
HealthHub
Finland EDIH
How to navigate the
Finnish Health Data Landscape
Access and use of healthcare data for innovation
Co-funded by
the European Union

Foreword:

This handbook is for small and medium-sized enterprises (SMEs) that build digital health services, data-driven tools, medical technology, or artificial intelligence (AI) solutions in Finland and across the European Union (EU). It has been produced in co-operation with EDIH HealthHub Finland-project group, supported by legal advisor Sandra Liede, Laissa Oy. Its purpose is practical: to help you understand what kind of health data you are dealing with, which authorities and rules matter, and what questions to ask before you start a pilot, apply for data access, run a study, or launch a product. Inside, you will find guidance on data types and how sensitive they are, synthetic data, key Finnish bodies such as Kanta, Findata, the Finnish Institute for Health and Welfare (THL), Fimea and the Finnish Supervisory Agency (which took over Valvira's tasks from 1 January 2026), and the main rules that shape this field. These rules include the General Data Protection Regulation (GDPR), the Secondary Use Act, the Medical Devices Regulation and In Vitro Diagnostic Regulation (MDR/IVDR), the AI Act, the Data Act, the European Health Data Space (EHDS) and the Network and Information Security Directive 2 (NIS2). This is a working guide for teams that want to move faster, make better decisions, and know when to get expert help.*

Ilona Raitakari,
Senior Business Advisor
HealthHub Finland EDIH
Business Tampere

*) Disclaimer: This document describes the situation at the time of writing and may become outdated. It provides general information only and is not legal advice. You should assess specific cases separately and get legal advice where needed.

1. PERSONAL DATA AND NON-PERSONAL DATA: THE THRESHOLD DISTINCTION

The starting point is whether health-related information can be linked to an identifiable person. If it can, it is personal data and the GDPR applies, governing how the data may be collected, used, stored and shared and giving individuals important rights over it.

If the data does not relate to any identifiable person, it is **non-personal data** and the GDPR does not apply. Common examples of non-personal data include datasets where individuals cannot realistically be identified, aggregated statistics (such as averages across large groups), environmental measurements that cannot be traced back to anyone, and artificially created test data. However, these categories are not always clear-cut.

> A dataset described as anonymised may still count as personal data if it is possible to determine who the data relates to. For example, a combination of age, a rare diagnosis and a small municipality may be enough to identify a specific person.
> Aggregated statistics may relate to groups small enough to single out individuals. For example, where a table shows only one 97-year-old female patient in a small municipality receiving a particular treatment.
> Test data created from real-world sources may still contain traces of personal information. For example, names may have been removed but dates of birth, timestamps, device IDs or free-text clinical notes may remain. Whether data is truly non-personal always requires a case-by-case assessment.

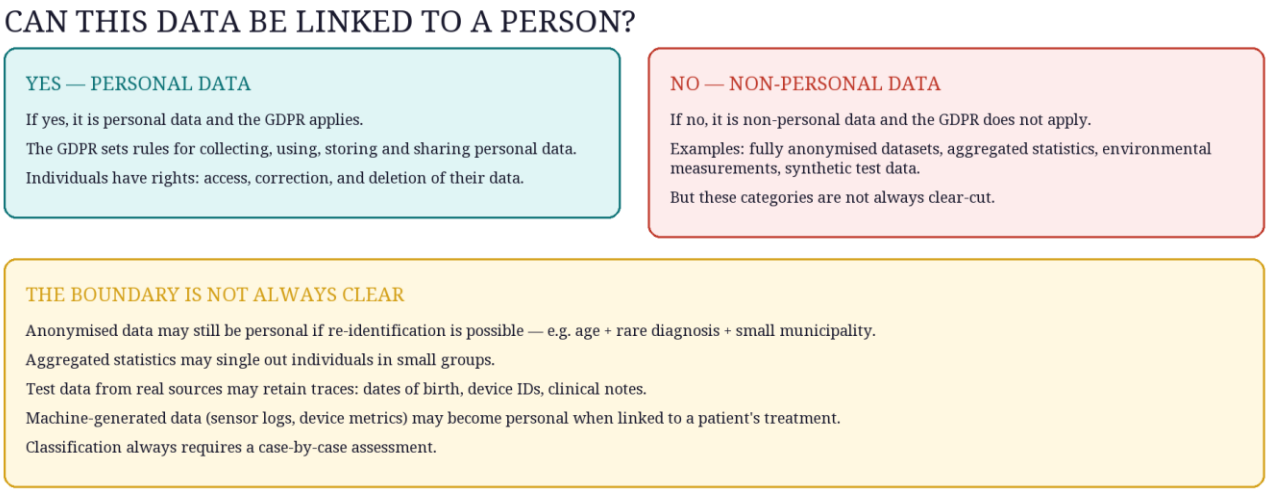
Industrial and machine-generated data may in some cases be non-personal. For example:

- Equipment performance logs, temperature and humidity records from storage facilities, calibration data, and operational metrics from hospital infrastructure.
  - However, the classification is not always straightforward. Sensor readings from a medical device, for example, may be non-personal data when they relate only to the device's technical performance. But they may be personal data if they can be linked to a specific patient's treatment or monitoring session.
- Where a device log includes a patient ID, treatment time and ward location. The assessment therefore depends on context: whether the data, alone or in combination with other available information, can be traced back to an identifiable individual.

Even though the GDPR does not apply, contractual or sector-specific restrictions may still limit how non-personal data is used or disclosed.

- **Confidentiality duties:** for example, a hospital may share anonymised operational data with a vendor, but the recipient may still be bound by confidentiality obligations that prevent onward disclosure.
- **Contractual restrictions:** for example, a data-sharing agreement may permit use of anonymised device-use data for service improvement only, and prohibit resale, publication or broader commercial reuse.
- **Ethical commitments:** for example, a research team may have promised participants or an ethics committee that data will be used only for a defined health research purpose, even if the final dataset is anonymised.

- **Research protocols:** for example, a study protocol may require that data remain within a secure research environment, be accessed only by the named study team, or not be shared with commercial partners without further approval.
- **Sector-specific expectations:** for example, a healthcare organisation may decide not to disclose an anonymised patient-related dataset too broadly if doing so could undermine trust, conflict with clinical norms or create reputational risk, even where the data falls outside the GDPR.



Personal data is any information that can be linked to a specific person. The link can be **direct** — for example, a name, a national identity number, a photograph or an email address. It can also be **indirect** — a combination of details such as date of birth, postcode, occupation and language may be enough to single someone out, even without a name. In short, if someone could reasonably determine who the data relates to, it is personal data.

This matters especially in healthcare, where even limited information may identify a person when combined with other data. Organisations should therefore assess early whether the data they plan to use is personal data, because that determines which legal rules apply and how the data may be accessed.

When data is personal, the organisation using it **must have a valid legal reason** to do so and **must follow the GDPR's rules** on fairness, transparency, data security and individuals' rights. Health data is treated even more strictly. Using it is generally prohibited unless a specific exception applies.

An important point about the boundary between personal and non-personal data is the difference between pseudonymisation and anonymisation. **Pseudonymised** data is data where obvious identifiers (such as names or ID numbers) have been replaced with codes, but it is still possible to trace the data back to a person if someone has access to the key.

- For example, a hospital might replace names with study numbers but keep a separate list that links the numbers back to patients. This means pseudonymised data is still personal data under the GDPR.

Anonymised data, by contrast, has been processed so thoroughly that no one can realistically identify the individuals behind it. Only truly anonymised data falls outside the GDPR. The difference between the two is discussed further in the section on data sensitivity levels below.

> **Key takeaway: Before starting any new product, service or research project involving health-related information, check whether the data is personal or not. This affects which data access routes are available, what security measures you need, whether you need a documented risk assessment, and how you should set up agreements with data partners.**

Operational steps for SMEs:

- Define the dataset and the intended use case at the outset.
- Check whether the data contains direct identifiers, indirect identifiers, or information that could reveal a person's health status when combined with other data.
- Assess whether the dataset is identifiable, pseudonymised, or genuinely anonymised, and avoid assuming that removal of names alone is enough.
- Document the reasoning early and revisit it if the product, dataset, partner set-up, or purpose of use changes.
- If there is real uncertainty, escalate the issue for legal or privacy review. Until that assessment is complete, it is usually safest to treat the data as personal data.

2. What is Health Data?

The next question is whether personal data also counts as health data, because that triggers stricter rules.

Health data is broader than medical records alone and can come from several sources. The categories below are commonly recognised, but the boundaries between them are not always clear. Whether a particular dataset counts as health data under the GDPR often depends on context rather than the source alone.

The key question is often not where the data comes from, but whether it relates to an identifiable person’s health status, healthcare, or inferred health condition. Even data from a non-clinical source can count as health data in context. For example, data from a consumer wellness app may become health data if a provider uses it to assess a patient's condition or treatment needs. Because these boundaries are not fully settled, organisations should document their classification reasoning and be ready to revisit it as case law and regulatory guidance develop.

Health Data Categories

Clinical Data

DESCRIPTION

Data from health records, including diagnoses, treatments, medications, images and laboratory results.

LEGAL COMMENT

Classified as health data under Article 4(15) GDPR and protected under Article 9.

Patient-Generated Data

DESCRIPTION

Data from apps, wearables, medical devices and surveys (e.g., heart rate, sleep, activity, symptoms).

LEGAL COMMENT

Often qualifies as health data when linked to physical or mental health context. Boundaries may be unclear — e.g., step-count data may or may not be health data depending on use context.

Omics Data

DESCRIPTION

Genomic, proteomic, metabolomic and related molecular data (e.g., DNA sequences, biomarkers, metabolite panels).

LEGAL COMMENT

When linked to an identifiable person, this falls under special categories of personal data. May also reveal information about biological relatives depending on identifiability.

Social Determinants of Health Data

DESCRIPTION

Lifestyle, socioeconomic and behavioural data such as housing, education, employment or preferences.

LEGAL COMMENT

May be ordinary personal data or health data depending on whether it reveals health status or is used to infer health-related outcomes (e.g., predicting readmission risk).

Pharmacy and Prescribing Data

DESCRIPTION

E-prescriptions, dispensing records, medication histories and adherence-related data.

LEGAL COMMENT

Can reveal treatment pathways and underlying health conditions.

Registry, Claims and Administrative Care Data

DESCRIPTION

Public-health register data, reimbursement records, referrals, discharge records and service-use data.

LEGAL COMMENT

Qualifies as health data where it reveals treatment history, access to care, or health status (e.g., records showing cancer medication or psychiatric admission).

Inferred Health Data

DESCRIPTION

Non-medical data that becomes health data when used to infer health status, risks or diagnoses (e.g., shopping patterns, sleep data or absence records used to predict depression, pregnancy or cardiovascular risk).

LEGAL COMMENT

One of the most debated categories due to its broad potential scope.

> **Key takeaway for SMEs: do not assume data falls outside health-data rules just because it comes from a non-clinical source. Assess the use case, document your reasoning, and revisit the assessment if the product or purpose changes.**

Operational steps for SMEs:

- Identify exactly what data is being collected, from whom, and for what purpose.
- Check whether the use case could reveal health status, treatment needs, or a likely diagnosis, even if the source data is not clinical.
- Record the classification reasoning in writing and note what assumptions it depends on.
- Review whether the product design, customer context, or intended outputs could change the classification over time.
- Where the answer is materially uncertain, a prudent approach is to treat the data as potentially health data and obtain legal or privacy input before proceeding.

