

An Estonian Databanking Pilot

A proposal to test custodial separation on Estonia's existing data infrastructure

Dr Dan Protopopescu, University of Glasgow, Scotland, UK | databanking.org | October 2026

— Concept note

Databanking is a proposed model for regulated personal-data intermediation in which personal data remains under the custodial control of trusted intermediaries, while approved computations are brought to the data and only authorised, policy-constrained outputs are released.

The central insight is simple: organisations frequently do not need a copy of a person's underlying data. They need an answer derived from it.

Estonia has already built much of what such a model requires. X-Road lets institutions query one another's registries instead of replicating them. The once-only principle obliges the state to ask a person for any given fact a single time. Strong electronic identity is in everyday use, and the Data Tracker on the state portal shows people which institutions have accessed their records. What Estonia has not yet built is the step that keeps a record from being copied when it crosses into the private sector. When a person authorises a company to use state-held data through the consent service, the data is transferred to that company, which from then on holds its own copy.

This proposal suggests a **bounded Estonian pilot that aims to replace such transfers with queries**. The record would be held by a licensed custodian of the person's choosing, the relying company would submit its computation to that custodian, and only the permitted result would be returned. The pilot is designed to test, on infrastructure that already works at national scale, parts of the proposed Databanking model that have not been tested by any existing system: a custodian independent of both the source registry and the relying company, more than one such custodian competing for accounts, portability between them, and a share of each access fee returned to the person whose data was queried.

The model is described in the Databanking whitepaper:

<https://doi.org/10.2139/ssrn.6992518>

with further material at <https://databanking.org>.

— 1. What Estonia already has

X-Road. The state data-exchange layer, in production since 2001 and operated by the Information System Authority (RIA), connects public and private institutions so that registries are queried where they sit rather than copied into every system that needs them. It is [federated with Finland's Suomi.fi Data Exchange Layer](#), and its software is maintained by the Nordic Institute for Interoperability Solutions, whose members are Estonia, Finland and Iceland.

The once-only principle. The state asks a person for a given fact once, and draws on the registry that holds it thereafter.

Electronic identity. Strong authentication by ID card, Mobile-ID or Smart-ID is routine, and binds each transaction to the personal identification code.

The Data Tracker. Available on eesti.ee since 2017, the [Data Tracker](#) shows a person which institutions have accessed their data in the registries that implement it. In 2025 the Chancellor of Justice found that state agencies had accessed residents' bank account information through the enforcement register without a proper legal basis. The government [responded by bringing those enquiries into the Data Tracker](#), and at the end of 2025 the Ministry of Justice and Digital Affairs [proposed amending the Public Information Act](#) to make the Data Tracker mandatory for nearly all public information systems holding personal data. At that point 15 of more than 300 such systems used it.

The consent service. Developed by RIA from 2020 and in use since the end of 2021, the [consent service](#) lets a person authorise the state to release a defined set of their data to a named company. Datasets offered include tax data from the register of taxable persons, health insurance status and prescription records. Its first financial use was a solvency check against Tax and Customs Board records for instalment credit, and by May 2024 [about a fifth of Estonian adults](#) had used the service. At its launch the Government Chief Data Officer said that people “[will have the opportunity to charge a fee for the use of their data if they so wish](#)”.

These are the technical and civic foundations of the Databanking model, operating at national scale: querying in place, identity binding, a citizen-visible access log, and release of data initiated by the person it concerns. RIA groups the consent service and the Data Tracker under the heading of people-centred data exchange, which this proposal extends.

— 2. What it does not yet have

Within the state, each registry still holds and uses its own data. X-Road federates access between institutions that are both the custodians of their records and the parties that analyse them. The pilot leaves this arrangement untouched and concerns only the boundary with the private sector.

At that boundary the consent service ends in a transfer. Once a person consents, the state-held data is released to the company, which then holds a copy under its own retention policy and its own security. A person who applies for credit with three lenders creates three copies of the same tax record. The consent service logs each transfer, but no log can follow a copy after it has left.

