

FinEst Centre
for Smart Cities

Feasibility of Personal Data Spaces in Estonia

Feasibility, value proposition and implementation path

Executive synthesis of the final feasibility report commissioned by the Estonian Ministry of Justice and Digital Affairs, 31 March 2026

*Authors (alphabetical order): Kärt Salumaa-Lepik, Ralf-Martin Soe, Sille Sepp, Taivo Kangilaski
FinEst Centre for Smart Cities, TalTech*



EXECUTIVE SUMMARY

Estonia has a strong foundation for developing personal data space services: a mature digital identity system, secure data exchange infrastructure, established public registries, and early human-centric components such as data tracker and data consent service. However, the study finds that the country has not yet fully translated this technological maturity into a consistently human-centric data economy. Individuals have formal rights over their personal data, but often lack simple, integrated and understandable means to exercise those rights, reuse their data, or see how data are used across organisations, especially in the private sector.

The report defines a **personal data space** not as a single central database or platform, but as a **flexible, federated framework** realised through one or more digital services. Such services should allow a person to manage, control and derive value from their personal data held across multiple organisations. Data should normally remain at source and be accessed through trusted, standardised and auditable mechanisms. A person may use several sector-specific or cross-sector services in parallel.

The central feasibility finding is affirmative but conditional. The required technologies largely exist, and the legal framework does not generally prohibit implementation. The decisive **barriers are economic and institutional**: insufficient commercial incentives, unclear value distribution, fragmented governance, high integration costs, uncertainty about legal roles and data processing grounds, and limited willingness of organisations to share data if it currently provides a competitive advantage. Successful implementation therefore depends less on building new infrastructure than on **creating viable use cases, trust frameworks, cooperation models and sustainable business arrangements**.

The two detailed use cases illustrate different pathways. The case study on **life insurance** describes the potential for more accurate risk assessment and personalised products, but also signals challenges such as processing sensitive health data, significant proportionality and profiling risks, uncertain market scale, and a demanding business case. Another case study on **skills and education data related service** is found technically and legally feasible and could reduce administrative burden while strengthening individual autonomy, but its commercial potential in Estonia is limited; it is more likely to require public leadership and a cooperative ecosystem model.

The report recommends a phased approach for future developments: appoint a clear lead for cross-sectoral coordination; launch pilots in high-value sectors; develop legal guidance, certification and access policies; establish a modular reference architecture aligned with existing national and European components; support private-sector collaboration and experimentation; and scale only after value, trust and interoperability have been demonstrated. The strategic question is therefore not whether personal data spaces are possible, but how to implement them so that **people, organisations and society receive visible and fairly distributed value**.

This following document provides an LLM-assisted synthesis and summary of the full report (available in Estonian) introducing the overall purpose of the study, the concept of personal data spaces, value proposition for individuals and companies, necessary capabilities as well as the role model for a human-centric data ecosystem. The study also explored two beforementioned use cases, which feasibility is presented in a concise manner. The study concluded with key recommendations and roadmap, focused primarily on actions directed towards state authorities, while other necessary actions were also referenced.

The authors would like to thank all interviewed study participants for their insightful contributions as well as representatives of the commissioning organisation for their wide-ranging support.

1. Purpose, Scope and Method

The feasibility study examines how Estonia could advance a **human-centric data economy** and what role **personal data spaces** could play in that development. It asks how people can better understand, manage and benefit from data about themselves while enabling new data-driven services and business models. The analytical focus is deliberately practical: **defining the concept, identifying organisational needs, describing potential use cases, and determining the conditions for implementation in Estonia**. The research questions are provided in Annex 1.

The study intended to concentrate primarily on **private-sector and cross-sector data cooperation**, especially business-to-consumer, business-to-business and business-to-government models. However, several service provisioning and data sharing processes transcend sectoral boundaries already now, as found also in the selected use cases in finance and insurance, and education, skills and labour-market services. These cases were selected as they combine relatively mature data environments with identifiable service needs. The report does not attempt a full macroeconomic impact assessment, an exhaustive review of every relevant legal instrument, or a detailed redesign of national digital infrastructure. Instead, it explores enabling and challenging conditions for implementing personal data spaces, and their use cases, in Estonia.

