Contribution to EDPB Public Consultation GDPR Templates

I acknowledge that the EDPB invited one-page submissions; however, I have included additional technical context solely to ensure clarity. The core template itself fits within a single page, and the extended material is provided only to aid understanding with Real world Examples on GDPR Enforcement in general via machine verifiable template and its possible alignment with Digital Euro

Which template would be most helpful?

Proposal: Machine-Verifiable "Lawful-Purpose & Jurisdiction Token" (LPJT) Template

Protected under the **Patent Cooperation Treaty (PCT) at the World Intellectual Property Organization (WIPO), Genev**a — WO 2025/210622, WO 2025/210623, WO 2025/215626 (2,550+ coordinated claims). Offered royalty-free for sovereign regulatory use; FRAND for commercial adoption.

The UK Department for Science, Innovation & Technology (DSIT) has formally acknowledged this work and retained it for reference (Ref: TO2025- 00013881-JK)

Introduction

To make GDPR compliance simpler, clearer, and more resilient—particularly for SMEs—I propose an **optional, machine-verifiable template** that allows key GDPR obligations to be expressed **inside the data flow itself**, not solely through organisational policies or paper-based documentation.

Today's compliance ecosystem relies heavily on documents (privacy notices, ROPAs, DPIAs, contractual clauses). While essential, these documents:

- impose high recurring costs on SMEs,
- can be interpreted inconsistently, and
- operate out-of-band from real-time data processing.

Meanwhile, modern systems (cloud, mobile apps, AI models, APIs) operate **in milliseconds**, where violations can occur long before paperwork is reviewed.

A **protocol-level template** would allow GDPR principles to be **verified automatically at the moment data moves**, strengthening protection against unlawful processing and reducing administrative burden.

Proposed Template:

Lawful-Purpose & Jurisdiction Token (LPJT)**

The LPJT is a **machine-readable, standardised structure** (e.g., JSON Schema or CBOR) containing core GDPR-relevant fields:

- **Lawful purpose / legal basis**
- **Consent state** (including consent hash)
- **Data categories involved**
- **Processing context** (analytics, security, service delivery, etc.)
- **Jurisdiction & transfer constraints (Arts. 44–49)**
- **Storage, retention, expiry**
- **Revocation and withdrawal status**

When cryptographically bound to a **Virtual Identity (VI)**—a pseudonymous representation of the device, user, or application performing the processing—the LPJT becomes a **verifiable compliance envelope**.

Every data flow, API call, or cross-border transfer can then be checked **automatically** to ensure it conforms to the declared purpose and jurisdiction.

Why This Template Would Be Helpful

1. Strengthens GDPR enforcement at the protocol layer

Today, GDPR works on *policies, contracts, and post-facto audits*. This template shifts compliance to a **binary, cryptographically verifiable rule** inside the network:

- **Valid LPJT (lawful-purpose token) → allow**
- **Invalid / absent token → block inline**

This directly aligns with the protocol-level architecture described in your Executive Summary and Feasibility Note.

---

2. Prevents unlawful transfers before they occur

Cross-border data misuse is one of the biggest gaps in GDPR enforcement. This template ensures:

- Data **cannot leave the EU** unless the LPJT explicitly authorises that jurisdiction.
- No “invisible enrichment” in foreign servers or partner clouds.
- No covert ad-tech or AI-driven routing to third countries.

Flows without correct jurisdiction tags fail in **<5 ms**, as outlined in the feasibility benchmarks.

---

3. Reduces SME compliance burden

Today, SMEs struggle with:

- SCCs
- DPIAs
- Contract chains
- Repetitive privacy documentation

By embedding lawful-purpose checks into every flow:

- SMEs simply integrate an API/SDK (like TLS/SSL)
- Manual compliance cost drops 40–80%
- No complex cross-border paperwork

This aligns directly with the European Strategic Impact Note.