Importance of Health Data

Once a dataset is recognised as health data, the central question is no longer just what the data is, but what it can be used for and under what conditions. Health data matters because it supports a wide range of activities across the healthcare system — from direct patient care to research, product development and public-health decision-making. For an SME, this is often the stage at which legal classification starts to shape real commercial and operational choices.

- In **personalised care**, health data supports diagnosis, treatment planning, follow-up and remote monitoring.
- In **medical research and drug development**, it helps identify disease patterns, validate hypotheses, evaluate treatments and generate evidence on safety and effectiveness.
- In **regulatory and reimbursement settings**, it may be used as real-world evidence to support regulatory decisions, health technology assessment and market-access discussions.

For smaller companies, this has immediate practical consequences. The same product idea may look very different depending on whether the use case is clinically embedded, research-driven, product-facing or built for collaboration with healthcare providers. A company developing a tool for hospital use, for example, may need clinical integration, contracts with care providers and stronger governance. A company pursuing a research or validation use case may instead need permits, secure environments and a different evidence strategy.

In practice, health data underpins remote monitoring, chronic care management and AI-enabled tools such as medical image analysis, clinical documentation support and predictive models. But the commercial value of those tools does not depend on technical performance alone. It also depends on whether the data can be accessed lawfully, whether it is accurate and usable enough, whether it can be integrated into clinical or operational workflows, and whether the overall governance model gives hospitals, partners and regulators confidence.

For that reason, the practical value of health data is closely tied to four recurring factors: **lawful access**, **data quality**, **interoperability** and **trustworthy governance**. If one of those is weak, the use case may become slower, more expensive or less credible even where the underlying technology is strong.

Data Sensitivity Levels

The same features that make health data valuable also make it legally sensitive. Under Article 9(1) of the GDPR, health data is a special category of personal data. Using it is **generally prohibited unless a specific exception applies**. Organisations must therefore assess how identifiable the data is and apply safeguards accordingly. As a general rule, the more identifiable the data, the stricter the legal, technical and organisational controls need to be. That assessment should be documented, particularly for large-scale or higher-risk processing. In practice, organisations should distinguish between the following data states:

> **Identifiable personal data**: this is individual-level data that identifies a person directly or could reasonably be used to identify them, whether on its own or combined with other available information. It typically carries the highest risk and will generally need the strongest safeguards, such as access controls, encryption, logging and, where relevant, a data protection impact assessment (DPIA).

- In legal terms, this will often mean identifying a proper legal basis under Article 6 and, where relevant, an Article 9 condition under the GDPR, defining roles and responsibilities between controllers and processors, documenting purpose limitation and minimisation, and assessing whether you need a DPIA, data processing agreement, confidentiality arrangements or additional sector-specific permissions.

- In technical and organisational terms, it typically requires stricter user-access management, encryption in transit and at rest, audit logging, role-based permissions, secure environments, staff training, incident response procedures and tighter internal governance over who may access, analyse or export the data.

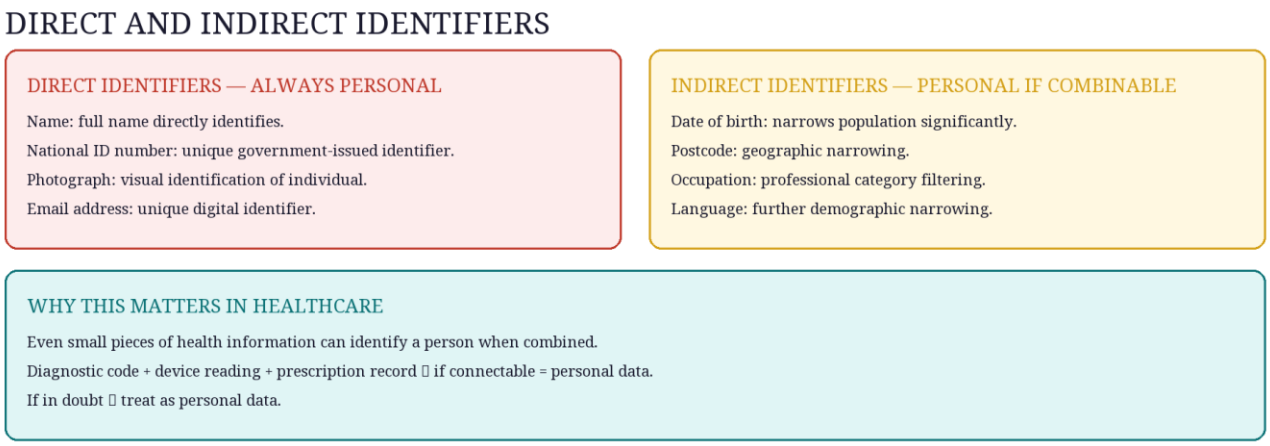
Some datasets may fall outside the GDPR where they have been processed so that individuals can no longer be identified by any reasonably likely means. You must assess that boundary carefully, especially for health data, because moving from identifiable or pseudonymised data to genuinely anonymised data can significantly change the level of legal, technical and organisational controls you need.

> **Anonymised data:** data processed so that individuals can no longer be identified by reasonably likely means. If re-identification remains reasonably possible, the data is still personal data and the GDPR continues to apply. The exact anonymisation threshold remains debated in EU law.

Organisations should therefore assess anonymisation against re-identification risk in context. This includes the size and uniqueness of the dataset, the number of variables kept, the availability of external datasets that could be used for matching, and the means reasonably available to likely recipients. This is especially important for health data, because rare conditions, small populations, long-term records

and rich clinical variables can make individuals identifiable even where obvious identifiers have been removed.

If the anonymisation threshold is genuinely met, the data may fall outside the GDPR. However, you should still check whether confidentiality duties, contractual restrictions, ethical commitments, research protocols or sector-specific expectations continue to limit how the data may be used or disclosed.



Synthetic Data

> Synthetic data is artificially generated from patterns learned from real-world datasets. Unlike pseudonymised or anonymised data, it is created anew rather than altered from existing records.

This distinction matters because, if the synthetic output is sufficiently removed from the underlying records, it may fall outside the GDPR. However, as discussed below, whether that threshold is met in any given case requires a validated re-identification risk assessment. The generation process itself remains regulated where it uses real personal data as input.

Synthetic data is particularly relevant for SMEs because it may reduce some of the access barriers associated with real-world health data and support product development, testing and early experimentation. In Finland, this can be valuable where access to real data for secondary use may require permits and secure processing environments. However, whether synthetic data genuinely removes regulatory and practical barriers — rather than shifting them to the generation stage — is not yet settled and depends on the specific use case and how regulators treat the generation process.

> For example, an SME wanting to train a predictive model on hospital discharge data might use a synthetic dataset instead of applying for a Findata data permit. While the synthetic output may itself fall outside the GDPR if re-identification risk is low enough, generating that synthetic dataset from real patient records will generally still count as processing special-category personal data. This may require its own legal basis under the GDPR and may also require a data

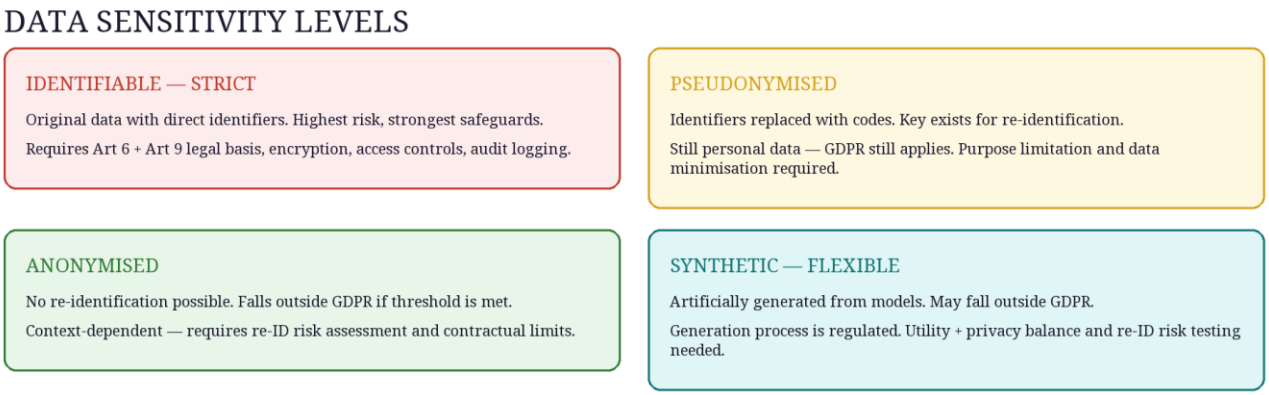
> permit under the Secondary Use Act and use of a secure processing environment. The regulatory burden is not eliminated — it is relocated to an earlier stage of the workflow.

The value of synthetic data depends on two things: **utility and privacy**.

Synthetic data should be realistic enough to support development and testing.
It should also be validated — that is, subjected to a documented re-identification risk assessment using appropriate statistical or technical methods, such as linkage testing, outlier analysis or distance-based metrics — to support the conclusion that individuals from the source data cannot be identified, directly or indirectly, from the synthetic output.

- Under the GDPR, synthetic data may fall outside personal-data rules only if people from the source data cannot realistically be re-identified from it. Guidance is still limited, but regulators generally treat synthetic data as a privacy-enhancing technique while stressing that creating it from real personal data is itself regulated processing and still requires a legal basis and safeguards. Organisations should therefore clearly distinguish between the input stage (which is regulated) and the output stage (where the GDPR status depends on a validated re-identification risk assessment).

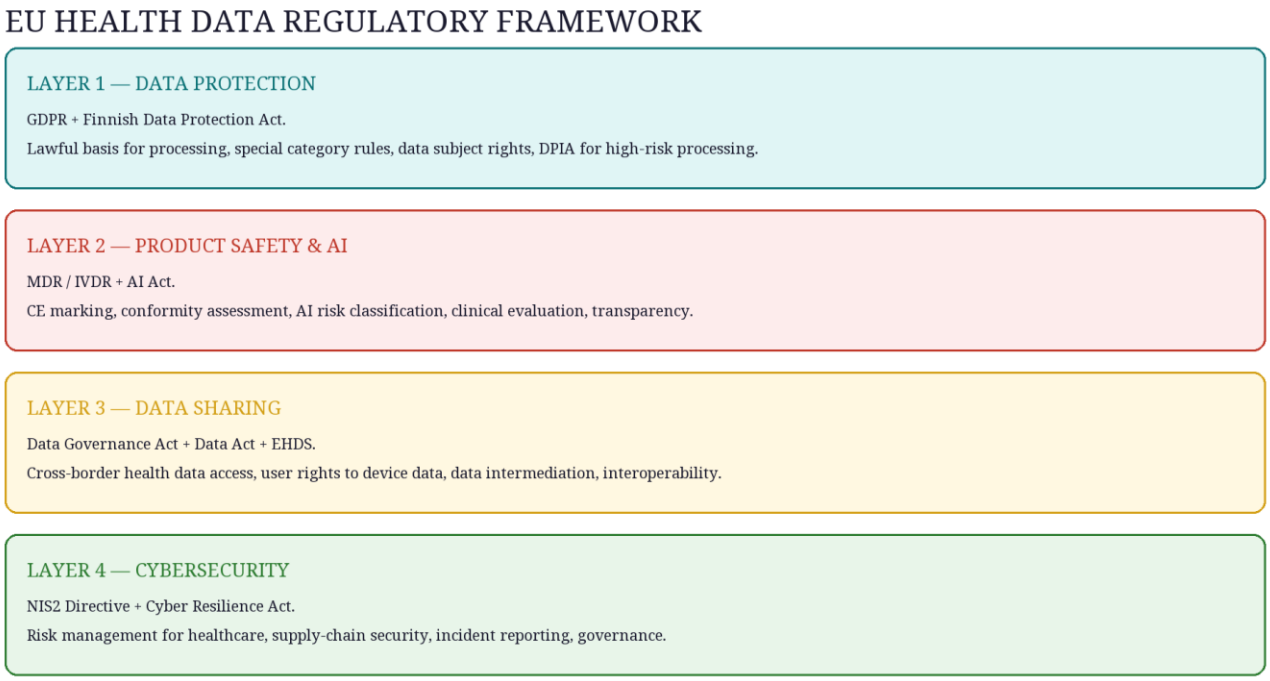
- For SMEs, synthetic data is often most useful as a bridge between concept development and access to real-world datasets. It can help teams test workflows, train models, demonstrate functionality and refine technical assumptions before engaging with stricter real-data access routes. That said, how reliable synthetic data is as a substitute or stepping stone depends on the quality of the generation model, how closely the output matches reality, and whether regulators and research partners accept synthetic data for the intended purpose. These factors vary across use cases and are still evolving.