The evidence base combines **desk research** of academic, policy and legal materials with **18 semi-structured interviews involving 31 experts** from companies, public authorities, civil-society organisations and educational institutions. The team also used **workshops and stakeholder sessions** to test emerging findings, identify risks and refine use cases. The **analysis is qualitative, inductive and iterative**. Its strength lies in detailed stakeholder insight, while the results cannot be statistically generalised. Direct engagement with ordinary citizens was limited, so assumptions about user value and adoption require further validation through future pilots and user research. Furthermore, the digital landscape around digital identity wallets, European data spaces, privacy-enhancing technologies, standardization and data regulation are evolving rapidly. Hence, the report should be treated as a strategic and architectural foundation rather than a fixed (technical) specification.

2. Conceptual Model for Personal Data Spaces

The report starts with a critique of the prevailing organisation-centric data economy. Data processes are commonly designed around institutional goals, while individuals remain passive sources of data and recipients of services. A human-centric model does not reject organisational interests; rather, it seeks a more balanced system in which people can exercise agency, receive value, and understand the consequences of data use. Five principles frame this approach (Lähteenoja 2021):

1. the person as a central integration point across fragmented systems;
2. individual empowerment through practical control and meaningful use of data;
3. an ecosystem perspective that links technology, governance and business models;
4. pluralism across sectors and jurisdictions; and
5. proportional, fair distribution of rights, risks, responsibilities and benefits.

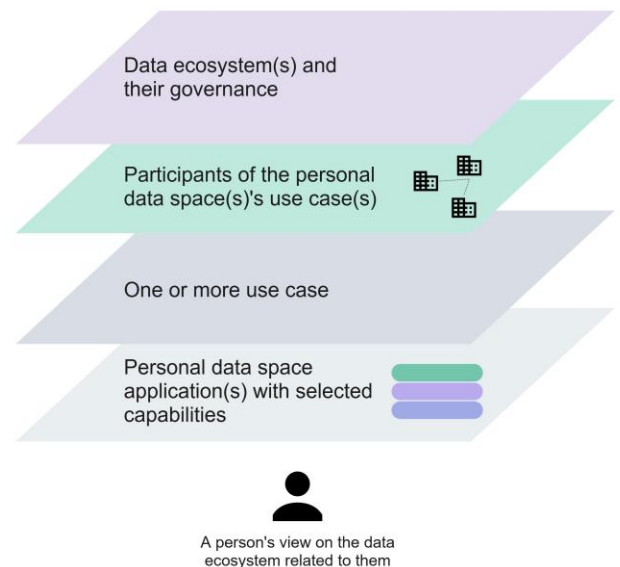
Human-centricity is therefore not a binary property. It must be designed and governed across service, organisational, national and international levels.

Given the diversity of human-centric technology and governance models, the report defines a **personal data space** as...

... a flexible conceptual framework realised through one or more digital services.

Personal data space service, however, is defined as...

... a digital service that enables a person to manage, control and derive value from their data.



This definition has several important implications:

- A personal data space refers to a **flexible conceptual framework**, realised through **concrete use cases and one or more digital services**; different services may cover different sectors and data sources;
- The person may use **several personal data space services in parallel**, provided that they are interoperable and do not create new silos;
- Participation should be **voluntary** and should function as a **convenience and empowerment service** rather than transferring all responsibility to the individual;
- The model should allow **using existing distributed data sources and national digital infrastructure** wherever possible; creating a new central repository is neither necessary nor desirable.
- **Control is broader than consent**. It includes transparent information, purpose and time limits, revocation where applicable, auditability, challenge mechanisms and access to useful services.

The study also stresses that merely making data processing more transparent or collecting consent is insufficient to foster human-centricity. A credible personal data space must demonstrably serve the person's interests. This raises the possibility of **fiduciary or stewardship functions** that go beyond conventional organisational data management. At the same time, service providers need sustainable business models, and essential public services must retain lawful alternatives when consent is not appropriate or is withdrawn.