SME Compliance Savings (Practical Economic Impact)

- **40–50% reduction in GDPR compliance costs** by replacing DPIAs, SCCs, contract chains, and repeated legal audits with automatic, protocol-level checks.
- **"Compliance by default"** — SMEs integrate a simple SDK/API (similar to TLS, UPI, Stripe) instead of hiring specialised GDPR consultants or lawyers.
- **No paperwork burden** for cross-border data, since LPJT tokens encode jurisdiction automatically (expiry, purpose, consent, adequacy).
- **Instant auditability** — every transaction auto-generates a regulator-verifiable LAVR, eliminating audit preparation work for SMEs.
- **Level playing field** — small businesses gain the same compliance strength that only previously afforded through large legal teams.
- **Cross-border trust boost** — SMEs can safely expand into EU-wide or international markets without risk of accidental GDPR violations.
- **Reduced breach risk & penalties** — cryptographic enforcement prevents violations before they occur, protecting SMEs from €4M+ average EU breach costs or accidental unlawful transfers.
- **Competitive advantage** — SMEs can advertise verifiable, token-based privacy compliance to earn customer trust with zero additional overhead.

---

4. Improves auditability & consistency

Regulators no longer rely on PDFs, contracts, or voluntary disclosures.

Instead:

- Every decision (allow/deny) becomes a **Ledger-Anchored Validation Receipt (LAVR)**.
- These records contain *only compliance metadata* — no user identifiers.
- Regulators gain **real-time audit capability**.

This closes the "months-later discovery" gap of GDPR.

5. Protects Digital Euro from unlawful enrichment

The Digital Euro requires:

- Privacy
- AML compliance
- Jurisdictional integrity
- Real-time policy enforcement

This template embeds all of these inside each transaction:

- **Each payment carries a VI + LPJT**
- **No token → no transaction**
- Prevents cross-border laundering, replay fraud, illicit metadata extraction
- Ensures compliance with GDPR Articles 5, 6, 7, 25, 30, 32, 44–49

This turns the Digital Euro into the world’s first **protocol-level GDPR-aligned CBDC**, as described in your CBDC Research Paper.

---

6. Reinforces Election Integrity

This is one of the strongest benefits.

European regulators increasingly recognise that **unauthorised profiling influences democracy** — especially when data flows to foreign jurisdictions.

- Election manipulation
- Behavioural profiling
- Cross-app enrichment
- Foreign amplification
- Ad-tech precision targeting
- Romanian 2024 election interference case

With this template:

- Every political-ad, profiling attempt, or micro-targeting action must present its **LPJT purpose**.
- If not explicitly authorised → **flow fails cryptographically**.
- Covert political messaging cannot be routed, boosted, or enriched across borders.

This gives Europe the first **technical election-integrity firewall** in history

8. Aligns cleanly with Article 25: Data Protection by Design

Today, “Privacy by Design” is mostly theoretical. With the template:

- Privacy becomes *machine-enforced*, not *policy-declared*.
- Purposes, consents, and jurisdictions are verifiable in every transaction.
- Systems across the EU implement GDPR in a **uniform** way.

This template converts GDPR obligations into cryptographically enforced protocol rules.

It protects the Digital Euro, democratic processes, and cross-border data integrity by ensuring that every digital flow carries a verifiable, lawful-purpose token.
No valid token → no transfer, no profiling, no misuse — all enforced in <5 ms.

What this proposal does *not* do

- It does **not** amend or reinterpret GDPR.
- It does **not** impose any new legal obligations.
- It does **not** require new data categories or new lawful bases.
- It does **not** replace SCCs, DPAs, DPIAs, or consent frameworks.

It simply provides a technical template that makes existing GDPR obligations easier to implement, verify, and audit—especially in automated systems.

ANNEX X — Machine-Verifiable Lawful-Purpose & Jurisdiction Token (LPJT) Template

(Optional Technical Instrument Supporting GDPR Articles 5, 6, 7, 25, 30, 32, 44–49)

1. Objective

This Annex provides an optional, machine-verifiable template (Lawful-Purpose & Jurisdiction Token — LPJT) enabling controllers and processors to express GDPR-relevant obligations in a structured, machine-interpretable format that may accompany digital data flows.