Nor is there a custodial market. There is one state layer, no competing custodians, no account to move between them, and no mechanism by which part of the value of an access returns to the person whose data was accessed. The fee envisaged in 2021 is one of the things the pilot would test directly.

— 3. The proposition

The pilot would introduce one new institution, a licensed custodian or **Databank**, and route a single class of transaction through it.

1. The individual opens an account with one of the pilot Databanks, authenticating with Estonian eID.
2. On the individual's instruction, the relevant record is released once, over X-Road, into that account. The consent service already provides this mechanism. The only change is the recipient: a custodian the individual chose, instead of the company that will rely on the answer.
3. A relying company that needs a decision submits its computation to the Databank, not a request for the record. The Databank checks the request against the individual's permissions, runs the computation in an isolated environment where it alone meets the record, and returns only the permitted result.
4. Every query appears on the individual's account statement and, through the Data Tracker protocol, on eesti.ee alongside every other access to their data.
5. The relying company pays an access fee, and a fixed share of it is credited to the individual.

The Databank never analyses what it holds. It keeps the record, enforces the individual's permissions, executes approved computations and releases bit-scarce results under an auditable leakage budget, and it earns revenue from custody and authorised access alone. The individual can move the account to the other pilot Databank at any time, on a standardised account schema, without the record passing through any relying company.

Every element of this flow except the custodian already exists in Estonian production infrastructure.

— 4. Why Estonia

The value of a pilot lies in testing the assumptions most vulnerable to failure. For Databanking these are institutional and economic: whether individuals will entrust a record to an independent custodian, whether relying organisations will accept an answer in place of the record, whether custodians can compete and accounts can move between them, and whether a custodian can sustain itself without exploiting what it holds.

In most jurisdictions, much of a pilot's budget would go into building what Estonia already runs: a data-exchange layer, identity binding, authoritative source registries, and a channel through which a person can release state-held data. In Estonia these exist, are trusted and are used daily, so the resources of a pilot there can be concentrated on the parts of the model that no existing system tests.

Estonia also brings a civic habit that elsewhere would have to be built from nothing. Its residents have been able to see on the state portal who accessed their records since 2017, and the state's response to misuse has been to extend that visibility. A Databank account statement listing every query and its result would extend something already familiar to Estonians.

At about 1.36 million people, with a compact set of institutions that already cooperate across the public and private sectors on X-Road, Estonia is of a scale at which a bounded infrastructure experiment is meaningful and its results legible.

Finally, Estonia is a Member State of the European Union. A demonstrator there would operate directly under the GDPR, the Data Governance Act, the European Digital Identity framework and the Consumer Credit Directive, so the results would bear on EU law as it stands, and on

the amendments now before the co-legislators. Because Estonia's X-Road is federated with Finland's, a cross-border phase is also available without new infrastructure.

— 5. A lead use case: affordability for consumer credit

The initial transaction should be selected jointly with the participating organisations and regulators. One candidate fits Estonian conditions closely enough to be proposed as the starting point.

Under the Creditors and Credit Intermediaries Act and the principle of responsible lending, Estonian lenders must verify a borrower's income before granting credit. From 20 November 2026 the revised [Consumer Credit Directive \(EU\) 2023/2225](#) requires the creditworthiness assessment across the EU to rest on "relevant and accurate information on the consumer's income and expenses" that is "necessary and proportionate" to the credit, verified where necessary against independently verifiable documentation. Today an Estonian lender can meet this duty by obtaining the applicant's tax data, through the consent service or otherwise, and deriving the affordability decision itself.