3. Value Proposition and Organisational Needs

For individuals, the value proposition of personal data spaces consists of four connected outcomes: **greater trust in service providers; stronger agency and freedom to make data-based decisions; a more coherent view of one's digital life; and specific benefits from data use.** These benefits may include convenience, better or more proactive services, new personal insights from one's data, financial savings, and contributions to wider social value. The study's core adoption insight is straightforward: **control alone will not motivate participation.** People must see a clear and proportionate benefit, and the service must be easier and more understandable than existing arrangements.

For organisations, the potential value lies in **improved access to reliable and timely data, more accurate decisions, personalised services, reduced manual verification, innovative data-driven products and services, and better cross-organisational cooperation.** Stakeholder interviews identify a consistent set of **business needs and constraints:**

- Access to trustworthy, timely, sufficiently granular and machine-readable data whose origin can be verified.
- Reduced fragmentation of data, metadata, interfaces and semantic models across organisations.
- Lower costs for integrations, legal agreements, compliance and ongoing operation, particularly for smaller companies.
- Sufficient basis for developing personalised services without requiring excessive collection and storage of personal data.
- Predictable rules for consent, contracts, statutory duties and other legal bases, and clarity on consequences when a permission is changed or withdrawn.
- International scalability and compatibility with European digital infrastructures and regulatory developments, rather than dependence on Estonia-specific solutions alone.

The report finds that organisations often have incentives to retain exclusive control of data because data assets provide competitive advantage. Sharing therefore requires credible value exchange and a fair distribution of costs, risks and benefits. **Data intermediaries and value-added service providers** may help by reducing bilateral integration costs, improving data quality, translating formats, managing permissions and providing analytics. However, these actors also need a sustainable business model.

4. Feasibility Conditions

4.1 Legal and institutional conditions

European and Estonian law provides a strong rights-based foundation, but formal rights do not automatically create practical control. The General Data Protection Regulation (GDPR), the Data Governance Act (DGA), the Data Act (DA), digital identity regulation (eIDAS) and sector-specific rules create a multi-layered environment. The main challenge is not the absence of law, but **applying existing rules consistently** in a multi-party, cross-sector ecosystem.

A key legal insight is that **consent should not be treated as the universal or the most appropriate ground for supporting human-centric data processing**. Consent under the GDPR must be freely given, specific, informed, unambiguous and revocable. It is also legally distinct from mandating data processing (including data sharing) with a contract. Naturally, other legal bases exist, such as protecting vital interests or carrying out a public task. Implementation therefore requires purpose-specific legal design. Public-sector provision may require an explicit statutory basis, while private-sector provision may rely on contractual, consent-based or other lawful grounds depending on the function. Sensitive data, large-scale profiling and automated decisions require heightened safeguards, including data protection impact assessments, proportionality analysis, meaningful human intervention and effective appeal mechanisms.

4.2 Business considerations

Critical business-related drivers for personal data spaces are the existence of viable business incentives and (data) cooperation models. Organisations could benefit from better access to reliable data, lower verification and administrative costs, improved decision-making, and more personalised services. However, investment is constrained by fragmented data, integration and compliance costs, uncertainty around consent-based processing, unclear allocation of responsibilities, and limited willingness to share data.

The appropriate economic model is likely to vary considerably between use cases. Commercial arrangements may include bilateral data transactions, data marketplaces and data- or analytics-as-a-service, while other contexts may depend on open data, trusted intermediaries or broader cooperation-based models.