The LPJT supports the principles of:

- Lawfulness, fairness, transparency (Art. 5)
- Purpose limitation and minimisation (Art. 5(1)(b)(c))
- Lawful basis and consent (Arts. 6–7)
- Data Protection by Design and by Default (Art. 25)
- Records of processing (Art. 30)
- Security of processing (Art. 32)
- Cross-border data transfers (Arts. 44–49)

This Annex does **not** create or amend legal obligations. It serves as a voluntary mechanism to support consistent implementation of existing requirements.

---

2. Structure of the LPJT Template

The LPJT consists of the following fields:

Field	Description
lpjt_version	Version of the template specification
lawful_basis	Legal basis for processing as defined in Art. 6
purpose_code	Declared purpose of processing (standardised taxonomy)
consent_state	Consent obtained, withdrawn, or not required
consent_reference	Hash or reference to the consent record
data_categories	Types of personal data processed
processing_context	Context of processing (analytics, security, service delivery, etc.)
retention_expiry	Maximum retention period or expiry condition
jurisdiction_rule	Geographic or regulatory constraints
recipient_scope	Permitted recipients (first-party, processor, sub-processor)
revocation_status	Status of consent or legal basis
vi_binding_hash	Binding to a Virtual Identity (VI) for technical enforcement
signature	Optional cryptographic signature (e.g., DPO, controller, regulator)

---

3. Intended Use

Controllers may attach the LPJT to:

- outbound data flows,
- API calls,
- cross-border disclosures,
- automated processing operations,
- training data for AI systems,
- intra-group transfers,
- cloud-to-cloud workflows.

Processors may use it to:

- demonstrate compliance to controllers,
- enforce processing scope as contractually defined,
- reduce manual audits by providing machine-verifiable controls.

Regulators may use it to:

- support harmonised interpretation across Member States,
- reduce small-business compliance burden,
- improve transparency and oversight.

---

4. Interoperability With the Digital Omnibus, AI Act & Data Act

4.1 Digital Omnibus

The LPJT supports simplification goals of the Digital Omnibus by:

- providing a unified, machine-readable format across sectors,
- reducing duplicative compliance documentation,
- enabling “once-only” implementation of lawful-purpose metadata.

4.2 AI Act (Art. 10 & 28)

LPJT fields map to:

- data governance and quality (AI Act Art. 10),
- traceability and logging requirements,
- clear purpose specification for training datasets.

The LPJT enables consistent *purpose binding* for data used in AI training and evaluation.

4.3 Data Act

The LPJT supports:

- enforcement of data-sharing agreements,
- transparent purpose limitation in B2B and B2G transfers,
- machine-readable expression of contractual boundaries.

---

5. Enforcement Neutrality

The LPJT does not mandate any specific enforcement architecture.
It may be implemented using:

- existing platforms,
- API gateways,
- cloud services,
- software libraries, or
- protocol-level validators (e.g., Virtual Identity binding).

---

6. Optional Machine-Verifiable Binding (VI)

Controllers may bind an LPJT to a **Virtual Identity (VI)** representing a device, system, or authorised processing agent.

This enables deterministic (yes/no) enforcement of:

- purpose scope,
- jurisdiction constraints,
- retention expiry,
- consent withdrawal,
- transfer restrictions.

---

2. LPJT JSON EXAMPLE

```
{
  "lpjt_version": "1.0",
  "lawful_basis": "consent",
  "purpose_code": "P-ANALYTICS-01",
  "consent_state": "valid",
  "consent_reference": "hash:92d8fe3aa1c...",
  "data_categories": ["device_ip_truncated", "session_metadata"],
  "processing_context": "first_party_analytics",
  "retention_expiry": "2026-12-31T23:59:00Z",
  "jurisdiction_rule": "EU_ONLY",
  "recipient_scope": ["controller", "processor"],
  "revocation_status": "active",
  "vi_binding_hash": "h3c2f9e1b4...",
  "signature": "SIGN_DPO( ... )"
}
```

---

3. LPJT YAML EXAMPLE

```
lpjt_version: "1.0"
lawful_basis: "contract"
purpose_code: "P-SERVICE-DELIVERY-02"
consent_state: "not_required"
data_categories:
  - account_id_pseudonymised
  - service_usage_metrics
processing_context: "service_delivery"
jurisdiction_rule: "EU_EEA_ONLY"
retention_expiry: "90_days"
recipient_scope:
  - controller
  - processor
revocation_status: "n/a"
vi_binding_hash: "9ab233ff0e1ac..."
signature: "SIGN_CONTROLLER(...)"
```