In the pilot the same transaction runs inside a Databank:

- the applicant's income record from the Tax and Customs Board is held in the applicant's Databank account;
- the lender submits its affordability rule as a computation, parameterised by the requested amount and term;
- the computation runs inside the Databank against the income record;
- the lender receives only whether the requested credit satisfies its rule, and holds that result no longer than the decision requires;
- the Databank's audit ledger records the query, the computation and the result, so that the assessment can be evidenced to the supervisor without the lender retaining the record.

The baseline already exists: the same transaction runs today through the consent service with a full transfer of the record, so the pilot can compare answer against record directly, with the same lenders and comparable applicants, rather than against a hypothetical. The relying organisations are supervised and under a legal duty to verify, so the regulatory question is precise: can the supervisor accept a Databank result, and the Databank's audit record, as discharging that duty? Income is the standard target for leakage, since repeated affordability queries at different amounts would progressively narrow the income on which they depend, and the pilot would test the leakage budget on exactly the class of query that most needs one. The transaction carries enough value to support a fee, so the economics and the individual's share can be measured on real terms. And both sides can see the benefit: the applicant discloses less, and the lender holds less personal data that it must secure, retain and eventually delete.

Other Estonian candidates remain open: age and eligibility attestations drawn from the population register, health-insurance and prescription data for private health providers (two datasets already offered through the consent service), and research access to health records, the most institutionally demanding of them.

— 6. The pilot ecosystem

A realistic Databanking transaction involves four roles. Three are already filled in Estonia; the pilot adds the fourth, with two custodians rather than one.

The individual, an Estonian resident holding eID, who opens a pilot account, chooses the custodian and authorises queries.

The authoritative data provider, here the Tax and Customs Board, which releases the income record into the individual's account over X-Road at the individual's instruction.

Two Databanks, licensed for the duration of the pilot, admitted as X-Road members, implementing the Data Tracker protocol, and bound by the custodial duties set out in the whitepaper: no analysis of what they hold, revenue from custody and authorised access only, a standardised account schema, and portability on request. The whitepaper allows a Databank to be a commercial company, a non-profit or a state-backed institution. The pilot custodians may take any of these forms, provided each is independent of both the source registry and the relying organisations.

The relying organisations, two or more lenders who agree in advance to accept a Databank result in place of the record.

Above these sits the governance layer: the Ministry of Justice and Digital Affairs for policy; RIA as operator of X-Road, eesti.ee, the consent service and the Data Tracker; Finantsinspektsioon, the Financial Supervision and Resolution Authority, for the lenders; the Data Protection Inspectorate; and an independent auditor. Which authority licenses and supervises the custodians themselves is settled in the first phase.

Two custodians are the minimum at which choice, switching and portability on a common schema can be observed in practice. Estonia's infrastructure keeps the cost of the second one low, since both connect to the same exchange layer, the same identity system and the same source registry.

— 7. Solving the initial adoption problem

Databanking has an inherent multi-sided network problem. Individuals have little reason to open an account until organisations accept its answers, organisations have little reason to integrate until enough individuals hold one, and data providers have little reason to build interfaces before either.

In Estonia two of the three sides are already connected. The source registry offers its data over X-Road through the consent service, and lenders already use that service in credit applications. The pilot therefore needs to add only the custodian and a closed group of participants: lenders that agree in advance to accept a defined Databank output, and a bounded cohort of applicants recruited at the point where the consent service already appears in the lender's application. An applicant at that step can be offered the choice between releasing the record to the lender and holding it with a Databank, which also gives the pilot a natural comparison group.

— 8. What the pilot would test

The pilot would test four forms of viability, weighted towards the institutional and the economic.

Technical viability Largely established by X-Road and Estonian eID. What remains open is narrower: sandboxed execution of a lender's computation inside the custodian, and enforcement of a leakage budget on a continuous value.

Institutional viability Can a custodian independent of both the source registry and the relying company maintain a credible structural separation between custody and exploitation, backed by governance, audit and enforceable duties, and be seen to do so through the same Data Tracker that already covers the state?