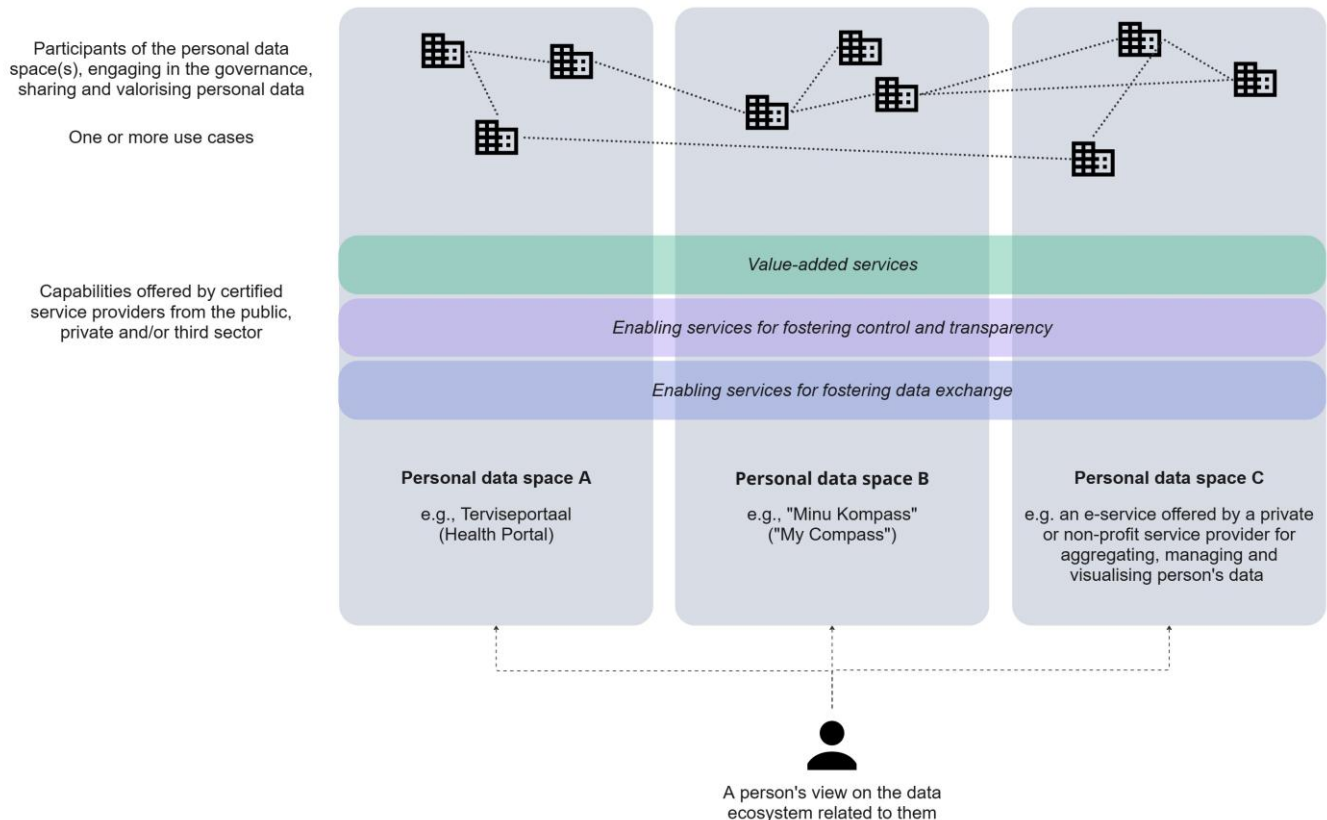
Economic feasibility should consequently be validated through concrete use-case pilots rather than assumed at the level of the overall concept. Each pilot should demonstrate tangible value for individuals and participating organisations, define how costs, risks and benefits are distributed, and assess whether the resulting service can be sustained and, where relevant, scaled beyond Estonia. Public-sector action can reduce early-stage innovation risk by establishing common standards and a predictable trust framework, supporting cross-organisational experimentation, and enabling reusable data-intermediation services. Long-term implementation nevertheless requires the personal data space to be integrated into participating organisations' business strategies rather than treated solely as a technical or compliance initiative.

4.3 Functional capabilities and technical architecture

The report groups the required functional capabilities into three layers. The first two are foundational; the third creates direct user and commercial value.