4. DIAGRAM — LPJT BOUND TO A VIRTUAL IDENTITY (ASCII FORMAT)

```
┌──────────────────────────────────────────────────────────┐
│                   Virtual Identity (VI)                   │
│  - pseudonymous key                                       │
│  - device/app/session scoped                              │
│  - generated in TEE/secure module                         │
└──────────────────────────────────────────────────────────┘
                 │
                 │ (binding_hash)
                 ▼
┌──────────────────────────────────────────────────────────┐
│         Lawful-Purpose & Jurisdiction Token (LPJT)        │
│  - lawful basis                                           │
│  - purpose code                                           │
│  - consent reference                                      │
│  - jurisdiction rule                                      │
│  - retention expiry                                       │
│  - recipient scope                                        │
│  - revocation status                                      │
│   - signature (optional)                                  │
└──────────────────────────────────────────────────────────┘
                 │
                 │ (attached to)
                 ▼
┌──────────────────────────────────────────────────────────┐
│                   Data Flow / API Request                 │
│  - HTTP request / API call / cross-border transfer        │
│  - Enforced by validator or system logic                  │
└──────────────────────────────────────────────────────────┘
```

Unilateral Enforcement Model

The framework is intentionally designed to function even if only one jurisdiction chooses to adopt it. Enforcement occurs at the origin of the data flow, meaning a jurisdiction can apply VI+CJT validation unilaterally, without requiring adoption or coordination from any other country or external system. All outbound data generated within that jurisdiction must carry a valid, purpose-bound CJT before it leaves the territory. If a remote service provider or application does not voluntarily adopt the mechanism, the jurisdiction can still enforce the policy across multiple technical layers—at the application wrapper, browser, operating system, telecom/network gateway, or API/edge-gateway level—ensuring that lawful-purpose and jurisdiction rules are upheld without dependency on external actors.

A. Enforcement Points Without Cooperation From the Remote System

A jurisdiction adopting VI+CJT can implement enforcement at several independent technical layers:

1. **Application Layer**
    - Enforcement can be applied through an application wrapper or platform-level integration.
    - The VI and CJT are attached before any outbound request is generated.
    - No changes are required on the remote system.
2. **Operating System Layer**
    - OS-level controls ensure that all outbound data flows carry a valid VI+CJT.
    - If a token is invalid, expired, or missing, the OS blocks transmission automatically.
3. **Browser Layer (for Web-Based Services)**
    - Browser-level validators can attach VIs and CJTs to all cross-origin requests.
    - Requests lacking a valid token are blocked locally before leaving the jurisdiction.
4. **Network / Telecom Layer**
    - Enforcement can also occur at the telecom gateway, ISP, or network edge.
    - Gateways validate the VI+CJT before allowing data to cross a jurisdictional boundary.

5. **API Gateway / Edge Validator Layer**

    - API gateways operating within the jurisdiction can validate all outgoing API traffic.
    - Only requests containing valid, purpose-bound CJTs are permitted to route to external servers.

B. Why Remote Systems Do Not Need to Adopt the Framework

The VI+CJT mechanism operates **asymmetrically**:

- Validation and enforcement happen on the **sending side** of the transaction.
- The remote system merely receives a compliant, policy-conforming request.
- No cooperation, software update, or policy adoption is required from the external environment.

This design ensures:

- **Interoperability** with all existing systems
- **Continuity of service**, even when remote systems do not adopt the framework
- **No disruption** to international digital operations
- **Full compliance** with cross-border data protection requirements

C. Final Explanation

Even if a remote service provider does not implement VI+CJT on its side:

- Outbound data from the adopting jurisdiction is still validated locally.
- Compliance is enforced **before any transfer occurs**.
- Cross-border protection remains effective.
- There is **no dependency** on foreign adoption or global coordination.

