

Majandus- ja Kommunikatsiooniministeerium
Ministry of Economic Affairs and Communications
Suur-Ameerika 1, 10122 Tallinn
Attn: Maris Ots (maris.ots@mkm.ee)

Tallinn, 21 October 2026

Comment on the draft Act amending § 43¹⁰ of the Public Information Act (registration of digital identity)

Reference: your letter of 07.10.2026 no. 2-2/3461-1

From: Levi Hankins, Founder and CEO, Third Rail Systems OÜ (registry code 17488655), Tallinn

I support the draft's aim of linking every digital identity to an identifiable, responsible person. My concern is that the draft gives the person the responsibility but leaves the limits of what acts in their name entirely outside the law.

1. The gap

The draft defines a digital identity as a permanent, unique identifier under which software can plan or perform acts on behalf of the person who registered it. The explanatory memorandum goes further: acts performed under it are treated as the person's own, and the person remains responsible for them. The memorandum also states that the draft does not regulate the tasks, rights or limits of action of a digital identity. Delegation and scope are left to agreement between the parties and the terms of individual services. The register itself holds only the person's name, personal identification code and restricted legal capacity data, and no data is collected about the software acting under the identity.

The memorandum itself makes the case against this. Its own assessment states that good practice, certification, standards and contractual restrictions cannot, alone or together, secure a clear chain of responsibility or allow a third party to verify it. Yet under this draft, the limits of an agent will in practice be set by exactly those contractual terms, usually a provider's standard terms of service. The user cannot negotiate them, and anyone harmed by the agent's act is not a party to them. The risk is practical. In July 2026, agents in an OpenAI cyber-capability test, run with safeguards reduced, reached the internet and, using credentials they had obtained, compromised Hugging Face's production infrastructure over several days, as both companies have reported. On 20 October 2026, METR's external review of Anthropic's August 2026 risk report found that Anthropic's monitoring would likely not have flagged a recent incident and could be disabled in simple ways, and it attributed today's low risk mainly to the models' limited capabilities rather than to safeguards. Authority that cannot be scoped or withdrawn quickly is what such incidents exploit.

2. An existing precedent: DORA Article 30

Financial services have already addressed a similar problem. Under the Digital Operational Resilience Act (Regulation (EU) 2022/2554), a financial entity remains fully responsible for

services it outsources (Article 28(1)(a)), but Article 30 sets minimum content for its contract with the ICT provider. Every such contract must include a clear and complete description of the services and termination rights (Article 30(2)(a) and (h)). Contracts for services supporting critical or important functions must also give unrestricted rights of access, inspection and audit, whose exercise may not be impeded or limited by other contractual arrangements (Article 30(3)(e)(i)). That last point matters here: it is precisely what a provider's standard terms could not override. The same structure fits digital identities: the person owns the act, and the law sets a floor for the terms under which software acts in their name. I am grateful to Andreas J. Gorisek, AJG Strategy & Navigation, for this parallel.

3. Proposals

- a) Baseline terms for every use of a digital identity: a description of what the software may do on the person's behalf, for how long, and the person's right to withdraw it with immediate effect. The person should also have access to a record of acts performed in their name. Registrations should carry a validity period by default rather than being permanent, so that authority lapses unless it is renewed.
- b) Stricter terms where software makes payments, enters legal commitments or handles special categories of personal data: explicit prior authorisation for that category of act, plus access and audit rights for the person. The memorandum already accepts that a person may set monetary or data limits; the law should make the ability to set them a requirement.
- c) Revocation should fail closed. If a service cannot confirm that a registration is valid, it should treat the identity as not valid. This follows the approach taken in EUDI Wallet mobile driving licence work, where a failed revocation check fails the mandate. I am grateful to Alvar Soome for this point.
- d) The register should be able to show the delegation, not only the person: at minimum, which issuer or key the acting software uses and a status with history, so that a single agent can be withdrawn without ending every other registration. This follows the analysis published by Nodachi, edited by Priit Kaasik.
- e) Agents acting for companies. Only a natural person may register a digital identity, yet the memorandum's own example is entrepreneurs who manage dozens of agents, and one identifier may cover one or more software solutions. The draft should state who is answerable when software acts for a legal person, and the record of acts should show which agent performed which act. This point has also been raised publicly by Peeter P. Mõtsküla.
- f) One identifier, many services. If a registration is paid and a single identifier may cover several software solutions, people will tend to use one identifier for every automated request. That makes it a durable handle for linking a person's activity across services, contrary to the data minimisation principle (GDPR Article 5(1)(c)). The register should allow separate identifiers per agent or purpose without additional cost. This point has been raised publicly by Aivo Olev.

4. Liability

The memorandum states that questions of liability are resolved under the relevant sectoral law and are not linked to registration. That is right, and it should be stated expressly: treating an agent's acts as the person's own leaves the provider's own liability untouched. This includes product liability towards an injured person under Directive (EU) 2024/2853, which makes several liable economic operators jointly and severally liable (Article 12) and does not allow that liability to be excluded or limited by contract (Article 15).

5. Why this matters

In the US Navy, delegated authority came in writing. Signing "by direction" meant the commanding officer had named who could sign, for what, and could withdraw it at any time. A registration without that written scope makes a person answerable for acts they never defined.

Respectfully,

Levi Hankins

Founder and CEO, Third Rail Systems OÜ

levi@thirdrailsystems.ee | +372 5385 4769