3. Health Data Legal Landscape

The starting point for the legal analysis is EU law. At EU level, the rules can be understood in four layers. First, the GDPR sets the basic rules for using personal and health data. Second, if the product is a medical device or diagnostic tool, the MDR or IVDR applies, and if it also uses AI, the AI Act adds

another layer. Third, the Data Governance Act, the Data Act and the EHDS deal with data access, sharing and interoperability. Fourth, NIS2 adds the cybersecurity layer.



The following sections examine each of these regulatory layers in detail. The chapter begins with the GDPR and Finnish data protection framework, including the distinction between primary and secondary use of health data. It then turns to health technology and AI regulation, followed by data sharing and interoperability, and concludes with cybersecurity.

EU General Data Protection Regulation ((EU) 2016/679)

The General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR") is the main EU law governing the use of personal data, including health data. It applies directly in all Member States and sets a uniform set of principles, obligations and rights that any organisation using personal data must follow, regardless of sector. For companies working with health data, the GDPR is not just a background compliance requirement. It is the legal framework that determines whether, how and on what basis you may collect, use, share and keep data.

Core Principles

The GDPR is built on a set of core processing principles set out in Article 5.
By way of illustration, consider an SME that develops an AI-based tool for analysing dermatological images to support clinical diagnosis:

GDPR Principle	Practical Application for Patient Image Processing
Lawfulness	The company must identify a valid Article 6 legal basis and, where special-category data is involved, an applicable Article 9 condition before processing any patient images.
Purpose Limitation	Images collected to train a diagnostic algorithm may not be repurposed—for example, for marketing or unrelated commercial analytics—without a separate legal assessment and compatible purpose evaluation.
Data Minimisation	Only the image data and clinical metadata strictly necessary for the algorithm's intended function should be collected; full patient records should not be ingested.
Accuracy	The company must verify and, where needed, correct clinical labels attached to training images, as inaccurate labels undermine both model performance and the integrity of the personal data.
Storage Limitation	The company must define and enforce retention periods and delete, anonymise, or otherwise appropriately handle training images once they are no longer required for the stated purpose.
Integrity and Confidentiality	Images must be protected throughout their lifecycle using appropriate technical and organisational measures such as encryption, access controls, and audit logging.
Accountability	The company must document each assessment, decision, and safeguard and be able to demonstrate compliance to the supervisory authority upon request.

Legal Basis

Using personal data requires a **legal basis under Article 6(1) of the GDPR**. In the health data context, organisations will generally also need a separate Article 9(2) condition for the health-data element, as discussed below. The Article 6 bases most commonly encountered in health-sector activities include the following, each illustrated with an example relevant to an SME working in the health space.

Lawful Basis	Short Description	Sector--Relevant Example (Digital Health / MedTech)
Consent	Processing is based on the data subject's freely given, specific, informed and unambiguous consent.	A digital health -startup offering a wellness app relies on user consent to process symptom--tracking data for personalised recommendations.
Contract	Processing is necessary to perform a contract with the data subject or to take steps at their request prior to entering into a contract.	A remote physiotherapy SME processes only the health data strictly necessary to deliver telehealth services, while relying on a separate Article 9 condition for special--category data.

Legal Obligation	Processing is necessary to comply with EU or Member State law applicable to the controller.	A regulated private healthcare provider in Finland must maintain patient records and transmit required data to Kanta Services.
Vital Interests	Processing is necessary to protect someone's life or health when the data subject is unable to consent.	An emergency response device provider processes location and health--alert data without prior consent when the user is incapacitated and immediate medical intervention is required.
Public Interest / Official Authority	Processing is based on a task in the public interest or the exercise of official authority, grounded in law and assigned to the controller.	A company running a population--level screening programme for a wellbeing services county cannot assume this basis applies to it; the county relies on Article 6(1)(e), while the company processes data on the county's behalf.
Legitimate Interests	Processing is necessary for the controller's or a third party's legitimate interests, unless overridden by data subjects' rights and freedoms.	A cybersecurity monitoring provider processes limited access--log data (e.g., staff identifiers) to detect unauthorised access to hospital systems. This basis is widely debated due to its broad potential scope.

Note that Article 6(1)(f) is not available to public authorities acting in the performance of their tasks. Where health data is involved, reliance on Article 6(1)(f) must also be assessed together with the relevant Article 9(2) condition discussed below.

> **Key takeaway for SMEs: the choice of legal basis is not a formality. It determines the rights available to data subjects, the conditions under which you may continue processing, and the consequences if the basis is later found to be wrong. Choosing the wrong basis, or failing to identify one before you start processing, may undermine the entire data-processing arrangement.**

Operational steps for SMEs:

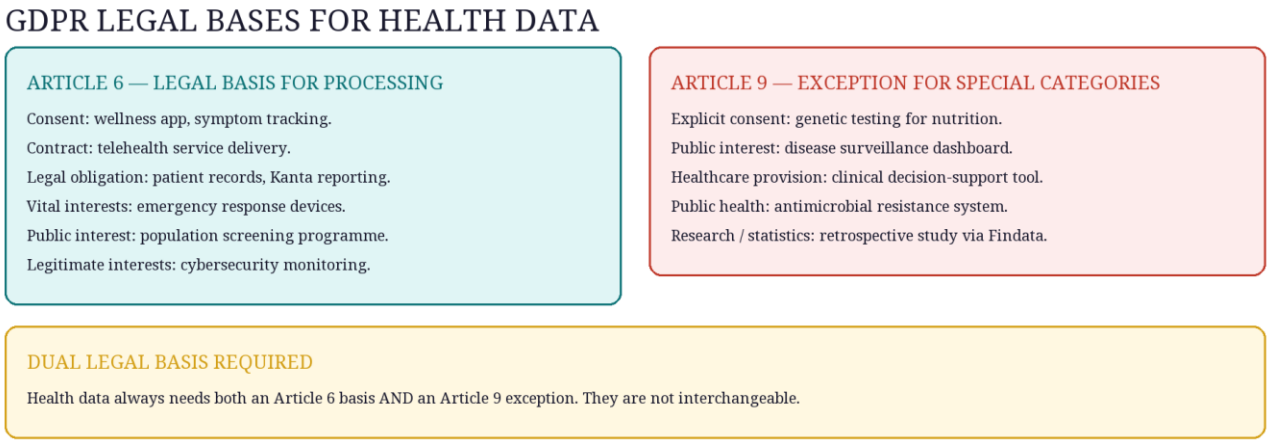
- Identify the most appropriate Article 6(1) legal basis for each distinct processing activity, rather than applying a single basis across all operations.
- Where consent is relied upon, verify that it meets the GDPR's requirements for freely given, specific, informed and unambiguous consent, and consider whether the relationship between the company and the data subject creates any imbalance that could undermine the validity of consent.
- Where legitimate interests are relied upon, carry out and document a balancing test assessing the company's interest against the rights and freedoms of the data subjects, and note that this basis is not available to public authorities acting in the performance of their tasks.
- Record the chosen legal basis and the supporting reasoning before processing begins, and do not change the legal basis retrospectively.

Health Data Exceptions

Because **health data** is a special category of personal data under Article 9(1), using it is generally prohibited unless one of the **conditions in Article 9(2) applies**. The most relevant conditions for health data include the following, each illustrated with an example relevant to an SME working in the health space.

Explicit Consent	Special-category data may be processed where the data subject gives explicit, informed and freely given consent for a specific purpose.	An SME providing a genetic-testing service for personalised nutrition processes a customer's genetic data based on explicit consent to analyse and store their genetic profile.
Substantial Public Interest	Processing is necessary for reasons of substantial public interest, based on Union or Member State law that provides suitable safeguards.	An SME contracted by a public authority to build a population--level disease--surveillance dashboard processes aggregated patient data under legislation enabling communicable--disease monitoring.
Preventive/Occupational Medicine & Healthcare Provision	Processing is necessary for medical diagnosis, preventive or occupational medicine, or health/social care provision, carried out by or under a professional bound by secrecy.	An SME supplying a clinical decision--support tool within a hospital EHR may process patient data where processing is performed under the responsibility of a health professional subject to professional secrecy.
Public Health	Processing is necessary for public-health purposes (e.g., ensuring high standards of quality and safety of healthcare), grounded in law with specific safeguards.	An SME developing an early--warning system for antimicrobial resistance for a wellbeing services county processes laboratory data to support public--health objectives in accordance with applicable safeguards.
Scientific Research, Statistics, Archiving	Processing is necessary for scientific or historical research, statistical purposes, or archiving in the public interest, subject to Article 89(1) safeguards and national rules.	An SME conducting clinical research using retrospective patient data obtained via a Findata permit relies on this exception under GDPR Article 89(1) and national legislation, such as the Secondary Use Act (552/2019).

In practice, this means that an organisation using health data will generally need to identify both an Article 6 basis and an Article 9 condition, and to document that assessment before it starts processing.



Data Subject Rights

The GDPR gives individuals a comprehensive set of **rights**, including:

Right	Example in Digital Health Context
Access	A patient asks a digital health provider to confirm whether it holds their health data and to provide a copy.
Rectification	A user requests correction of an inaccurate medication entry or outdated contact detail.
Erasure	A person asks a wellness app to delete their data when there is no longer a valid basis to keep it.
Restrict processing	An individual asks an organisation to stop using disputed data while its accuracy or legal basis is being reviewed.
Data portability	A user requests their app-based health data in a structured format so they can transfer it to another service.
Objection	A person objects to processing carried out on the basis of legitimate interests.
Withdrawal of consent	Where processing relies on consent, the individual withdraws that consent at any time.

These rights are subject to certain limitations, particularly in the research context, where Member States may restrict certain rights under Article 89(2).

DPIA

Organisations must carry out a **data protection impact assessment ("DPIA")** where processing is likely to create a high risk to individuals' rights and freedoms. In healthcare, that threshold is often met because of the scale, sensitivity or technological intrusiveness of the processing.