This unilateral-enforcement capability is a core strength of the architecture:
a jurisdiction can enforce lawful-purpose, consent, and jurisdictional rules independently, ensuring that all outgoing data generated within its territory complies with its regulatory requirements.

Why this is not by passable

For LPJT + VI enforcement, every data flow must satisfy a fixed set of verification conditions. These checks are deterministic, and each one must succeed before any request is allowed to proceed.

A flow is accepted only when all of the following are valid:

1. **The Virtual Identity (VI)** has been generated inside an attested TEE/secure module.
2. **The LPJT/CJT signature** is valid and originates from an authorised issuing authority.
3. **The binding hash** correctly links the token to the specific VI and the declared domain/service.
4. **The jurisdiction field** matches the validator's approved regulatory zone.
5. **The declared purpose** aligns with the validator's accepted scope.
6. **The expiry time** has not passed.
7. **The token is not listed in any active revocation update.**

If any one of these conditions is not met, the validator immediately denies the request.
The entire decision process completes within a few milliseconds and does not rely on discretionary interpretation, manual approval, or external policy files.

This design ensures that data flows operate only within their authorised purpose and jurisdiction, with real-time revocation and auditability built in.

Why LPJT + VI Cannot Be Bypassed by a VPN

A VPN only hides or alters **network location**, but the LPJT + VI system does not rely on the device's visible IP address to determine jurisdiction or permission.
Instead, the validator enforces jurisdiction and purpose **using cryptographically signed fields inside the LPJT**, which a VPN cannot modify or influence.

For every request, the validator checks:

1. **The LPJT's jurisdiction_rule**
2. **The LPJT's purpose_code**
3. **The LPJT's binding_hash tied to the VI**
4. **The LPJT's authorised destination domain**
5. **The LPJT's signature from the issuing authority**

A VPN cannot change any of these values, because:

- They are **fixed and signed inside the LPJT**
- They are **verified independently of device IP**
- Any alteration breaks the signature and the request is rejected
- The validator uses **LPJT jurisdiction**, not IP geolocation, for decisions

Even if a VPN tunnels traffic through another region, **the LPJT still declares the true authorised jurisdiction**, and the validator compares *that* to the policy — not the apparent network location.

Therefore, VPN routing has no effect on the validation outcome.

Example: Clinical Data Leaves One Region and Goes to Another Region

A hospital machine measures a patient’s heart-rate trend.
It needs to send a short summary of the trend (not raw patient records) to an external specialised analysis service located in another region.

Before sending anything, the machine receives a digital permission slip (LPJT).
This LPJT states:

- Purpose: clinical analysis only
- Recipient: the named external analysis system only
- Retention: 7 days
- Territory: may transfer to the specific external region listed
- No onward transfer beyond that system
- No secondary use such as research, advertising, insurance scoring, or profiling
- Only decryptable under the same purpose, by the approved system

The machine also generates a temporary identity (VI) valid only for this session.

The machine sends: the summary + the LPJT + the VI.

A validator checks the request. Only if all conditions match the LPJT, the transfer is allowed.

Once the data arrives in the external country, the same rules continue to apply.

Scenario 1: Legitimate Clinical Analysis

(Allowed and Visible to Regulators)**

The external analysis system performs only the approved clinical analysis.

To process the data, it requests decryption.

The validator checks:

- Is the LPJT still valid?
- Is the purpose still “clinical analysis only”?
- Is the receiving system the same one listed in the LPJT?
- Is the retention time still valid?

If all match, the key is released.

A small audit record is created:

- Which machine asked
- What LPJT was used
- What purpose was approved
- Which system received the data
- When processing occurred

Regulators (including EU data regulators) can see this record.

No personal identifiers are in the record, only compliance facts.

Evaluation:
The transfer was limited, purpose-bound, and logged.
No hidden reuse possible.
This meets Article 44–49 requirements.

Scenario 2: Attempted Use for Research or Advertising

(Blocked Immediately)**

The foreign system tries to use the same clinical summary for research or marketing.

It requests a new operation: “process for research”.

The validator checks the LPJT.

The LPJT says: “clinical analysis only.”

The purpose does not match.

The request is denied.

