# 1) Title

**Comments on EDPB Recommendations 2/2025 — Account Creation on E-Commerce Websites: Execution-Time Purpose Limitation and Privacy-Preserving Alternatives**

# 2) Introductory Note

This contribution is provided in good faith for informational purposes. It offers an implementation-level perspective on how the principles reflected in the Recommendations—necessity, proportionality, data minimisation, storage limitation, and privacy by design and by default—can be applied consistently in automated e-commerce systems. It does not propose new legal obligations or amendments.

# 3) Key Point

The Recommendations correctly identify that mandatory account creation is lawful only in limited circumstances (e.g., subscriptions or genuinely restricted offers), and that **guest purchase options are generally the most privacy-protective approach**, aligned with Article 25 GDPR.

# 4) Implementation-Level Observation (the technical gap)

In practice, many e-commerce systems require accounts because current architectures treat "identity persistence" as the default mechanism for:

- order tracking,
- customer support,
- returns/warranty handling,
- fraud controls,
- "convenience" features.

This creates systemic risks highlighted by the Recommendations: unnecessary identification, longer retention, easier linkage across contexts, and function creep toward profiling.

**The technical gap is not legal uncertainty.**
It is that legal conditions (necessity, purpose limitation, retention limits) are often enforced inconsistently or after the fact, rather than **at the moment the system executes an action** (checkout, storage, sharing, reuse).

# 5) Brief Description : VI, CJT, and ALF

## Virtual Identity (VI)

A **Virtual Identity** is a **pseudonymous, purpose-scoped identifier** that can be:

- **transaction-scoped** (single purchase),
- **session-scoped** (a short period),
- **service-scoped** (subscription duration),
  and is designed to avoid persistent cross-context linkage by default.

## Compliance/Jurisdiction Token (CJT)

A **CJT** is a machine-verifiable authorisation token that encodes:

- **purpose** (e.g., order fulfilment, returns, fraud prevention),
- **expiry / retention window**,
- **scope** (which system/service can use it),
- optional constraints (e.g., one-time use, quota, revocability).

## ALF (Algorithmic Logic Fingerprint) — Purpose-limited execution

An **ALF** is a cryptographic fingerprint of the *approved execution logic* for a given purpose (e.g., "returns eligibility check", "fraud-risk scoring"), enabling systems to verify that the logic being executed matches what was approved for that purpose—**without inspecting or disclosing source code**.

**In combination:**
A system may allow "guest mode" purchasing while still supporting operational needs, by using **VI + CJT** for purpose limitation and expiry, and **ALF** to prevent "purpose drift" in automated decision logic.

# 6) Five Real-World Examples (how it works in practice)

## Example 1 — One-time purchase (default guest checkout)

- User buys as a guest.
- Site issues a **Purchase-VI** valid only for that order.
- CJT purpose: **order fulfilment**, expiry: **X days** (until delivery + buffer).

- Result: delivery happens; after expiry, the system cannot keep using the identifier for unrelated purposes.

## Example 2 — Returns / warranty without a permanent account

- User requests a return via a link from the receipt email.
- A **Return-VI** is generated for that case only.
- CJT purpose: **returns processing**, expiry: **return window**.
- Optional ALF ensures the "return eligibility decision" logic cannot be repurposed into profiling or marketing.

## Example 3 — Subscription (where account may be necessary)

- A genuine subscription requires repeated authenticated interactions.
- User has a **Subscription-VI** lasting only for the subscription term.
- CJT purpose: **subscription access**, expiry: **subscription end + defined retention**.
- This supports EDPB's view that mandatory accounts may be justified for subscriptions—while still enforcing storage limitation.

## Example 4 — Exclusive offers (closed community)

- Access requires verified eligibility (e.g., invitation/validated membership).
- User receives a **Member-VI** bound to eligibility.
- CJT purpose: **member access**, expiry: **membership duration**, scoped to "exclusive offers".
- Prevents "open-to-everyone account creation" being misused as a legal basis.