Minimal example checklist for a DPIA:

- Describe the processing activity, purpose, dataset and parties involved.
- Explain why the processing is needed and whether the same goal could be achieved with less data or lower risk.
- Identify the main risks to individuals, such as unauthorised access, re-identification, misuse, bias or function creep.
- List the safeguards, such as access controls, encryption, logging, minimisation, retention limits and restricted outputs.
- Record who approved the assessment, what risks still remain after the planned safeguards, whether the data protection officer's advice was sought where applicable, and whether further legal, security or ethical review is needed.

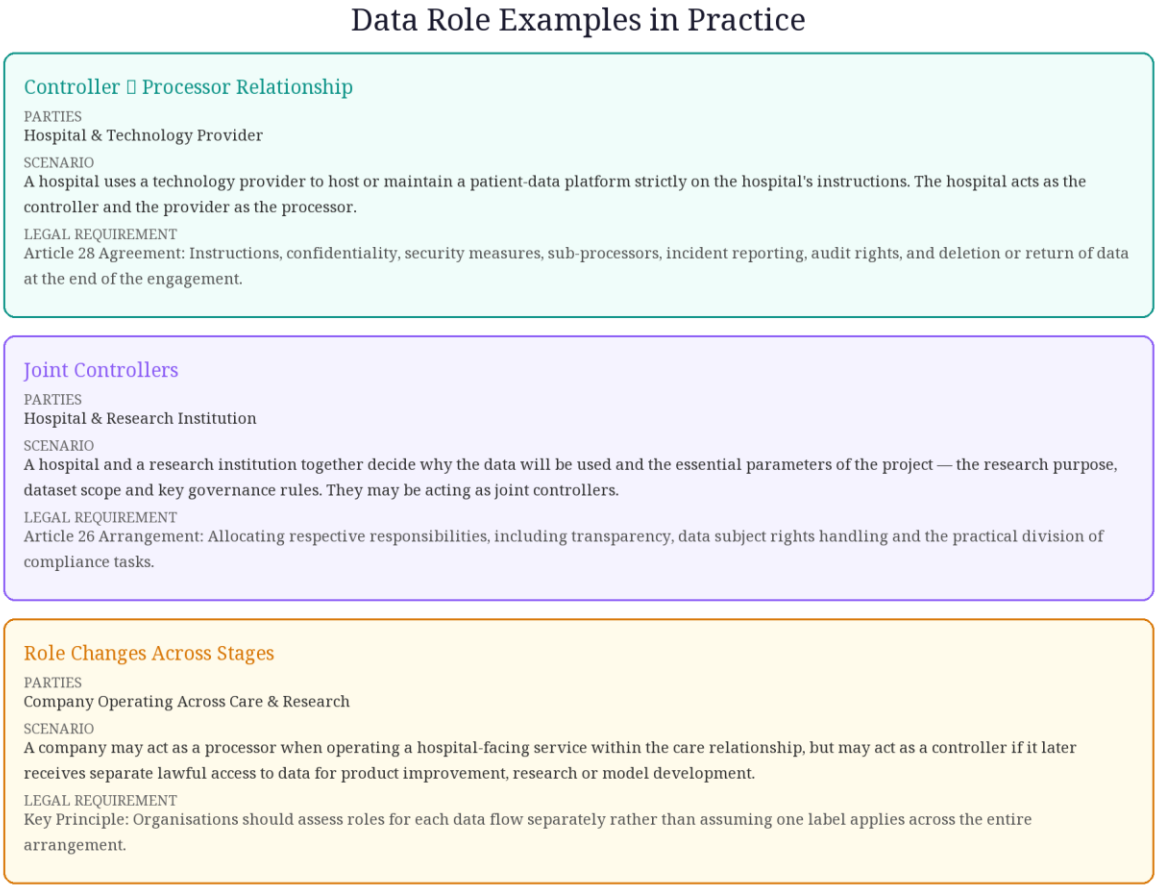
> **SMEs can often do an initial DPIA review themselves, but should get expert help if the project is new, large or high-risk. If serious risk remains after safeguards are in place, the controller may need to consult the supervisory authority before processing begins.**

Controller and Processor

The GDPR also sets a clear split of responsibilities between **controllers** (who decide the purposes and means of processing) and **processors** (who process data on behalf of the controller). Where two or more controllers jointly decide the purposes and means of processing, they must enter a **joint controllership** arrangement under Article 26. Controller-processor relationships must be governed by a binding agreement meeting the requirements of Article 28.

Situation	Implication for the Organisation's Role
Your organisation decides why the data is processed and the key parameters of how it is used.	The organisation is likely acting as a **controller**.
Your organisation handles the data only on another party's documented instructions.	The organisation is likely acting as a **processor**.
Two parties jointly decide the purpose of the processing and the essential parameters of the arrangement.	They may be **joint controllers** and should put in place a joint-controller arrangement.
The role changes across different stages or data flows.	The role must be **assessed separately for each stage**, rather than assumed to be the same throughout the project.

These structural requirements are particularly relevant in the health data context, where data flows between hospitals, technology providers, research institutions and public authorities often involve complex multi-party arrangements.



Enforcement, Transfers and National Discretion

The GDPR is enforced by national data protection authorities. If a company operates in several EU countries, one lead authority will often coordinate with the others so that the case is handled consistently across the EU. This matters for companies whose services or research activities cross borders.

Transfers of personal data to countries outside the EU or to international organisations are allowed only if the GDPR's transfer rules are met — for example, because the destination country has been approved as providing adequate protection, the parties use approved transfer safeguards such as standard contractual clauses, or a narrow exception applies.

The GDPR is also supplemented in Finland by the Finnish Data Protection Act (1050/2018), which provides national rules on matters left to Member State discretion and works alongside sector-specific health and social care legislation. In practice, this includes national rules on supervision, procedural matters, sanctions and certain research-related exceptions and safeguards. The chapter therefore turns first to primary use and secondary use before addressing the wider institutional and supervisory framework.

Finnish Health Data Framework

Once data is identified as health data, the next practical question is not only what rules exist, but what purpose the data will be used for. In Finland, this **purpose-based distinction** is fundamental because the legal pathway differs depending on whether the data is used in direct care or for purposes beyond care.

Primary use refers to the processing of health and social data for the purpose of direct patient care and service delivery within the care relationship itself.

The boundary between primary and secondary use is not always clear-cut. The classification of a given processing activity may be debated depending on the specific circumstances. For instance, where data generated during care is simultaneously used to improve a clinical tool or inform service development.

The following are generally regarded as examples of primary use:

- a clinician accessing a patient's electronic health record to inform a treatment decision;
- a hospital deploying a clinical decision-support tool that analyses patient data in real time to assist in diagnosis;
- an SME providing a remote monitoring platform through which a physician tracks a patient's vital signs as part of an ongoing treatment plan; or
- a private physiotherapy provider recording treatment notes and sharing them with the referring physician through Kanta Services, Finland's national digital health infrastructure for functions such as electronic prescriptions, patient records and related care-data exchange.

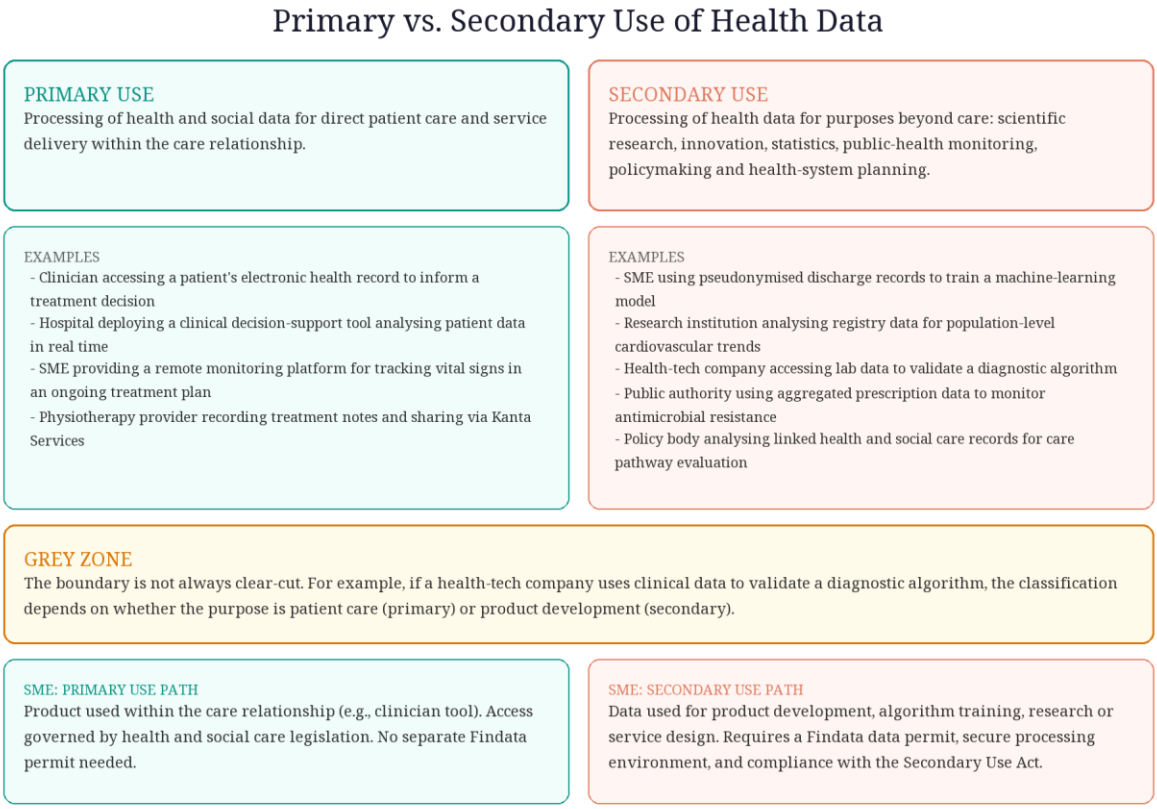
Secondary use refers to the processing of such data for purposes other than the original care or service context. This includes scientific research, innovation, statistics, public-health monitoring, policymaking and health-system planning.

> The classification is not always obvious. For example, if a health-technology company uses real-world clinical data to validate a diagnostic algorithm, the key question is whether the data is being used as part of patient care and quality assurance within the care relationship (which may point towards primary use) or for the company's own product development or improvement purposes (which may point towards secondary use). The answer may depend on the actual purpose of the processing and on the contractual and organisational arrangements in place.

The following are generally regarded as examples of secondary use:

- an SME using pseudonymised hospital discharge records to train a machine-learning model for predicting patient readmission risk;
- a research institution analysing registry data to study population-level trends in cardiovascular disease;
- a health-technology company accessing laboratory data to validate the performance of a diagnostic algorithm against real-world outcomes;

- a public authority using aggregated prescription data to monitor antimicrobial resistance patterns; or
- a policy body analysing linked health and social care records to evaluate the effectiveness of a regional care pathway reform.



For SMEs, the distinction between primary and secondary use has direct **practical consequences**.