A log entry is created saying: “Attempted non-permitted purpose.”

EU regulators can see that an improper attempt was made, but the data was not released.

Evaluation:
Cross-purpose use was technically impossible.
Attempt was visible and blocked.
No risk to patient privacy.

Scenario 3: Attempted Onward Transfer to Another External Server

(Blocked Immediately)**

The external system tries to forward the clinical data to a second external server.

It asks for processing at a new destination.

The validator checks:

- The LPJT lists only one authorised recipient (the original analysis system).
- The new destination is not listed.

The validator denies the request.

A record is generated: “Attempted onward transfer; rejected.”

auditors see that even if the foreign operator tried to send the data onward, the system prevented it.

Evaluation:
No onward transfer possible.
LPJT acts as a cross-border guard.
Full compliance with EU territorial rules.

Scenario 4: Attempt to Decrypt Data in a Non-Authorised Location

(Blocked and Reported)**

Someone tries to decrypt the data on a different server that is not listed in the LPJT.

The validator checks:

- Location does not match.
- Purpose does not match.

The decryption key is not released.

A log entry is created showing: “Decryption request at unauthorised location; denied.”

Auditors can see this entry.

Evaluation:
Access control is enforced at the cryptographic layer.
No silent decryption possible.
Violations are detectable.

Scenario 5: Data Kept Longer Than Approved Retention

(Processing Automatically Stops)**

Seven days pass.

The LPJT expires.

If the external system tries to continue processing or even tries to read the data again:

- the validator checks expiry
- the operation fails immediately

After expiry, no key release is permitted.

Even if the foreign system stores the ciphertext, it cannot decrypt it anymore.

Evaluation:
Automatic enforcement of retention.
Data becomes unusable at the expiry point.
No reliance on promises or manual deletion.

Scenario 6: Attempt to Merge Clinical Data With Another Database

(Blocked Automatically)**

Someone tries to combine the clinical data with another dataset for trend analysis, behavioural profiling, or product development.

The new operation requires a new LPJT purpose.

The issued LPJT does not include those purposes.

The validator denies the merge.

A log entry shows: “Merge attempt denied due to incompatible purpose.”

Evaluation:
Data minimisation and purpose limitation enforced.
No uncontrolled combination of datasets.
GDPR Article 5(1)(b)(c) satisfied.

Scenario 7: Attempt to Bypass Using a VPN or Rerouted Traffic

(Not Possible)**

Even if the external country tries to route traffic through different networks, or use different IP addresses, the validator does not check location by IP.

It checks:

- the LPJT purpose
- the authorised destination ID
- the expiry
- the identity binding

Since the permission slip says “only this approved system,” rerouting does not help.

The operation fails.

Evaluation:
No geographic trick can override LPJT rules.
The enforcement happens above routing level.
GDPR cross-border restrictions remain intact.

Scenario 8: Attempt to Decrypt Data Offline or Without Asking

(Not Possible)**

Encrypted data stored in the external system cannot be decrypted offline.

All decryption keys require:

- a valid LPJT
- an approved purpose
- a valid time window
- the authorised environment
- a validator request

If someone tries offline decryption, it does not work.

If someone tries unauthorised online decryption, it is logged and rejected.

Evaluation:
Encryption alone is not the protection.
Key-release rules enforce GDPR even outside the EU.

Conclusion

Even when data is transferred to another country **with proper authorisation**, the following remain guaranteed:

1. The data can only be used for the allowed purpose.
2. The data can only be processed by the approved system.
3. No secondary use is possible.
4. No onward transfer is possible.
5. No hidden decryption is possible.
6. Retention is enforced automatically.
7. Every operation, allowed or denied, is visible to EU regulators.
8. Violations cannot occur without creating an audit trail.

The privacy protection does not stop at the EU border.
It travels with the data and remains enforceable everywhere.

Example: Digital Euro – Privacy and AML Together

A user wants to pay a shop using the Digital Euro.

Before the payment is sent, the user’s device creates a temporary digital identity (VI).
This VI does not contain the user’s name, account number, phone number, or any personal details.