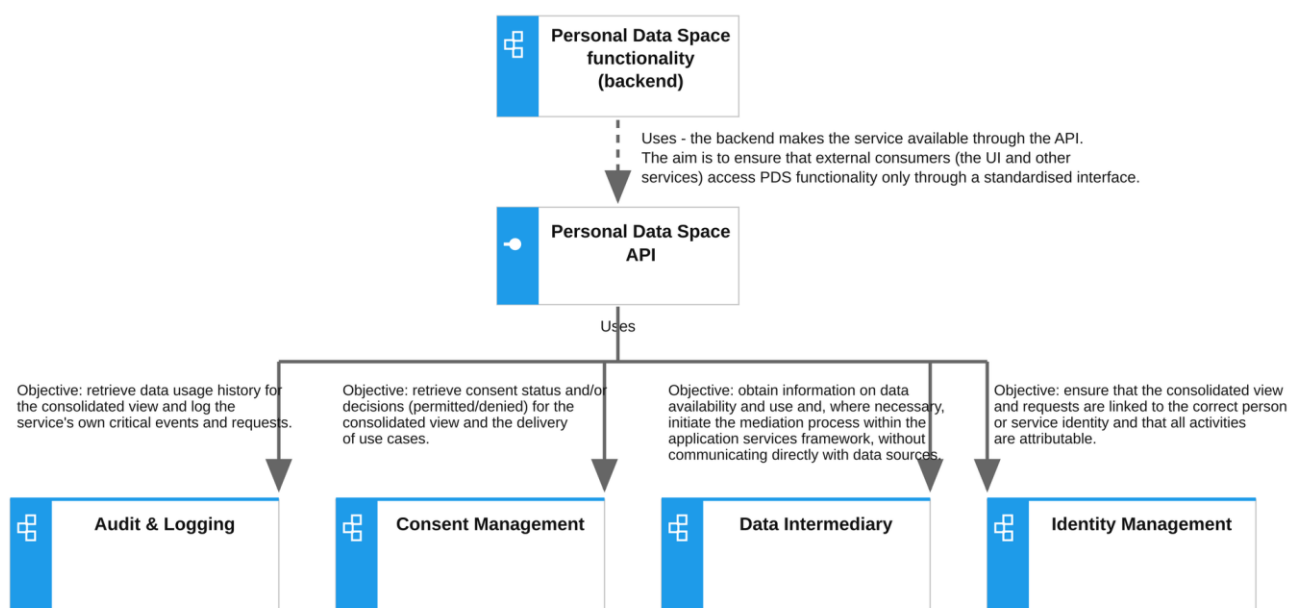
1. **Control and transparency:** rights and permission management, authorisation, access control, consent services, activity logging, audit support, and interfaces through which people and organisations can view and manage data use. Personal storage is optional, not mandatory.

2. **Data exchange and support:** trusted digital identity and authentication, discovery of data providers and consumers, service descriptions, technical enforcement of policies, secure exchange, harmonisation of data models, and governance rules for participation and responsibility.
3. **Value-added services:** understandable data visualisation, analytics and AI-based services, personal data-product management, data enrichment, and mechanisms for exchanging monetary or non-monetary value.



The proposed architecture is modular, federated and API-based. It separates decision-making, execution and evidence, thereby reducing overlap and systemic risk. Five core components are identified:

- **Identity management** validates a cryptographically verifiable identity and role context while relying on existing trusted identity providers.
- **Consent management** evaluates whether a particular request is permitted, considering identity, purpose, scope, recipient and validity period. It returns a machine-readable allow, deny or conditional decision.
- **Data intermediation** enforces the decision and routes requests between data consumers and data holders/providers.
- **Audit and logging** records critical events and decisions through correlation identifiers, timestamps and policy references. Logs contain metadata rather than the underlying personal data.
- **A personal data space interface** presents permissions and data-use history through a common logical access point for users and machine clients without becoming a new data warehouse.