## Example 5 — Fraud prevention without forcing persistent accounts

- Fraud signals are checked at checkout using a **Fraud-VI** and CJT purpose: **fraud prevention** with strict expiry.
- ALF restricts the fraud logic to permitted checks (e.g., abnormal payment velocity), preventing drift into behavioural profiling.
- This addresses the Recommendations' point that accounts are not necessary for fraud prevention and may increase risk.

# 7) Problems Today and How They Are Addressed Technically

## Problem A — Account creation becomes identity persistence by default

### What goes wrong today

In most e-commerce systems, account creation is not just an access method—it becomes a **permanent identity anchor**:

- A single account identifier links purchases, browsing, returns, customer support, and marketing.
- This identifier persists long after the transaction is complete.
- Even when a user makes only one purchase, the system is technically structured as if a long-term relationship exists.

### Why this matters for data protection

This design:

- Enables cross-context linkage by default
- Increases re-identification risk
- Makes future reuse of data technically easy, even when legally unjustified

### Technical addressing

Instead of a permanent account identifier, the system issues:

- a **transaction-scoped or session-scoped Virtual Identity (VI)**

This VI:

- Exists only for the operational task (e.g. a single purchase)
- Cannot be reused across unrelated contexts
- Automatically expires

### Result

The system still functions operationally, but **identity persistence is no longer the default technical state**, aligning with data minimisation and privacy by default.

## Problem B — Retention extends beyond necessity ("orphaned accounts")

### What goes wrong today

Many accounts become inactive but remain stored indefinitely:

- No automatic enforcement of retention limits
- Data remains technically accessible
- Old identifiers can be reactivated, queried, or repurposed

### Why this matters

Storage limitation is often implemented as a **policy intention**, not a technical rule.
As a result, retention depends on manual clean-up or organisational discipline.

### Technical addressing

Each VI is inseparably bound to a **Compliance/Jurisdiction Token (CJT)** that encodes:

- the permitted purpose
- a **hard expiry timestamp**

Once the CJT expires:

- the system **cannot** continue processing using that identifier
- access fails automatically
- reuse is blocked before execution

### Result

Retention is no longer discretionary.
It becomes **technically enforced**, directly supporting storage-limitation obligations.

## Problem C — Purpose creep (order data reused for marketing or profiling)

### What goes wrong today

In many systems:

- the same account identifier is reused for fulfilment, analytics, marketing, and profiling
- purpose separation exists only in documentation or database flags
- developers can repurpose data without changing identifiers

•

**Why this matters**

This enables silent drift from:

“order fulfilment” → “customer insights” → “behavioural profiling”

even when no new legal basis exists.

**Technical addressing**

The CJT encodes **explicit purpose binding**:

- e.g. `order_fulfilment`, `returns_processing`, `fraud_prevention`

Processing is permitted **only if**:

- the declared execution context matches the purpose encoded in the CJT

Any attempt to reuse the same identifier for a different purpose:

- fails validation
- is blocked before execution

**Result**

Purpose limitation is enforced **at the moment of use**, not merely at collection.

## Problem D — “Last-minute consent” and deceptive design during checkout

**What goes wrong today**

Common patterns include:

- guest checkout initially offered
- account creation suddenly required at payment
- additional data collected under time pressure
- consent bundled with transaction completion

**Why this matters**

This undermines genuine user choice and inflates data collection beyond necessity.

**Technical addressing**

The system defaults to:

- **guest checkout using a Purchase-VI**

Additional features (accounts, saved preferences, loyalty benefits):

- are technically separate
- require issuing a **new VI with a different CJT**
- must be activated through an explicit, separate choice

**Result**

Users complete purchases without forced identity escalation.
Additional data collection becomes an **opt-in feature**, not a technical prerequisite.