- If a company's product or service is used within the care relationship itself, for example, as a tool used by clinicians in patient treatment, the data-access route will usually be governed by health and social care legislation and the relationship with the data controller (such as a wellbeing services county or hospital), without needing a separate permit from Findata.
- If a company wants to use existing health or social data for product development, training, research or service design, the secondary-use pathway will often apply. This typically requires a Findata permit, a secure processing environment, and compliance with the Secondary Use Act's purpose and output restrictions.

Operational Compliance Requirements

Client Data Act (703/2023)

Current law. The Client Data Act (703/2023) can affect how you plan, build and use a product or service in practice. If a system handles client data within the care relationship, you may need to build certain safeguards and working methods into the system from the outset rather than add them later.

What this means in practice depends on the company's role and the type of service or system involved. You may need clear rules on who can access data, how users are identified, how data use is recorded, how responsibilities are divided, and how the system fits with the customer's security requirements and other systems. You may also need appropriate internal procedures, staff guidance, incident handling and oversight of subcontractors.

For example:

- a software vendor providing a patient-record or clinical support tool may need role-based access controls, audit logging, compatibility with the customer's care-data environment, and compliance with the provider's security and documentation standards from the outset;
- an AI or health-tech startup deploying a tool in a clinical workflow may need to limit access to authorised users, align the system with the provider's security and documentation requirements, control subcontractors appropriately, and use the data processing agreement to allocate incident, audit and end-of-engagement data responsibilities clearly; and
- a service provider working with hospitals may need to align its operating model with the hospital's legal and technical requirements and demonstrate compliance through audits, certifications or contractual assurances.

If the service connects with national systems such as Kanta Services, additional technical and organisational requirements may also apply.

Pending reform. SMEs should monitor the proposed amendments to the Client Data Act (HE 159/2025 vp). If enacted, the proposal would allow health professionals to use patient data in the healthcare organiser's own register for purposes such as defining screening and health examination target groups, monitoring care, and early identification of health problems, even where it is unclear whether an active care relationship exists. This may affect how systems and services are designed where the product supports proactive or anticipatory care workflows such as population-level screening, risk stratification or care-gap identification.

Secondary Use Act (552/2019)

For secondary use, the compliance framework changes significantly. As at the time of writing, the live framework under the Secondary Use Act (552/2019) still operates primarily through a permit-based model, and companies should understand the current access route before planning a project.

- **Findata**, the Health and Social Data Permit Authority, acts as the **single point of access** especially where a request concerns data held by **multiple data controllers** or national register sources.
- Where data is requested from a **single data controller** for a purpose falling within the Act's scope, that controller may in certain cases issue the permit itself. In practice, however, multi-source requests and requests involving national register data are routed through Findata.

In practice, a company will usually need a **data permit** under the Act. Depending on the data source and route, that permit is issued either by Findata or, in some single-controller cases, by the relevant controller. The application must specify the legal purpose of the processing, the datasets requested, the GDPR legal basis under Articles 6 and 9, and the applicable safeguards. The processing must fall within one of the purposes listed in the Act:

- scientific research
- statistics
- development and innovation
- teaching
- knowledge management
- supervisory activities

The data application must show that the requested data is necessary and proportionate and that the purpose cannot reasonably be achieved with less sensitive or non-personal data. The permit authority may impose conditions, including restrictions on scope, duration, permitted analyses and output format.

Data is typically accessed only through a **secure processing environment** maintained or approved under the Secondary Use Act framework. As a rule, the company may not transfer raw or record-level data to its own systems. The environment imposes technical constraints on available software, internet connectivity and data import and export. Outputs are subject to disclosure control before they may be extracted.

Additional obligations may include a data protection impact assessment and, where applicable, an ethical review under the Medical Research Act (488/1999). The company must also comply with any conditions attached to the permit, including reporting, data retention and deletion requirements, and restrictions on further use or disclosure of results.

One current exclusion should be noted. Since 1 January 2026, the Secondary Use Act **no longer applies to the processing of personal data in clinical trials, medical device investigations and medical research where the participant or the participant's legal representative has given consent under the applicable research legislation.** Those projects may still require GDPR compliance, ethics review and compliance with the relevant research legislation, but they do not follow the Secondary Use Act route merely because health data is involved.

Further amendments are scheduled to enter into force on 1 May 2026 and are expected to change permit routing, data assembly and the conditions for using alternative secure environments. Until those changes take effect, companies should plan on the basis of the current framework described above and verify the applicable route shortly before filing an application.

Biobank Act (688/2012)

Current law. Where a company's product development, research or validation activities involve biological samples or sample-derived data held by Finnish biobanks, the Biobank Act (688/2012) imposes a distinct set of requirements on consent, governance and access. These differ significantly from both the care-data pathway and the Findata data permit pathway discussed above. Finnish biobanks collect, store and make available biological samples — such as tissue, blood and DNA — together with associated clinical and lifestyle data, for the purpose of biobank research.

The biobank framework operates under its own governance model, with separate rules on donor consent, institutional oversight and data access. For SMEs, understanding this framework is important because biobank materials represent a significant source of real-world biological and clinical data for algorithm training, biomarker discovery, diagnostic validation and other health-technology applications. The key features of the biobank framework relevant to SMEs are as follows.

- **Biobank consent** is an ethical consent indicating the donor's voluntary decision to participate in biobank research. It is **not** GDPR consent. Therefore, the legal basis for processing biobank personal data typically comes from **Article 6(1)(e)** (public interest), together with **Article 9(2)(i)** (public health) and the Biobank Act.
  For SMEs, this means that **withdrawing biobank consent does not invalidate past processing** carried out under a separate GDPR basis; it usually only prevents the biobank from providing the donor's samples or data for **future** research.
- **Biobanks have specific governance obligations:** they must appoint a responsible researcher, maintain a code of conduct describing operating principles and access criteria, and comply with Fimea's supervision. Fimea maintains the national biobank register and may issue orders or revoke the right to operate. For SMEs, the biobank's governance standards may help demonstrate the provenance and quality of training data used in medical devices or AI systems.
- **Access to biobank samples and data** is granted through a written agreement—a material transfer agreement for physical samples or a data-access agreement for data—after the biobank reviews the scientific merit, ethical acceptability and data-protection adequacy of the proposed project.
- The **Finnish Biobank Cooperative (FINBB)** coordinates national biobank operations and runs **operates Fingenious® service**, a centralised solution allowing companies and researchers to search biobank collections, assess feasibility and submit multi-biobank access applications.

While Fingenious® service streamlines the process, **each biobank makes its own access decision**, and terms and timelines may differ.

- Where a project uses **only biobank samples or data**, a Findata permit is generally **not** needed. However, if the project combines biobank data with other health or social data governed by the **Secondary Use Act**, a Findata permit is typically required for the non-biobank component. The **two pathways must be coordinated** for timing, scope and conditions, and GDPR legal bases must be assessed **separately** for each data source.

  For SMEs, this often means **parallel interactions** with both the biobank (or FINBB/ Fingenious® service) and Findata, each with its own criteria and timelines.

Medical Research Act (488/1999) and Ethical Pre-Assessment

Current law. Where a company's activities involve medical research on human subjects — including research that uses identifiable health data — the Medical Research Act (488/1999) may apply. The Act sets out the conditions under which medical research may be conducted in Finland and establishes a system of mandatory ethical pre-assessment. The Act applies to research aimed at increasing knowledge of health, the causes, symptoms, diagnosis, treatment or prevention of diseases, or the nature of diseases, where the research involves intervention in a person's physical integrity or where identifiable personal data is processed for the purposes of such research.

> **For SMEs, this threshold question is important: not all activities involving health data count as medical research under the Act. For example, purely technical product testing using anonymised data, or secondary analysis of aggregated statistics, would generally fall outside its scope. But a clinical validation study involving patient data or a prospective observational study with identifiable participants would typically fall within it.**

Before medical research may begin, the research plan must be submitted for review by an ethics committee. The national Committee for Medical Research Ethics (Tukija) is responsible for issuing opinions on clinical trials of medicinal products and clinical investigations of medical devices. For other medical research, the review is carried out by a regional ethics committee. The ethics committee assesses, among other things, the scientific validity of the research plan, the rights and safety of research subjects, whether informed consent arrangements are adequate, and whether the use of personal data is justified. A favourable opinion from the competent ethics committee is a precondition for starting the research.

For SMEs, the Medical Research Act is relevant in these situations:

Situation	Description
Company as Research Sponsor or Conducting Research	When the company itself conducts or sponsors medical research — e.g., a clinical validation study for a diagnostic algorithm using patient data — the Medical Research Act applies directly. This includes requirements for ethical review, informed consent, and research-governance obligations.

Ethical Review Required for Findata Permit (Secondary Use Act)	Even if the company is not the research sponsor, an ethical review under the Medical Research Act may be required as a prerequisite for obtaining a Findata data permit when the secondary-use purpose is scientific research that meets the Act's definition of medical research.
Use of Biobank Samples or Data Constituting Medical Research	Under the Biobank Act (Section 4), the Medical Research Act governs medical-research conditions and ethical pre-assessment. When a company uses biobank samples or data in a manner that constitutes medical research, the ethical-review obligations of the Medical Research Act apply *in addition to* biobank-specific access and governance requirements.

Companies should therefore assess at an early stage whether their planned use of health data — whether obtained through Findata, a biobank or another route — counts as medical research under the Act and, if so, factor the ethics committee review process and its timeline into their project planning.

Pending reform. A government proposal circulated for comment in December 2025 proposes a broad clarification and consolidation of Finnish research legislation. According to the proposal, the main package would enter into force on 1 January 2028, with certain personal-data provisions entering into force on 1 January 2027.The points likely to matter most for SMEs are:

Element	Description
Scope	The Medical Research Act would be expanded so that research involving deceased persons and the secondary use of biological samples is brought under the Act.
Secondary-Use Interface	The relationship between the Secondary Use Act and medical research would be clarified, including a proposed exclusion for certain rare-disease research where the participant has consented, or where a deceased person is not known to have objected during life.
Appeals	The ethics-committee appeal system would be unified, creating a single appeal pathway within Tukija for several research-related opinions that are currently managed through a fragmented structure.
Feasibility Work	The proposal would establish clearer legal bases for feasibility assessments in scientific research and, in some clinical research contexts, for identifying and contacting potential participants.
Biobanks	Significant amendments to the Biobank Act are proposed, including removal of the definition of "biobank research", broader statutory tasks for biobanks, explicit feasibility services for clinical trials, and a new recall-consent mechanism.
Practical Relevance for SMEs	If enacted, these reforms could materially change how research, rare-disease projects, feasibility work and biobank-based projects are planned. SMEs with research programmes extending beyond 2027 should monitor the proposal and avoid assuming the current process map will remain unchanged.

4. HEALTH TECHNOLOGY & ARTIFICIAL INTELLIGENCE

For many digital health companies, the legal analysis does not stop once access to health data is permitted. If the solution itself functions as software, a medical device, or an AI-enabled clinical tool, product-regulatory requirements apply in parallel. A company may have lawfully obtained a Findata data permit, complied with the GDPR and satisfied the requirements of the Medical Research Act, and yet still need CE marking before its product may be placed on the EU market.

Conversely, a product may be CE-marked as a medical device and yet still require a separate data permit for the secondary use of health data in its development or validation. The two regulatory layers must both be satisfied, and they must be planned for in parallel rather than sequentially.