Market viability Will individuals choose a custodian, and move between two? Will lenders accept a result in place of the record? Does the individual's share of the access fee matter, and at what level?

Regulatory viability Can the supervisor accept a Databank result, and the Databank's audit record, as discharging a lender's verification and documentation duties? Where would a Databank sit under the Data Governance Act as it stands, and under the Digital Omnibus proposal that would fold its intermediation rules into the Data Act?

— 9. Technical and governance research programme

The demonstrator should sit alongside an interdisciplinary research programme. Estonian infrastructure settles parts of some of these questions and sharpens others, and the last is specific to Estonia.

1. **Query leakage.** Affordability queries at different amounts can bisect the income beneath them. The retention-bounded leakage budget described in the whitepaper, a per-datum quota shared by all Requestors and derived from the short period for which a result may lawfully be held, would be tested on live lending traffic.
2. **Computation scrutiny.** Lenders' affordability rules are proprietary. A rule has to be approved for execution without being disclosed beyond what approval requires, and without becoming a channel for extracting the record.
3. **Correctness and provenance.** Tax data is authoritative but lags current income. The pilot must define how corrections flow back to the Tax and Customs Board, and who is responsible when the source is wrong.
4. **Identity binding.** Largely settled by the personal identification code and strong eID, which frees the pilot to concentrate elsewhere. What remains is authorisation by representatives, and the binding of a lender's application to the right account without the lender learning more than it already holds.
5. **Liability and dispute resolution.** Responsibility has to be allocated among the source registry, the Databank, the lender's computation and the lender itself.

6. **Coercive authorisation.** A lender could make a broader query a condition of credit. The Consumer Credit Directive's proportionality requirement gives the governance model a legal anchor for defining which queries a lender may request.
7. **Concentration and resilience.** With two custodians, breach containment and continuity can be tested directly, including the transfer of accounts if one custodian fails.
8. **Interoperability and portability.** Accounts must move between the two pilot Databanks on a common schema. In a later phase the same test can run across the Estonia–Finland X-Road federation.
9. **Economic sustainability.** The pilot should measure the cost of custody, computation, audit and support against fee income and the individual's share, and set both against what lenders spend today on holding copies: security, retention and deletion.
10. **Audit visibility.** Can a non-state custodian's access log appear on eesti.ee through the Data Tracker protocol, and do people read it? Estonia offers an established baseline of public use against which this can be measured.

— 10. Success criteria

The decisive test is whether three propositions hold at the same time. Individuals are willing to entrust the relevant record to a custodian they chose. Relying organisations accept the minimal authenticated result instead of the underlying record, and their supervisor accepts that they have done so lawfully. The Databanks provide the service on economically sustainable terms while remaining strictly independent of commercial exploitation of what they hold.

Three further criteria are specific to the Estonian design: accounts move between the two custodians on the common schema without loss and without passing through any relying organisation; the individual's share of each access fee is paid and visible on their statement; and every query is visible on eesti.ee.

Secondary measures include the number of record copies that would otherwise have been transferred to lenders, accuracy, latency, dispute and correction rates, the frequency with which leakage budgets bind, integration cost for lenders, and compliance cost. Failure on any of these is itself evidence, and identifies where the model requires modification.

— 11. Proposed programme structure

Phase 1 — Scoping and consortium formation Confirm or replace the lead use case with the Ministry of Justice and Digital Affairs, RIA, Finantsinspektsioon, the Data Protection Inspectorate, the Tax and Customs Board and the participating lenders. Determine the legal basis on which the pilot custodians are licensed and which authority supervises them, and recruit academic partners in law, computer science and economics.

Phase 2 — Architecture and governance design The standardised account schema, integration with X-Road and the consent service, implementation of the Data Tracker protocol, the sandbox and leakage budget, licensing conditions, audit, liability allocation and fee structure.

This phase also settles whether results are best delivered to relying organisations as electronic attestations of attributes presented from the European Digital Identity Wallet.