## Problem E — Automated logic drifts into higher-risk processing

**(Expanded explanation of ALF)**

**What goes wrong today**

Modern e-commerce systems rely on automated logic for:

- fraud checks
- eligibility decisions
- recommendations
- risk scoring

Over time:

- algorithms evolve
- thresholds change
- new features are added
- logic becomes more invasive

From a compliance perspective:

- it becomes difficult to know **whether the logic being executed still matches the original purpose**
- auditing often happens **after** harm has occurred

# What ALF Is — Brief Explanation

## ALF (Algorithmic Logic Fingerprint)

An **Algorithmic Logic Fingerprint (ALF)** is:

a cryptographic fingerprint of **approved execution logic for a specific purpose**, not of source code, data, or models.

In simple terms:

- The system computes a **unique, non-reversible fingerprint** of the logic class that is allowed to run for a given purpose (e.g. "fraud eligibility check").
- This fingerprint represents **what kind of logic** is allowed—not how it is implemented.

Importantly:

- **Source code is never disclosed**
- **Models, weights, and parameters remain proprietary**
- Regulators do not inspect algorithms

# How ALF Works at Execution Time

1. A purpose is approved (e.g. "fraud prevention at checkout")
2. The corresponding execution logic class is fingerprinted once
3. The CJT references the allowed ALF
4. At runtime, before execution:
    - the system checks whether the logic being invoked matches the approved ALF
5. If it matches → execution proceeds
6. If it does not → execution is **blocked before processing**

This check is:

- automatic
- binary (yes/no)
- performed before any output is produced

## Why ALF Matters for Purpose Limitation

ALF ensures that:

- a fraud check cannot silently evolve into behavioural profiling
- a return-eligibility rule cannot be reused for marketing segmentation
- logic changes that increase risk require **explicit re-authorisation**

This enforces **purpose limitation at the level of execution**, not documentation.

### Resulting Effect (Problem E Addressed)

- Automated systems remain auditable without revealing trade secrets
- Logic drift becomes technically detectable
- Higher-risk processing cannot occur "by accident" or through incremental changes

## Summary of Section 7

Across all five problems, the common improvement is that:

**Legal principles are enforced at execution time, not merely asserted at policy level.**

- VI limits identity persistence
- CJT enforces purpose, scope, and expiry
- ALF ensures that **only approved logic executes for approved purposes**

This makes compliance **systemic, predictable, and verifiable**, rather than reactive.

# 8 - Overall Conclusion

The Recommendations emphasise that mandatory account creation is generally unjustified for one-time sales and that guest purchase options represent a privacy-by-default approach. The implementation pattern described above illustrates how e-commerce services can achieve order fulfilment, returns handling, limited fraud controls, and user convenience **without forcing persistent accounts**, by enforcing necessity and purpose limitation at execution time through purpose-scoped identifiers (VI), purpose/expiry tokens (CJT), and logic-fingerprinting (ALF). This supports consistent application of Articles 5, 6, and 25 GDPR in automated environments.