The regulation of digital health technologies and AI-based solutions in the EU is mainly governed by two product-safety laws: the Medical Device Regulation (MDR) and the In Vitro Diagnostic Regulation (IVDR), together with the Artificial Intelligence (AI) Act, which adds further requirements for AI-enabled systems. These laws operate independently of the GDPR and the data-access frameworks discussed above, but apply at the same time where a product that processes health data is also placed on the market as a medical device or an AI system.

Medical Device Regulation ((EU 2017/745) & In Vitro Diagnostic Regulation ((EU) 2017/746)

The MDR and IVDR set the safety, performance and quality requirements for medical devices and in vitro diagnostic devices placed on the EU market. The MDR covers a broad range of devices, including software, while the IVDR applies to devices that analyse human specimens for diagnostic or related clinical purposes. Both regimes apply to the main economic operators and require conformity assessment before CE marking.

Software as a Medical Device

Whether software qualifies as a medical device depends entirely on its *intended purpose*. MDCG guidance (notably MDCG 2019-11 rev. 1 and MDCG 2021-24) makes clear that software performing actions on data beyond storage, archiving, communication, or simple search—and doing so for a medical purpose such as diagnosis, prevention, monitoring, prediction, prognosis, treatment, or alleviation of disease—is likely to fall under the MDR as medical device software (MDSW).

The intended purpose is established by the manufacturer's claims in labelling, instructions for use, promotional material, and other communications. A manufacturer cannot avoid MDR obligations by simply stating "no medical purpose" in technical documentation if marketing or real-world use indicates otherwise. Competent authorities and notified bodies will assess intended purpose holistically.

Conversely, software that only digitises administrative workflows, stores data without clinical interpretation, or provides general wellness information without a specific medical purpose is generally out of scope. Examples include appointment systems, basic fitness trackers with no health claims, and electronic health record systems that only store and display information. However, the boundary is

case-specific: adding even a single feature that performs clinical analysis may bring the product within MDR scope. Companies should therefore assess regulatory status early and re-evaluate it whenever functionality or intended purpose changes.

Classification and Rule 11

The MDR classifies devices into four risk classes—Class I, IIa, IIb, and III—according to Annex VIII. For software, Rule 11 is the key rule. Under Rule 11:

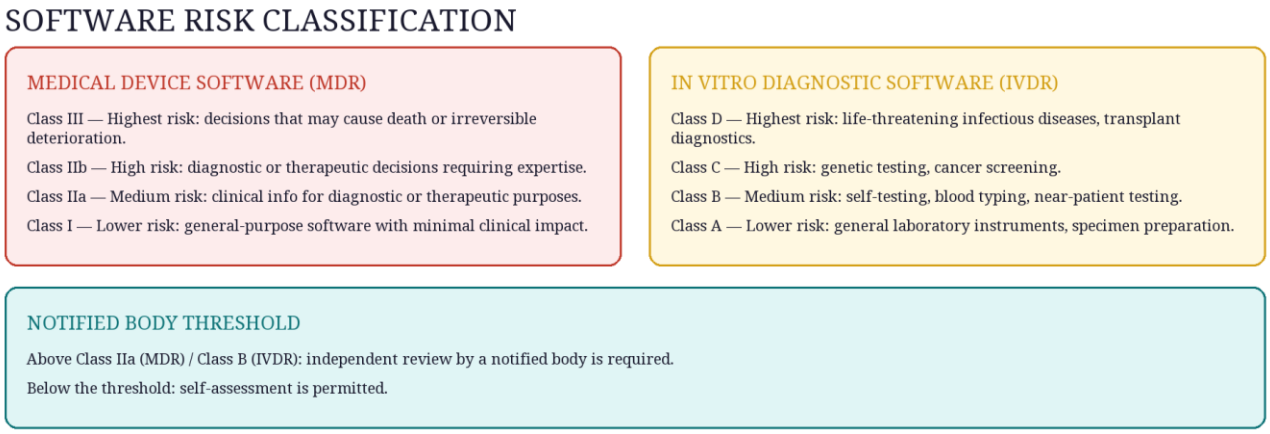
- software that provides information used for diagnostic or therapeutic decisions is Class IIa,
- unless incorrect decisions could cause serious deterioration of health or require surgical intervention (Class IIb),
- or could lead to death or irreversible deterioration (Class III).

Software used to monitor physiological processes is Class IIa, unless it monitors vital parameters where variations could pose immediate danger, in which case it is Class IIb. All other software is Class I. In practice, most software supporting diagnosis or treatment will fall into Class IIa or higher and therefore require notified-body involvement. Class I devices may be self-certified, except those that are sterile, have a measuring function, or are reusable surgical instruments.

Other MDR classification rules may also apply to software, such as Rule 10 (active therapeutic devices with diagnostic function) or Rule 22 (software controlling or influencing a device), which may result in a higher class than Rule 11 alone.

IVDR Considerations

Diagnostic software may instead fall under the IVDR, which has four risk classes (A–D). Software that analyses laboratory or genetic data to support a diagnosis may be covered by the IVDR and will require supporting evidence and formal conformity assessment. Although transition periods have been extended, new products must already comply with the core evidence, quality-system, and follow-up requirements.



Pre-market obligations

Before placing a medical device or IVD on the EU market, manufacturers must meet a comprehensive set of requirements:

- **Quality Management System (QMS):**
  Manufacturers must establish and maintain a QMS covering the entire product lifecycle—from design and development to production, post-market surveillance and vigilance.
  For SMEs, the QMS is often the most resource-intensive element of MDR compliance and must be planned early, not treated as a last-minute certification step.
- **Technical Documentation:**
  Manufacturers must prepare technical documentation showing compliance with the General Safety and Performance Requirements (GSPRs). This includes:
  - a description of the device and its intended purpose
  - design and manufacturing information
  - risk-management results
  - clinical evaluation (MDR) or performance evaluation (IVDR)
  - post-market surveillance planning
    For software, the documentation must also address the software lifecycle, version control, cybersecurity measures, and the handling of known anomalies.
- **Risk Management (ISO 14971):**
  Manufacturers must carry out a risk-management process covering risk identification, estimation, evaluation, control and ongoing monitoring.
  For software, this includes:
  - safety risks (e.g., incorrect outputs that could lead to clinical harm)
  - security risks (e.g., vulnerabilities affecting integrity or patient data)
    The risk-management file must be continuously updated based on new information, including post-market data.

- **Conformity Assessment and CE Marking:**
  Devices above Class I must undergo a conformity assessment by a notified body and obtain a CE certificate.
- **Registration and Traceability:**
  All devices must be registered in EUDAMED before market placement and assigned a Unique Device Identifier (UDI) to ensure traceability through the supply chain.

Post-market obligations

After a device is placed on the market, manufacturers must maintain:

- a **post-market surveillance system**
- **periodic safety update reports** (PSURs)
- **vigilance reporting** for serious incidents
- **post-market clinical follow-up** (PMCF) for higher-risk devices

Practical considerations for SMEs

In addition to the core requirements, SMEs should consider the following:

- **Define the intended purpose precisely.**
  Overly broad or ambitious claims can result in a higher classification or bring a product inside the MDR when it might otherwise fall outside it.
- **Plan for notified-body timelines.**
  Class IIa and higher devices require notified-body involvement, and current audit lead times must be factored into development and market-entry plans.
- **Assess changes after certification.**
  Software updates or algorithm modifications must be evaluated to determine whether they constitute a "significant change," potentially requiring new or supplementary conformity assessment.

Pending reform. On 16 December 2025, the European Commission published a proposal to amend the MDR and IVDR with the stated aim of simplifying and reducing the regulatory burden for medical devices and IVDs.If adopted, the proposal could affect classification rules, conformity assessment procedures and post-market obligations. Companies should monitor the proposal as part of medium-term regulatory planning, but should continue to plan against the current MDR and IVDR framework unless and until the amendments are enacted and in force.

Artificial Intelligence Act ((EU) 2024/1689)

The AI Act creates EU-wide rules for AI, with different obligations starting at different times. The Regulation entered into force on 1 August 2024, and its obligations apply in four phases:

- the general provisions and the prohibitions on unacceptable AI practices have applied since 2 February 2025
- the obligations for providers of general-purpose AI (GPAI) models have applied since 2 August 2025
- the obligations for limited-risk AI systems and for certain high-risk AI systems (including those classified as high-risk under Annex I, Section A, which covers AI systems embedded in products subject to EU product-safety legislation such as the MDR and IVDR) will apply from 2 August 2026
- the obligations for the remaining high-risk AI systems listed in Annex III will apply from 2 August 2027

For companies making AI-enabled medical devices, the key date is **therefore 2 August 2026**. From then, the full set of high-risk AI requirements will apply to AI systems that are safety components of, or are themselves, medical devices subject to third-party conformity assessment.

The regulatory structure is built on a tiered classification model that assigns obligations according to the **level of risk** an AI system poses to health, safety and fundamental rights. As a threshold matter, the AI Act applies only to AI systems as defined in Article 3(1). **An AI system** is a machine-based system designed to operate with varying levels of autonomy, that may adapt after deployment, and that — for explicit or implicit objectives — works out from the input it receives how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments.

> Simple software and deterministic decision-making systems that follow human-set rules without inference, autonomy or adaptiveness do not fall within this definition and are not subject to the AI Act. Companies should assess at an early stage whether their product meets the AI system definition, as this determines whether the AI Act applies at all.

At the top of the risk hierarchy, certain AI practices that pose an unacceptable risk are banned outright (Article 5). These bans have applied since 2 February 2025. While the banned practices are mainly directed at public authorities and surveillance contexts rather than at health-technology companies, SMEs should be aware of them because certain product features or use cases in the health domain could, if not carefully designed, approach the boundaries of the bans. The banned practices include, for example:

- **Social scoring** by public authorities — that is, evaluating or classifying people based on their social behaviour or personal characteristics in a way that leads to harmful or unfavourable treatment. While this ban is directed at public authorities, SMEs developing patient risk-stratification tools, treatment-adherence scoring systems or behavioural health platforms should make sure that their products do not function in a way that could be seen as evaluating individuals based on social behaviour for purposes unrelated to a legitimate and specific medical objective.
- Certain forms of **real-time remote biometric identification** in publicly accessible spaces for law enforcement purposes. Real-time remote biometric identification refers to the use of AI

systems that process biometric data such as facial images or other physical characteristics captured in real time from persons physically present in a public space, to identify those persons without their prior knowledge or active cooperation. While this ban is directed at law enforcement and public security contexts, it is relevant for health-technology SMEs in two respects.

⇒ Companies developing patient identification, access-control or monitoring systems that rely on biometric data (such as facial recognition for patient check-in, iris scanning for identity verification in clinical settings, or gait analysis for fall-risk monitoring) should assess whether their system's technical design and deployment context could bring it within the scope of the ban — particularly where the system operates in spaces that may be considered publicly accessible, such as **hospital lobbies, emergency departments or outpatient waiting areas**.

⇒ Even where a biometric system falls outside the ban because it is not deployed in a publicly accessible space or is not used for identification purposes as contemplated by Article 5, the use of biometric data in health applications remains subject to the GDPR's strict conditions for processing biometric data and the AI Act's transparency obligations for **emotion-recognition and biometric-categorisation** systems.