Phase 3 — Prototype Both Databanks connected to the X-Road test environment, running the affordability query on synthetic data, so that architecture and security assumptions are validated before operational personal data is involved.

Phase 4 — Regulated demonstrator A bounded cohort of applicants, two Databanks and two or more lenders making live credit decisions, collecting technical, behavioural, economic and governance evidence.

Phase 5 — Evaluation and extension decision Evaluate the four forms of viability and decide on extension to further queries, sectors or custodians, and to a cross-border phase with Finland over the federated X-Road.

A successful pilot should lead not automatically to scale-up, but to an evidence-based decision about which parts of the model merit further development.

— 12. Relation to EU law

Data Governance Act. A Databank would provide a data intermediation service between data subjects and data users, and the Act already requires such a service to be provided through a separate legal person and to use the data for no other purpose. The Commission's Digital Omnibus proposal of November 2025 would repeal the Act and carry its intermediation rules into the Data Act, as a voluntary label with functional rather than legal separation. The pilot would generate direct evidence on the question that change reopens: how much separation between holding data and using it is needed before individuals and relying organisations will trust an intermediary. The [comparison with EU data-governance law](#) sets out how far the Act already goes towards a Databank.

European Digital Identity. Each Member State must offer a European Digital Identity Wallet by the end of 2026. Public-sector services must accept it from then, and certain regulated private-sector providers from the end of 2027. [Estonia's wallet](#) is in procurement. A wallet presents attestations already issued, while a Databank computes a fresh answer from the record each time a regulated question is asked. The two are complementary, and the pilot can establish how a Databank result is best carried by the wallet.

Consumer Credit Directive. Its creditworthiness provisions apply from 20 November 2026, and their proportionality test is the legal standard against which the lead use case would be judged.

Interoperable Europe Act. Regulation (EU) 2024/903 and Implementing Regulation (EU) 2025/1420 allow public administrations to establish [interoperability regulatory sandboxes](#) around a clearly defined legal question, with at least three administrations taking part, ideally from different Member States. A cross-border phase linking Estonian and Finnish administrations over the federated X-Road, with a third participating administration, would fit that frame.

— 13. What it would take to start

The only commitments needed at this stage are those that allow the first two phases, scoping and design, to begin. None involves legislation, national deployment or funding.

From the Estonian authorities:

1. A scoping meeting convened by the Ministry of Justice and Digital Affairs with RIA, Finantsinspektsioon, the Data Protection Inspectorate and the Tax and Customs Board, to confirm or replace the lead use case and identify participating lenders.
2. Agreement in principle that two pilot Databanks may join the X-Road test environment, and that the register of taxable persons may offer its consent-based service to an account the individual holds with a Databank, using test data during Phase 3.
3. Agreement in principle from RIA that a pilot Databank may implement the Data Tracker protocol, so that its queries appear on eesti.ee.
4. A named contact at Finantsinspektsioon to examine whether a Databank result and audit record can discharge a lender's verification and documentation duties.

From the European Commission:

1. To forward this proposal to the Estonian counterparts named above.
2. To take the pilot into account as a source of evidence on the separation required of data intermediaries, in the work on the Data Governance Act and the Digital Omnibus.
3. To consider the cross-border phase for an interoperability regulatory sandbox under the Interoperable Europe Act.
4. To offer the same design to other Member States that operate a data-exchange layer, strong electronic identity and a channel for person-initiated release of state-held data.

Can Estonia demonstrate, on infrastructure it already operates, that a lender can make a lawful credit decision based on an answer instead of a record, where the record is held by an independent custodian that the prospective borrower chose and can change?

If the answer can be demonstrated convincingly, the resulting architecture, regulatory treatment and economic evidence would provide a basis for deciding whether Databanking should develop into a broader infrastructure industry, in Estonia and across the Union.

Enquiries: contact@databanking.org