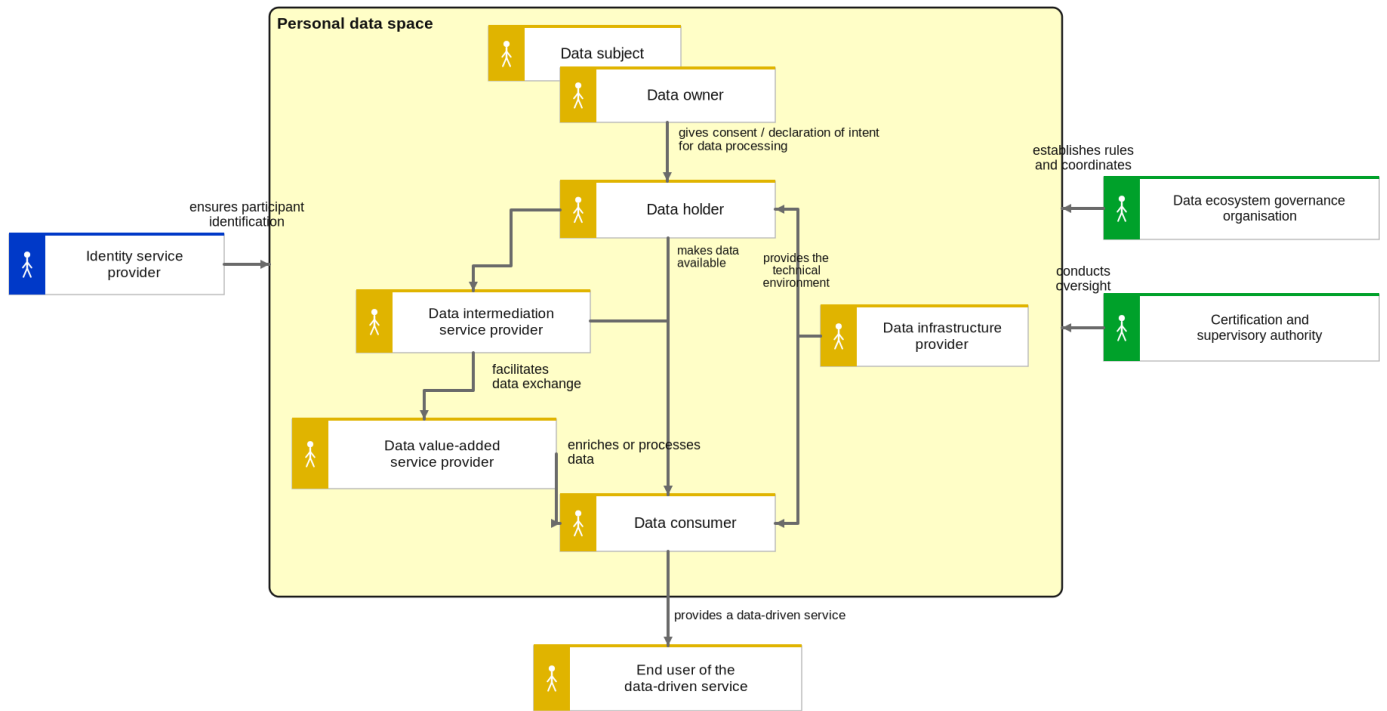
A typical transaction begins with a request, validates identity, evaluates permission, enforces the decision through the intermediary, records the full event chain, and then makes the outcome visible to the individual. The pattern can be implemented through existing components such as eID, X-Road, the national data consent service, digital identity wallets and sector-specific infrastructure, provided that interfaces and trust requirements are standardised.

4.4 Roles and governance

The role model distinguishes three groups:

1. Direct participants include the **data subject or data owner**, the **data holder**, the **data consumer** and the **end-user of the data-driven service**.
2. Supporting roles include **infrastructure providers**, **neutral data intermediaries**, **identity providers** and **value-added service providers**.
3. Ecosystem-level roles include a **governance authority** that sets participation rules and standards, and **independent certification and supervisory bodies** that verify compliance.