The AI Act also provides several exemptions from its scope that are relevant to health-technology companies:

- AI systems used exclusively for national security or defence purposes
- AI systems used solely for the purpose of scientific research and development
- AI systems that are still in the research and development phase before being placed on the market or put into service
- Non-professional use of AI systems
- Free and open-source AI software is generally exempt, unless it is placed on the market or put into service as a prohibited AI practice or as a high-risk AI system, and transparency obligations continue to apply to open-source systems that interact with natural persons

The AI Act assigns obligations to different actors in the AI value chain depending on their role. The three main roles relevant to health-technology companies are:

Role	Definition
Provider	A person, company or organisation that develops an AI system or GPAI model, or has one developed on its behalf, and places it on the market or into service under its own name or trademark. The provider carries the primary compliance obligations under the AI Act, including those for high--risk AI systems and GPAI models.
Deployer	A person, company or organisation that uses an AI system under its authority. In healthcare, deployers are typically hospitals, wellbeing services counties or other care providers who procure and use AI--enabled products in clinical settings. Deployers of high--risk systems must follow the provider’s instructions, ensure human oversight and monitor system operation.
Downstream provider	A provider of an AI system that integrates an AI model supplied by another party, whether via licence, API or other technical means.

The distinction between a deployer and a downstream provider is important: a company that merely uses an AI system as provided is a deployer, but a company that integrates an AI model into its own system and places that system on the market becomes a downstream provider and takes on the corresponding provider obligations. In practice, the following indicators suggest that the integration is substantial enough to make a company a downstream provider rather than a deployer:

- the company retrains or fine-tunes the model;
- the company changes the intended purpose of the system;
- the company builds a new user interface that influences the model's outputs; or
- the company chains multiple models into a new clinical decision-support process.

All downstream providers are deployers, but not all deployers are downstream providers. Companies should assess their role carefully, as the obligations differ significantly.

The AI Act applies to providers placing AI systems on the market or putting them into service in the EU, to deployers established or located in the EU, to providers and deployers located outside the EU where the output of their AI system is used in the EU, and to importers, distributors and authorised representatives of AI systems. Affected persons located in the EU are also within the Regulation's protective scope. The AI Act therefore has extraterritorial reach: a non-EU company whose AI-enabled health product generates outputs used by healthcare providers or patients in the EU is subject to the Regulation.

Below the banned tier, AI systems that pose a **high risk** to health, safety or fundamental rights must meet comprehensive mandatory requirements before they may be placed on the market. In healthcare, the high-risk classification is of central importance. An AI system is classified as high-risk where two conditions are both met:

- first, the AI system is intended to be used as a safety component of a product covered by EU harmonisation legislation listed in Annex I, Section A, or the AI system is itself such a product; and
- second, the product or safety component is required to undergo a third-party conformity assessment under that harmonisation legislation.

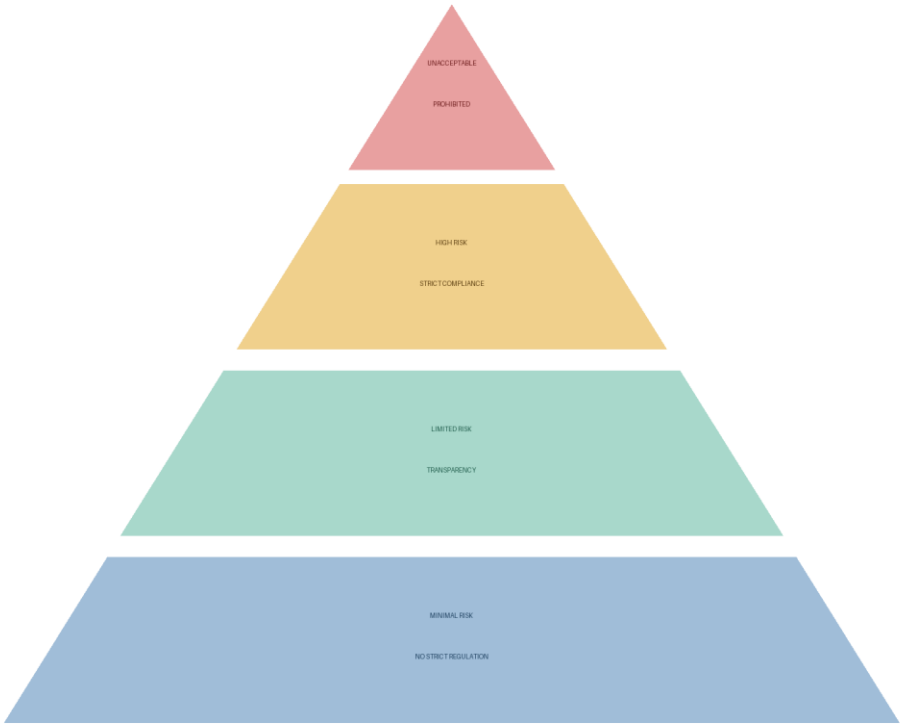
Because the MDR and IVDR are listed in Annex I, Section A, an AI system that is itself a medical device, or a safety component of one, is high-risk under the AI Act if it requires notified body conformity assessment. In practice, this generally covers MDR Class IIa, IIb and III devices, Class I sterile or measuring devices, and IVDR Class B, C and D devices or Class A sterile IVDs, but not Class I non-sterile, non-measuring medical devices or Class A non-sterile IVDs.

In-house devices manufactured and used within the same healthcare institution under Article 5(5) of the MDR or IVDR are also not high-risk under the AI Act, because they do not undergo third-party conformity assessment. However, the AI Act's general obligations — including the AI literacy obligation under Article 4 — apply to all AI users, including healthcare institutions using in-house AI devices.

High-risk AI systems must comply with requirements on:

- risk management

- data governance
- technical documentation
- transparency and human oversight
- accuracy, robustness and cybersecurity and
- must undergo a conformity assessment before being placed on the market.



Below the high-risk tier, the AI Act distinguishes between limited-risk and minimal-risk AI systems, each subject to a much lighter regulatory burden.

Limited-risk AI systems are mainly subject to transparency obligations. In practice, users should be told when they are interacting with AI or receiving AI-generated content, including in tools such as chatbots, symptom checkers and AI-assisted analysis reports.

Minimal-risk AI systems — that is, systems that are neither banned, high-risk nor subject to the limited-risk transparency obligations — are not subject to mandatory requirements under the AI Act. The vast majority of AI applications fall into this residual category. For such systems, the AI Act encourages but does not require providers to voluntarily adopt codes of conduct addressing, for example, environmental sustainability, accessibility, stakeholder participation and diversity in development teams.

Health AI products

Whether a health AI product is classified as *high-risk* under the AI Act depends largely on its MDR or IVDR classification. The AI Act automatically treats AI systems embedded in medical devices that require **third-party conformity assessment** as high-risk. In practice:

- **Not high-risk:**
  - MDR Class I (non-sterile, non-measuring)
  - IVDR Class A (non-sterile)
- **High-risk:**
  - MDR Class I (sterile, measuring, or reusable surgical)
  - MDR Class IIa, IIb, III
  - IVDR Class A (sterile), B, C and D

In-house devices Devices developed and used internally within the same healthcare institution under Article 5(5) MDR/IVDR do **not** undergo third-party assessment and are **not high-risk** under the AI Act. This exception is particularly relevant for hospitals and research institutions developing internal-use AI with no commercial distribution. However, **AI literacy obligations (Article 4)** still apply to healthcare institutions deploying in-house AI.

This MDR/IVDR–AI Act linkage produces several practical consequences:

- **Class I software may fall outside the AI Act's high-risk category.** If a software product is legitimately classified as MDR Class I, no third-party assessment is required and the AI Act's high-risk obligations are not triggered — even if the software performs meaningful clinical functions. However, **Class I software classification is a contested area**, and borderline interpretations are common.
- **Upgrading functionality can upgrade the risk class**If the same app is redesigned to analyse symptoms and **suggest a diagnosis**, it would likely shift to MDR Class IIa or higher. This automatically places it in the AI Act's high-risk category and activates the full set of AI-specific obligations. The boundary between "displaying clinical information" and "suggesting a diagnosis" is often unclear and must be evaluated carefully.

Some AI-enabled health apps fall outside MDR entirely

A general wellness app that tracks sleep patterns without a medical purpose is not a medical device and therefore not high-risk through the MDR/IVDR pathway.
But the **wellness vs. medical device** distinction is one of the most contested questions in digital health:

- A sleep-tracking app that **only records data** is unlikely to be a medical device.
- If the same app claims to **detect sleep apnoea** or provide **clinically actionable insights**, it may acquire a medical purpose and enter MDR scope.

Looking ahead

The boundaries between MDR/IVDR classification and AI Act high-risk status are not always clear-cut. The European Commission is expected to issue further guidance and harmonised standards to support consistent interpretation and help companies determine the correct regulatory pathway.

MDR and AI Act Interplay

Having addressed the classification questions that determine whether a product falls within the AI Act's high-risk category, the next issue is what happens when the answer is yes. Where a product is simultaneously a medical device under the MDR and a high-risk AI system under the AI Act, both regulatory frameworks apply at the same time — one does not displace the other. However, the AI Act is designed to avoid unnecessary duplication. Under Article 8(2), manufacturers may integrate the AI Act's requirements into the existing MDR or IVDR documentation and compliance processes, rather than maintaining separate parallel systems. In practice, this means that the same risk management system and quality management system may serve both the MDR and the AI Act, provided that compliance with both sets of requirements is ensured. The relationship between the two is structured as follows:

- The MDR governs the safety, performance and clinical evaluation of the device as a product placed on the market, including post-market surveillance and vigilance obligations.
- The AI Act adds a further layer of requirements directed specifically at the AI component, including data governance for training, validation and testing datasets, transparency obligations towards users, human oversight measures, and standards of accuracy, robustness and cybersecurity.

For high-risk AI medical devices, AI Act conformity assessment is integrated into the MDR or IVDR process. The same notified body reviews both frameworks as part of a single procedure, so companies should confirm early that their chosen notified body has the necessary competence.

> **Companies that have not yet begun preparing an AI Act compliance plan alongside their MDR conformity-assessment process should treat this as urgent. The dual-compliance requirement cannot be addressed retroactively at the point of CE marking. Both sets of obligations must be satisfied before the product may be placed on the market.**

Operational steps for SMEs preparing for dual MDR and AI Act compliance:

- Assess whether the company's AI-enabled product is classified as high-risk under the AI Act by virtue of its MDR or IVDR classification, and document that assessment.
- Conduct a gap analysis comparing the company's existing MDR quality management system and technical documentation against the AI Act's requirements on data governance, bias testing, transparency, human oversight and post-market monitoring.
- Develop an integrated compliance plan and timeline that addresses both MDR and AI Act obligations in parallel, rather than treating AI Act compliance as a subsequent step after CE marking.
- Engage with the notified body at an early stage to confirm its readiness and capacity to assess AI Act requirements as part of the MDR conformity-assessment procedure and factor any additional lead times into the product-launch schedule.
- Reassess the planned market-entry timeline considering the 2 August 2026 deadline and identify whether any interim measures — such as placing the product on the market before that date under the MDR alone, where permissible — are available and advisable.

5. Data Sharing and Interoperability

A third dimension of the regulatory landscape concerns the movement of data between organisations, systems and Member States.

The GDPR imposes specific requirements on data transfers and on the respective roles of controllers and processors. The Data Governance Act and the Data Act introduce additional obligations governing data intermediation, access rights and portability that apply alongside the GDPR rather than replacing it.