# 9) GDPR Articles Satisfied — Implementation Mapping (VI + CJT + ALF)

### Table 1 — Mapping of Technical Controls to GDPR Articles

| GDPR Article | GDPR Principle / Obligation | Technical Mechanism | How Compliance Is Enforced |
|---|---|---|---|
| **Art. 5(1)(a)** | Lawfulness, fairness, transparency | CJT (purpose + expiry) | Processing is permitted only if a valid CJT exists for the declared lawful purpose |
| **Art. 5(1)(b)** | Purpose limitation | CJT purpose binding + ALF | Reuse for a different purpose fails cryptographically before execution |
| **Art. 5(1)(c)** | Data minimisation | Transaction-/session-scoped VI | No persistent identifier exists beyond what is strictly necessary |
| **Art. 5(1)(e)** | Storage limitation | CJT expiry enforcement | Post-expiry access or reuse is technically blocked |
| **Art. 6(1)** | Lawful basis | CJT encodes legal basis (contract, consent, legitimate interest where applicable) | Execution requires the corresponding basis token |
| **Art. 7** | Conditions for consent | CJT issuance / revocation | Withdrawal invalidates the CJT immediately |
| **Art. 12–14** | Transparency | Deterministic purpose scopes | System behaviour is predictable and auditable |
| **Art. 25** | Privacy by design & by default | Guest-mode + scoped VI | Persistent accounts are not the default |
| **Art. 30** | Records of processing | Validation receipts (non-identifying logs) | Machine-verifiable evidence of purpose-bound execution |
| **Art. 32** | Security of processing | Fail-closed execution checks | Unauthorised processing cannot occur |
| **Art. 44–49** | International transfers | CJT scope restrictions | Execution outside permitted scope is blocked |

# 10) Real-World Examples — Execution Flow and GDPR Alignment

### Table 2 — Example-by-Example GDPR Mapping

| Example | Operational Need | Technical Pattern | GDPR Articles Satisfied | Why This Meets the Recommendations |
|---|---|---|---|---|
| **1. One-time purchase (guest checkout)** | Fulfil a single order | Purchase-VI + CJT (order fulfilment, expiry) | Art. 5(1)(b), 5(1)(c), 5(1)(e), 25 | No persistent account; identifier expires automatically |
| **2. Returns / warranty** | Handle post-sale rights | Return-VI + CJT (returns) + ALF | Art. 5(1)(b), 6(1)(b), 25 | Enables returns without identity persistence or reuse |
| **3. Subscription** | Repeated access | Subscription-VI + CJT (subscription access) | Art. 6(1)(b), 5(1)(e), 25 | Account necessity is limited to the subscription term |
| **4. Exclusive offers** | Access control | Member-VI + CJT (eligibility-bound) | Art. 5(1)(a), 5(1)(b) | Prevents misuse of "account creation" as a pretext |
| **5. Fraud prevention** | Risk control | Fraud-VI + CJT (fraud) + ALF | Art. 5(1)(b), 5(1)(c), 32 | Fraud checks without behavioural profiling |

# 11) Why This Directly Supports Recommendations 2/2025

The **European Data Protection Board Recommendations 2/2025** emphasise that:

- mandatory accounts must be **necessary**, not convenient;
- guest access is the **privacy-by-default baseline**;
- retention and reuse risks increase with identity persistence.

The implementation pattern described here shows **how these principles can be enforced technically**, not merely documented:

- **Necessity** is enforced at execution time (no CJT → no processing).
- **Purpose limitation** is enforced cryptographically (purpose mismatch → execution blocked).
- **Storage limitation** is enforced by expiry (no human discretion).
- **Guest checkout** remains fully functional without creating a shadow identity infrastructure.

This addresses the core concern identified by the Recommendations:
that account creation is often used as a *technical shortcut*, rather than a legal necessity.