An organisation may hold several roles, but the responsibilities must remain explicit. The report considers public leadership important for ecosystem governance and trust, while innovation and service provision can be led by private and third-sector actors.



5. Evidence from Use Cases in Insurance and Education/Skills

The use cases show that personal data spaces do not create value in the abstract. Feasibility depends on the service problem, market structure, legal sensitivity, data quality and the incentives of specific participants.

Dimension	Life insurance	Skills, education and labour market
Primary value	More accurate risk assessment, less manual disclosure, potentially personalised pricing and preventive services.	Verified competence profiles, faster recruitment, reduced document collection, personalised learning and career pathways.
Data involved	Identity, employment, income, health and lifestyle data; potentially highly sensitive and dynamic.	Formal education, qualifications, certificates, employment history, non-formal learning and potentially behavioural learning data.
Business case	Relatively stronger commercial potential, but constrained by Estonia's small market, voluntary demand, insurance mathematics, tax conditions and insurance companies' uneven willingness to share data.	Weak standalone private-sector business case in a small market; stronger public-interest and cooperative rationale.
Legal risk	High: special-category health data, purpose change, proportionality, profiling, automated decisions and likely impact assessment.	Moderate but material: lawful recruitment grounds, purpose limitation, profiling, explainability and discrimination risks.
Overall feasibility	Technically feasible, but commercially and legally demanding.	Technically and legally feasible; likely to require public leadership, standards and ecosystem coordination.

5.1 Life insurance

A personal data space could allow an applicant to authorise time-bound access to verified health and lifestyle data, improving risk assessment and reducing repeated data collection. The business process would remain recognisable, but data access would become purpose-bound, auditable and more transparent. The main constraints are the sensitivity of health data, the need for medical interpretation, proportionality of continuous data flows, the risk of opaque automated profiling, and uncertainty about whether enough customers would share comparable data to improve actuarial models. The report therefore sees potential, but not a ready-made business case just yet.

For more details on the legal, business, and technical feasibility, including the potential stakeholder mapping, please refer to the full report (only in Estonian).

5.2 Skills and education

Estonia is already developing an early prototype through the [Skills Compass](#) and the personal [My Compass view](#). An extended version of the service could combine education, qualifications, work history and learning records into a machine-readable competence profile, shared selectively with employers, training providers or career services. It could reduce administrative burden and improve the quality and comparability of recruitment decisions. The main difficulties are semantic interoperability, the large number of small training providers, incomplete private-sector data, algorithmic bias and limited commercial demand. The likely model is a publicly enabled or publicly funded infrastructure with private value-added services.

For more details on the legal, business, and technical feasibility, including the potential stakeholder mapping, please refer to the full report (only in Estonian).

Across both cases, the technical conclusion is similar: implementation is possible when a credible business or public-service owner exists. The legal conclusion is also conditional rather than prohibitive: clear roles, lawful purposes, minimisation, privacy by design, auditability and safeguards for profiling are essential. The differentiating factor is the economic and governance model.

6. Strategic Risks, Opportunities and Unresolved Choices

The report rejects the potential expectation for an universal service provided to Estonian residents that would gather their personal data into a single view. Private data is distributed across local and international organisations, which have different ambitions, incentives, legal duties and technical systems. A realistic future is therefore a **network of interoperable sectoral and cross-sector services**, with users able to connect them where value is clear.

Consent-based data sharing is important but difficult to scale. Existing data consent services cover only a limited set of data sources, while organisations may be unwilling or unable to finance integrations. The report therefore recommends considering a **portfolio of approaches for advancing human-centricity in data economy**: consent and/or other legally valid expressions of individual will as well as contractual and statutory processing grounds; privacy-enhancing technologies that allow verification or computation without disclosing raw data; and, **only for essential services with strong safeguards**, default-access models accompanied by visibility, opt-out rights and accountability.

Beyond the studied use cases, the study further presents **four opportunity clusters for value creation**:

1. convenience and efficiency;
2. voluntary contribution to social and research value;
3. privacy-preserving personalisation as an alternative to opaque tracking; and
4. personal or AI-assisted services that help people manage finances, careers, health or energy use.

