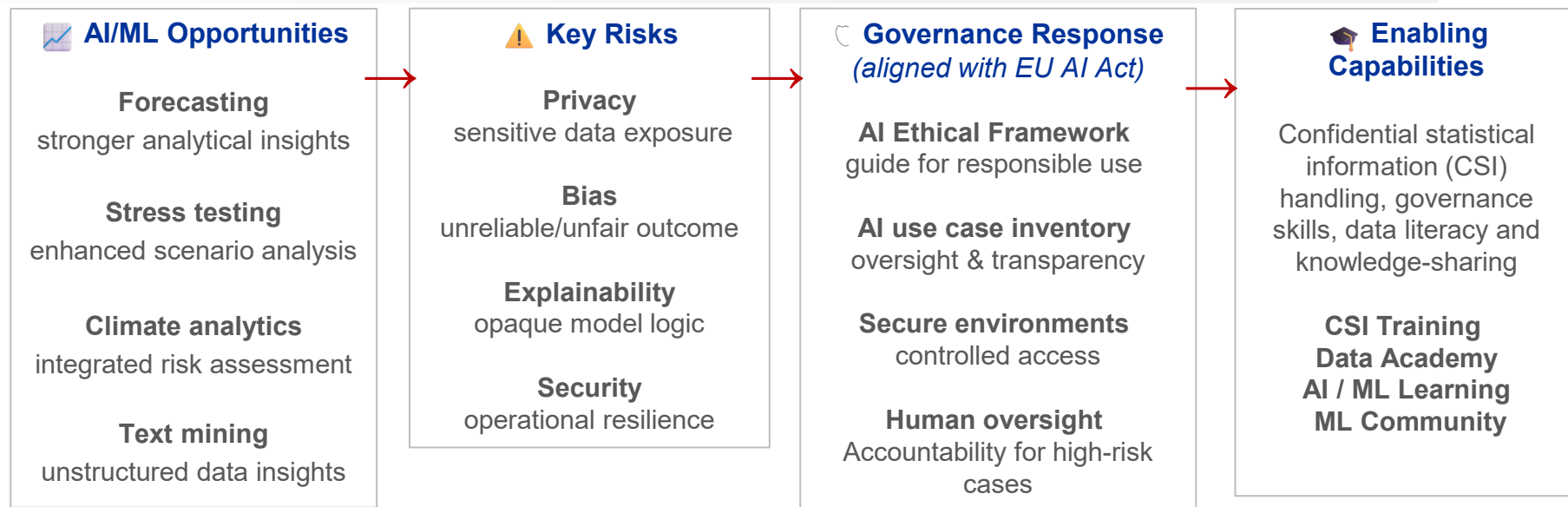
Embedding privacy into governance structures, policies and daily practices

Function	Purpose	ECB mechanism (for example)
Set direction	Define strategic priorities and accountability	Data Committee, Data Steward Group
Coordinate standards	Harmonise governance practices across ECB, ESCB & SSM	Statistics Committee and subgroups, Data Management & Governance Network
Define privacy controls	Apply safeguards, impact assessments and compliance oversight	Data Protection Framework & Office; DPIAs; Compilation & Processing Methodologies; IT Security Framework
Embed in workflows	Build controls into tools and processes	Policies for self-service Data Labs, Visualisation Tools, access controls and retention plans
Improve maturity	Assess gaps and prioritise improvements	Data Management Maturity Assessment

The key lesson is that Privacy-by-Design requires assigned roles, repeatable processes and governance escalation routes

5. Extending Privacy-by-Design to AI / ML

Extending privacy-aware governance to emerging technologies



Responsible AI depends on three foundations:

Privacy-by-Design governance | Secure technical environments | Trained users

6. How Privacy-by-Design supports transparency and controlled access

Applying Privacy-by-Design in interactions with external users

Transparency for external users

- Privacy notices
- Clear information on personal data handling
- Transparent enquiry and access procedures

Controlled Access to personal data

- Need-to-know principles
- Role-based access and secure CRM workflows
- Controlled involvement of subject matter experts

Accountability

- Complaint and appeal mechanisms for external users
- DPO and supervisory oversight; compliance with EUDPR

Statistics Hotline:

Privacy-by-Design in practice for External User Support

- Diverse external stakeholder groups, including public
- Customised off-the-shelf CRM system with controlled access
- Efficient processing supported by workflow automation
- AI-assisted support (chatbot, enquiry management)
- Direct enquiry resolution with a minimal need-to-know personal data processing

Trust is strengthened when users understand how their data is used and protected

7a. Practitioner takeaways: navigating trade-offs

The practical challenge: balancing innovation, usability and privacy

Key challenge	How trade-offs are managed
Innovation vs Privacy	Enable responsible analytics <u>while</u> protecting sensitive, confidential and personal data • Proportionality: Controls reflect sensitivity, risk and business need • Purpose limitation: Use remains aligned with approved purposes and need-to-know access • Privacy-enhancing techniques: Anonymisation, pseudonymisation and aggregation
Usability vs Security	Keep tools accessible for legitimate use <u>while</u> maintaining strong safeguards • Tiered access: Access levels reflect role, purpose and sensitivity • Secure environments: Sensitive data is used in controlled technical environments • Monitoring: Access and use are logged, reviewed and auditable
Organisational Silos & Resource Constraints	Align practices across business areas <u>and</u> prioritise controls based on risk • Standardised processes: Common workflows reduce fragmentation • Risk-based prioritisation: Resources focus on highest-risk and highest-impact use cases • Escalation: High-risk use cases go through DPIA, DPO consultation or committee review

Privacy does not prevent innovation – effective governance enables responsible innovation

7b. Practitioner takeaways: implementation considerations

Ask these questions when developing or reviewing a data initiative

Accountability

- ☐ **Ownership and accountability** assigned?

Data understanding

- ☐ **Metadata and lineage** documented?
- ☐ **Data sensitivity** classified?

Access and sharing

- ☐ **Access controls** defined?
- ☐ **Data-sharing arrangements** documented and standardised?
- ☐ **Monitoring and audit** in place?

Risk-based governance

- ☐ **Governance proportionate** to level of risk and business need?
- ☐ **Data Protection Impact Assessment (DPIA)** required?
- ☐ **Governance maturity** assessed?

AI / ML

- ☐ **Explainability** and **model governance** assessed?

Transparency

- ☐ **Data subject** and **external-user obligations** addressed?

If these questions are answered early, privacy becomes an enabler of trusted data use

8. Conclusion

Five broadly applicable lessons

Governance is an evolution

From confidentiality and security to lifecycle-based governance

Privacy starts at design

Privacy is most effective when embedded into systems and processes from the outset

Governance must be operational

Controls work best when built into tools, workflows and data products

Controls should be proportionate

Safeguards should reflect data sensitivity, risk and business need

Trust depends on people and transparency

Training, accountability and stakeholder engagement support responsible data use

Privacy-by-Design is not a one-off control, but a governance capability for trusted data use



Questions & Discussion

The views expressed in this presentation are those of the authors and do not necessarily reflect the official position of the European Central Bank (ECB) or its broader strategic direction.