# Before vs After — Impact of Protocol-Level Enforcement (VI + CJT + ALF)

### Table — Operational Reality Without vs With Execution-Time Enforcement

| Dimension | Before (Policy / Application-Layer Enforcement) | After (Protocol-Level Enforcement) |
|---|---|---|
| **Account creation** | Default requirement, even for one-time purchases | Optional; guest mode fully functional |
| **Identity persistence** | Long-lived account identifiers reused across contexts | Transaction- or session-scoped Virtual Identities (VIs) |
| **Data minimisation** | Depends on design choices and UI discipline | Enforced by scoped identifiers |
| **Purpose limitation** | Declared in policies; enforced post-hoc | Enforced at execution time via CJT |
| **Purpose creep risk** | High — identifiers easily reused | Low — purpose mismatch blocks execution |
| **Retention control** | Manual or policy-based deletion | Automatic expiry via CJT |
| **"Orphaned" accounts** | Common; data remains exploitable | Technically inaccessible after expiry |
| **Consent handling** | Often bundled or late in checkout | Separate, explicit, purpose-specific |
| **Fraud prevention** | Relies on persistent tracking | Uses purpose-limited Fraud-VI |
| **Automated logic changes** | Hard to detect; audits after the fact | ALF blocks unauthorised logic execution |
| **Algorithm transparency** | Requires documentation or audits | Verified without inspecting source code |
| **Trade secret exposure** | Risk during regulatory inspection | None — only fingerprints verified |
| **Compliance assurance** | Probabilistic, audit-driven | Deterministic, execution-gated |
| **Error handling** | Remedial (after misuse) | Preventive (fail-closed) |
| **Cross-context linkage** | Easy and often implicit | Cryptographically prevented |
| **Developer discretion** | High; rules can be bypassed | Low; protocol rules are binary |
| **User trust** | Dependent on privacy notices | Anchored in system behaviour |
| **Regulatory verification** | Retrospective, document-based | Real-time, technical, non-identifying |
| **Scalability of compliance** | Costly as systems grow | Constant-time, scalable |
| **Privacy by default (Art. 25)** | Design aspiration | Technical default |

**Before protocol-level enforcement**, compliance relies primarily on policies, UI design, and organisational discipline. Legal principles are asserted, but enforcement often occurs after data has already been collected, reused, or retained.

**After protocol-level enforcement**, the same legal principles are translated into **execution-time technical conditions**:

- **Virtual Identities (VI)** limit identity persistence
- **Compliance/Jurisdiction Tokens (CJT)** enforce purpose and expiry
- **Algorithmic Logic Fingerprints (ALF)** prevent unauthorised logic execution

As a result, unlawful or disproportionate processing becomes **technically impossible**, not merely prohibited by policy.

# 12) Closing Clarification

This contribution does **not** argue against account creation where it is genuinely required (e.g. subscriptions).
It demonstrates that **where accounts are not necessary**, e-commerce systems can still meet operational needs **without default identity persistence**, by enforcing necessity, purpose limitation, and retention **at the moment of execution** rather than retrospectively.

# Gratitude

The author expresses sincere gratitude to the **European Data Protection Board** for initiating and conducting the public consultation on **Recommendations 2/2025 — Account Creation on E-Commerce Websites**.

The Recommendations demonstrate the EDPB's continued leadership in translating the GDPR's foundational principles—necessity, proportionality, data minimisation, storage limitation, and privacy by design and by default—into clear and actionable guidance for contemporary digital services. In particular, the emphasis on guest access as a privacy-protective default for one-time transactions reflects a careful, experience-based understanding of both user rights and real-world system design.

The author is grateful for the EDPB's openness to technically grounded implementation perspectives and for its sustained engagement with evolving digital architectures, automation, and software-driven decision-making across the Union.

# Acknowledgements

This contribution is grounded first and foremost in the **European Union's own legal, regulatory, and institutional framework**, and in the extensive work already carried out by EU institutions. In particular, it builds upon:

- the GDPR and its authoritative interpretation through guidance and recommendations issued by the **European Data Protection Board**;
- the enforcement practice and practical experience of national supervisory authorities across Member States;
- the jurisprudence of the **Court of Justice of the European Union**, which has consistently underscored the need for effective, not merely formal, protection of fundamental rights;
- the policy, technical, and regulatory work of the **European Commission** in shaping a coherent and future-proof digital regulatory environment.

In addition, the author acknowledges the role of **open research papers, publicly available technical literature, and academic work**—including EU-funded research and independent peer-reviewed studies—which have explored practical methods for enforcing purpose limitation, minimisation, and accountability in automated systems. These open research contributions provide valuable implementation insights and help bridge the gap between legal principles and system-level design, while remaining subordinate to EU law and institutional guidance.