Additional concepts include a real-time **personal data balance sheet** (similar to personal financial reports), a verified life record, and contextual comparisons that show how an individual's outcomes relate to relevant population groups without necessarily exposing detailed source data.

The **principal risks** include weak or unclear user value, low data literacy, poor communication, cumbersome user experience, potential cyber incidents, malicious or politically excessive use of data, discriminatory profiling, legal ambiguity, technological lock-in, and the creation of new silos. There is also a **network-effect problem**: individual use cases may remain unattractive until multiple data providers and consumers participate, but organisations may not participate until sufficient demand exists. This makes coordinated pilots and shared standards essential.

7. Recommendations and Conclusions

The report proposes five mutually reinforcing directions for future developments. None is sufficient alone, and the sequence should combine early experimentation with gradual formalisation.

1. Raise public awareness and data literacy. People need general understanding how digital services use data, what choices they have, and what benefits and risks follow. Interfaces for permissions and data-use history must remain simple as the number of services grows.

2. Create a predictable legal and governance framework. Develop guidance for legal bases, roles, liability, data sharing, certification, access policies and supervision. Estonia should align with European developments and use ongoing regulatory discussions to clarify how personal data space services fit within the wider data framework.

3. Increase access to data and foster data sharing through existing digital infrastructure and trustworthy data intermediaries. Priorities include interoperability, standard data formats, clear contractual arrangements, strong security, and support for trusted intermediaries and value-added services.

4. Support data cooperation within private sector. Regulatory sandboxes, accelerators, innovation funding and shared components can lower integration and compliance costs, especially for small and medium-sized enterprises. The state should enable a market rather than centrally build every service.

5. Treat personal data space service development as strategic organisational change. It cannot be delegated as an isolated IT project. Participating organisations need to define executive ownership, a clear value proposition and responsibilities, start iterative pilots and ensure alignment with business strategy.

The feasibility study concludes that personal data spaces should be understood as a long-term transformation of how data-based value is created and governed, rather than as a single technology or governance initiative. It confirms that personal data spaces are realistically implementable in Estonia and are already somewhat emerging through services such as the national portal (eesti.ee), the health portal and skills-related platforms. However, Estonia's principal challenge is the ability to connect mature digital components into a governance model that exceeds public sector boundaries.

The report suggests an incremental and use case-driven implementation strategy that is rooted in principles of human-centricity and interoperability. Estonia should begin with services that have clear user value and committed ecosystem owners, while continuously developing reusable legal, governance and technical enablers. A successful model must give individuals more than formal rights: it must provide understandable control, visible benefits and meaningful remedies. It must also give organisations a credible reason to invest, including access to better data, lower transaction costs, new services and international scalability.

Annex - Research Questions

1. What is the current state of the personal data ecosystem in Estonia, including the high-priority sectors and domains, and to what extent are the principles of human-centric data governance being realised?
2. What is a personal data space, and how do Estonia's current legal framework, digital infrastructure, and cooperation models support the development of one or more personal data spaces, including:
 - a) What solutions currently exist in Estonia and elsewhere? What is missing and/or requires further development?
 - b) What are the principal business models of services that create value from personal data and of data intermediation services?
 - c) What potential market failures or other systemic failures may arise?
 - d) How do Estonian and European Union legislation affect the primary and secondary valorisation of personal data?
3. What level of interest and capabilities do stakeholders in a personal data space have to:
 - a) share, sell, purchase, and create value from data relating to individuals?
 - b) develop products and services based on data relating to individuals?
 - c) develop and/or manage infrastructure and a governance framework that support data intermediation?
4. What are the initial use cases and/or service models through which the implementation of one or more personal data spaces could be piloted in Estonia? To what extent are they feasible, considering business, technological, and legal aspects?
5. What recommendations and practical roadmap exist for implementing one or more personal data spaces in Estonia, considering technical, legal, and business/economic aspects as well as the expectations from different stakeholders?