Next, the payment system issues a small permission slip (CJT) for this specific payment.
The CJT states:

- the purpose: retail payment
- the maximum amount allowed
- the merchant who is allowed to receive it
- the time window for the payment
- the AML-required information in hashed or minimal form
- the rule that the payment cannot be forwarded to any other recipient

The user’s device sends:
VI + CJT + payment amount.

A validator checks:

1. Is this VI from a legitimate device?
2. Does the CJT allow a retail payment?
3. Is the amount within the AML-permitted limits?
4. Is the destination the approved merchant?
5. Is the payment within the allowed time?
6. Is the CJT still valid and not revoked?

If everything matches, the payment is completed.

During this process:

- The shop never sees the user’s real identity.
- AML obligations are satisfied because the CJT carries the required compliance information.
- No profiling is possible because the VI changes frequently and cannot be linked across transactions.
- Regulators can verify compliance through small audit records that contain no personal data, only proof that rules were followed.

If the amount exceeds AML thresholds or the payment purpose is incorrect, the validator blocks it immediately.

This allows the Digital Euro to achieve both goals at once:
strong privacy for users and automatic enforcement of AML rules without exposing personal information.

Note on Contribution:

This submission responds to EDPB's open public consultation inviting ideas on useful GDPR templates. The author submits this technical proposal in good faith as a contribution to European digital governance development, without any intention to influence internal EU policy processes inappropriately. The consultation is open to international participants, and this contribution aims to support the EU's stated objectives of reducing compliance burden while strengthening data protection.

Acknowledgment and Gratitude

This work is deeply indebted to the intellectual leadership of European research institutions and would not have been possible without the EU’s world-leading privacy frameworks and open scientific culture. The concepts and technical constructs presented here draw inspiration from the publicly available research and guidance of the European Data Protection Board (EDPB), the European Data Protection Supervisor (EDPS), the European Union Agency for Cybersecurity (ENISA), the Court of Justice of the European Union (CJEU), the European Commission, the European Central Bank (ECB), ANSSI (France), BSI (Germany), the Fraunhofer Institute, the NATO Strategic Communications Centre of Excellence, and contributions from the broader European academic community, including researchers at Oxford University and multiple EU-based institutions.

I am equally grateful for the support, research culture, and open knowledge made available by Indian institutions. The work has benefited from insights published by organisations such as NASSCOM, the Reserve Bank of India (RBI), and various Indian digital-governance bodies whose studies on payments, cybersecurity, and data protection have shaped the practical considerations of this framework. I also express my sincere appreciation to the **Indian Patent Office (IPO)** for its constructive support, accessibility, and administrative guidance, which has been invaluable to an independent inventor navigating complex, technically detailed filings.

This research has further drawn upon the publicly accessible work of leading United States institutions and research organisations. In particular, the National Institute of Standards and Technology (NIST), the National Science Foundation (NSF), the Federal Trade Commission (FTC), the Carnegie Endowment for International Peace, MIT’s Digital Currency Initiative (DCI), Stanford University’s Cyber Policy Center, the Electronic Frontier Foundation (EFF), and various US academic researchers working in cryptography, privacy engineering, financial-integrity systems, and cybersecurity have contributed important ideas to the global knowledge base that informs this work.

I express deep gratitude to the Government of India and the International Bureau of WIPO (Geneva) for the PCT fee-reduction programmes for individual inventors and SMEs—support that has made advanced, globally coordinated international filings financially accessible to independent researchers like myself.

This contribution is made with respect and gratitude to the European Union, India, and the United States for fostering an international research environment where independent innovation can emerge, evolve, and be shared for public benefit.

Disclaimer:

The estimated potential reduction in SME compliance effort (40–50% or more for SMEs) is provided solely for illustrative purposes.

It reflects general observations on repetitive documentation tasks (e.g., SCC renewals, DPIA cycles, cross-border assessments) and the operational efficiencies that machine-verifiable templates can theoretically offer.

Actual reductions will vary according to sector, organisational maturity, national supervisory expectations, and the specific implementation context.

This indication is not intended as a policy position, economic forecast, or recommendation. It is presented purely to help regulators understand the types of administrative burdens that automated compliance templates may mitigate.