The technical patterns described in this submission are not presented as new regulatory concepts, nor as alternatives to EU guidance. They are offered solely as illustrative examples of how the principles already articulated by EU institutions may be enforced more consistently at execution time in modern, automated e-commerce systems.

Any value in this contribution derives from the strength, clarity, and maturity of the European Union's existing data protection framework. Responsibility for any errors, omissions, or misinterpretations rests entirely with the author.

# About the Author

The author is an **independent technologist and inventor from Balasore town based in India**, working on **protocol-level mechanisms for enforcing lawful purpose, jurisdictional scope, and execution constraints** in digital systems, including financial infrastructure, digital identity, data processing, and automated compliance environments.

This work reflects **369 days and 9 hours of focused research and development** on protocol-level enforcement architectures designed to make legal obligations—such as those arising under the GDPR and related EU frameworks—**technically enforceable by design rather than post-hoc**.

The technical concepts referenced in this annex derive from **patent-pending research published through the World Intellectual Property Organization (WIPO)** and are shared solely to provide **implementation-level context**.

Relevant international patent publications include:

- **WO 2025/210622**
- **WO 2025/210623**
- **WO 2025/215626**

These publications are publicly accessible via WIPO Patentscope and Google Patents and are referenced **for transparency only**.

This submission does **not** request endorsement, adoption, or regulatory action, and does **not** imply that any specific intellectual property should be incorporated into EU legislation or implementing measures.

# Licensing and Access Commitment

### 1. Scope of the Commitment

Upon grant of the relevant patent applications and patent families, the inventor makes the following advance commitment regarding access to the patented technology described in this submission and its associated annexes.

This commitment is made in good faith to support lawful, secure, and interoperable digital systems, while preserving incentives for innovation and responsible commercial deployment.

### 2. Royalty-Free Commitment for Sovereign, Non-Commercial Use

The inventor commits that, upon grant, the patented technology shall be made available on a **royalty-free basis** for **sovereign, public-interest, and non-commercial use** by:

- national governments,
- EU institutions and bodies,
- public authorities and regulators,
- central banks and public payment infrastructures, and
- publicly funded research, supervisory, or regulatory initiatives,

where such use is **non-commercial in nature** and undertaken in the exercise of public functions, including but not limited to regulatory compliance, supervision, enforcement, public digital infrastructure, and public-sector services.

This royalty-free commitment is intended to ensure that **public authorities may adopt or reference the technology without financial or licensing barriers**, subject to applicable laws and technical conditions.

**3. FRAND Licensing for Commercial and Private-Sector Use**

For commercial, private-sector, or profit-generating use, the inventor commits to make the patented technology available under Fair, Reasonable, and Non-Discriminatory (FRAND) licensing terms, upon grant of the relevant patents, with the FRAND commitment referenced to the priority date of August 2025.

FRAND licensing shall apply, without limitation, to use by:

- private enterprises,
- technology providers,
- platform operators,
- financial institutions, and
- other commercial entities deploying the technology in products or services offered on a commercial basis.

**4. Priority and Reference Date**

For the avoidance of doubt, the **priority reference date for this licensing commitment is August 2025**, corresponding to the earliest international priority filings of the relevant patent family.

This commitment applies consistently across national, regional, and international phases of the patent applications deriving from that priority date.

**5. No Obligation to Adopt or Endorse**

This licensing commitment:

- does **not** request, require, or imply adoption by any authority,
- does **not** constitute an endorsement request,
- does **not** create any obligation on regulators, institutions, or market participants, and
- does **not** affect existing legal, procurement, or competition rules.

**It is provided solely to clarify access conditions in the event of voluntary adoption or reference.**

**6. Preservation of Legal and Institutional Autonomy**

Nothing in this commitment shall be interpreted as:

- limiting sovereign regulatory discretion,
- constraining supervisory or enforcement powers, or
- affecting the application of Union or national law.

All use remains subject to applicable legal, technical, and governance frameworks.