This is particularly relevant for platforms that depend on cross-organisational or cross-border data flows. A single transfer of pseudonymised patient data may trigger multiple requirements at once, including a GDPR lawful basis, Secondary Use Act permit and secure-processing rules, the relevant controller/processor arrangements, any applicable GDPR Chapter V transfer mechanism, and, once fully applicable, EHDS interoperability and access conditions.

The instruments discussed below — the Data Governance Act, the EHDS and the Data Act — each address a different aspect of this problem, but they do not form a single coherent code. They were adopted at different times, pursue partially overlapping objectives, and contain interaction clauses whose practical effect is not yet fully tested. Companies must therefore assess each data flow against each applicable instrument individually, rather than assuming that compliance with one framework satisfies the requirements of the others.

Data Governance Act ((EU) 2022/868)

Current law. The DGA establishes trusted mechanisms for voluntary data sharing, including recognised data intermediaries and the framework for European common data spaces. For health data, the DGA is particularly relevant in two respects.

1) It sets conditions for the re-use of protected data held by public-sector bodies, including health data, but does not itself create a right of access. In Finland, those conditions operate alongside the Secondary Use Act and the Findata permit process, and their precise interaction remains unsettled.

2) The DGA introduces a regulatory framework for data intermediation services. These are entities that facilitate data sharing between data holders and data users without themselves using the data for their own purposes. In the health context, this raises the question of whether platforms that aggregate or broker access to health data, for example platforms connecting hospitals with research organisations or technology companies, must register as recognised data intermediation services and comply with the associated neutrality, transparency and governance requirements.

European Health Data Space (EHDS)

Current law. The EHDS (Regulation (EU) 2025/327), which entered into force on 26 March 2025 with phased application thereafter, establishes a sector-specific governance framework for both primary and secondary use of electronic health data across Member States.

Current interpretation / caution. The EHDS does not replace the GDPR but builds on it, adding health-sector-specific rules on data quality, interoperability, prohibited purposes and governance. Several aspects of the EHDS framework are subject to ongoing debate.

Topic	Description
1.Findata and National Data Access Bodies	Finland's Findata is one of the most advanced national health-data access systems in the EU. Under the EHDS, Member States must appoint health data access bodies with functions similar to Findata. Companies holding existing Findata permits should expect that permit conditions may evolve as the EHDS is implemented.
Interoperability and Primary-Use Data Exchange	The EHDS requires electronic health data to be available in standardised formats enabling cross-border exchange. For countries with strong national infrastructures such as Finland's Kanta Services, the challenge is adapting national systems to the EU format without disrupting workflows. Companies integrating with Kanta may need technical updates once EHDS implementing acts define specific formats and standards.
Prohibited Purposes for Secondary Use	The EHDS bans certain secondary-use purposes, including decisions detrimental to individuals, advertising and marketing, and insurance underwriting. The prohibitions are broadly drafted, and borderline scenarios—such as using health data to develop a product later used in insurance, or using anonymised insights to inform commercial strategy—will require careful interpretation.
Cross-Border Governance and HealthData@EU	The EHDS introduces a new governance model for cross-border secondary use, involving the HealthData@EU infrastructure and a shared supervisory mechanism between the data holder's Member State and the applicant's Member State. This has no direct precedent in existing data-protection law. Companies operating cross-border should monitor implementing and delegated acts that will specify technical standards, formats and access conditions.

Examples of SME opportunities. The EHDS could make health-data access, interoperability and cross-border reuse more scalable across the EU.
Examples include:

- digital-health applications that connect more easily to EHR and e-prescription systems across Member States;

- AI, diagnostic and decision-support tools validated on broader secondary-use datasets through HealthData@EU; and

Data Act ((EU) 2023/2854)

Current law. The Data Act defines rules for access to and use of data generated by connected products and related services. It enables more balanced data sharing between manufacturers, users and public-sector bodies. In the health context, the Data Act is relevant where connected medical or wellness devices generate usage data. Users have a right of access to that data and may request its transfer to third parties, subject to trade-secret protections and GDPR safeguards.

Issue	Description
Data Act user access rights vs. MDR obligations	The interaction between the Data Act and the MDR remains unsettled. Connected medical devices generate data relevant both to the user's access rights under the Data Act and to the manufacturer's MDR post-market surveillance obligations, and it is unclear whether those MDR rules count as sector-specific "equivalent" access rights.
Trade-secret protection under the Data Act	The Data Act's trade-secret provisions create tension in health contexts. Manufacturers may argue that algorithms, calibration parameters or proprietary data formats embedded in device-generated data are trade secrets that limit user access. While the Data Act allows "reasonable measures" to protect trade secrets, it prohibits using trade-secret claims to undermine access rights entirely. The line between valid protection and unlawful obstruction is case-specific and may differ depending on whether the product is a regulated medical device (with additional MDR transparency obligations) or a general wellness device.
Data Act vs. EHDS access frameworks	The EHDS introduces its own access framework for electronic health data, including certain wellness-app data. When a connected product generates data that falls under both the Data Act and the EHDS (primary-use or secondary-use), the applicable access rules, transfer mechanisms and governance obligations may differ. Determining which Regulation takes precedence or whether both apply concurrently depends on the facts and on each Regulation's interaction clauses. Companies should expect interpretive uncertainty until EU-level guidance is issued and design systems flexible enough to adapt to evolving requirements.

Taken together, these instruments create a layered legal framework for health data sharing. In practice, organisations must assess not only the substantive access rules but also: the applicable data-transfer mechanism under GDPR Chapter V where data crosses borders; the contractual arrangements between joint controllers or controller-processor relationships; and any sector-specific conditions imposed by the EHDS, the Secondary Use Act or the relevant data controller.

6. CYBERSECURITY

For companies working with health data, cybersecurity is not a single obligation but a composite requirement arising from multiple overlapping instruments — the GDPR (Article 32), the MDR, the AI Act and the **NIS2 Directive (Directive (EU) 2022/2555)** — each with its own scope, supervisory authority and enforcement mechanism.

The NIS2 Directive, which replaced the original NIS Directive and had to be transposed into national law by 17 October 2024, significantly expands EU cybersecurity obligations. Entities are classified as essential or important based on sector, size and societal impact. In healthcare, essential entities typically include hospitals, healthcare providers, reference laboratories and manufacturers of critical medical devices. Important entities may include smaller healthcare providers and health-technology platforms.

The substantive obligations under NIS2 cover four main areas:

Obligation Area	Description
Risk Management	Requires comprehensive and proportionate cybersecurity measures, including incident handling, business continuity, supply--chain security, vulnerability handling and disclosure, and encryption.
Incident Reporting	Obligates entities to provide: (i) an early warning within **24 hours**, (ii) an incident notification within **72 hours**, and (iii) a final report within **one month**.
Governance	Places direct responsibility on management bodies to approve, oversee and ensure the implementation of cybersecurity measures; also requires management--level cybersecurity training.
Supply--Chain Security	Requires organisations to assess and address cybersecurity risks in supplier and service--provider relationships, including through contractual cybersecurity requirements.

For SMEs, NIS2 matters not only through direct scope rules but also through the supply chain: hospitals and wellbeing services counties increasingly pass NIS2 requirements down through procurement and supplier qualification processes. As a result, SMEs may face contractual obligations on risk management, incident reporting and compliance assurance even where they are not themselves classified as essential or important entities.

The interaction between NIS2 and other applicable instruments raises several points. NIS2 and the GDPR are complementary rather than substitutive: compliance with one does not discharge obligations under the other, and a single security incident may trigger reporting obligations under both, with different timelines and addressees.

> **Where a product is a medical device, the manufacturer must also comply with the MDR's cybersecurity requirements (Annex I) and, for high-risk AI systems, the AI Act's requirements under Article 15. These product-level obligations apply to the manufacturer through the conformity-assessment process, whereas NIS2 applies at the entity level to the**

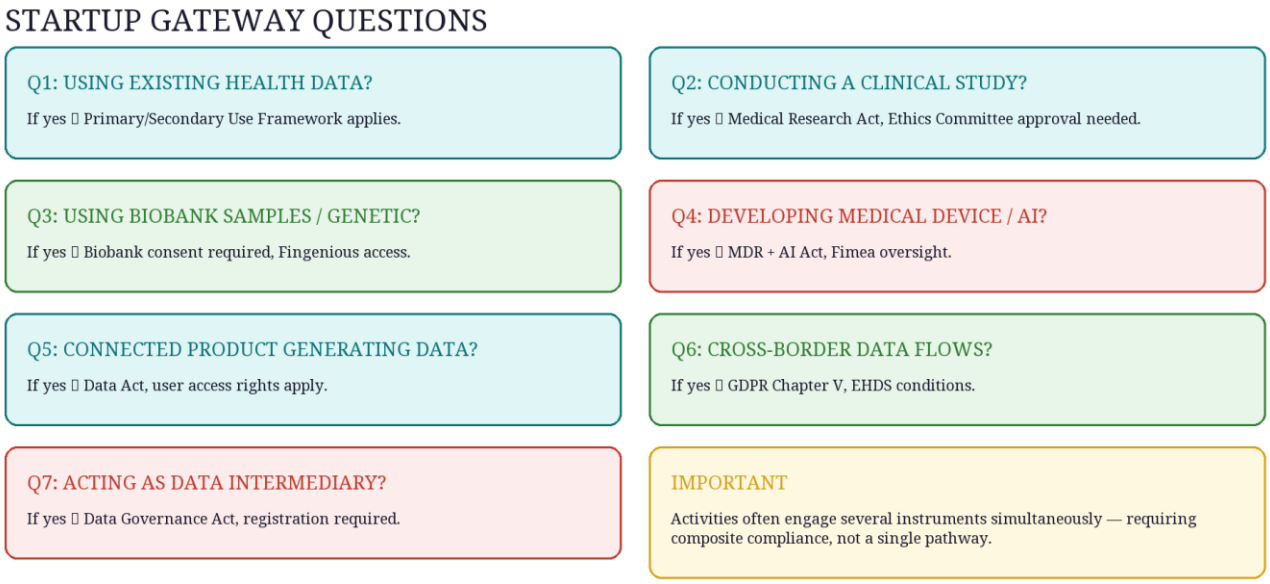
> **deploying organisation. A hospital deploying an AI-enabled medical device may therefore face cybersecurity obligations under NIS2, the GDPR, and indirectly under the MDR and AI Act. The allocation of responsibilities between deployer and manufacturer should be addressed explicitly in the relevant agreements.**

The Cyber Resilience Act (Regulation (EU) 2024/2847) establishes horizontal cybersecurity requirements for products with digital elements. However, the CRA expressly excludes medical devices and IVDs subject to the MDR or IVDR. The CRA is therefore mainly relevant for connected health products that fall outside those frameworks, such as general wellness devices, hospital IT infrastructure components or non-medical software used in healthcare settings.

In Finland, NIS2 has been implemented through national cybersecurity legislation. Supervisory competence is allocated to sector-specific authorities. In healthcare, Valvira handled matters until the end of 2025, but from 1 January 2026 all of Valvira's tasks transfer to the Finnish Supervisory Agency LVV, which continues pending matters automatically. Traficom's National Cyber Security Centre (NCSC-FI) retains a cross-sector coordination and technical guidance role. Entities classified as essential or important must register with the competent authority, implement risk-management measures and comply with incident-reporting obligations.

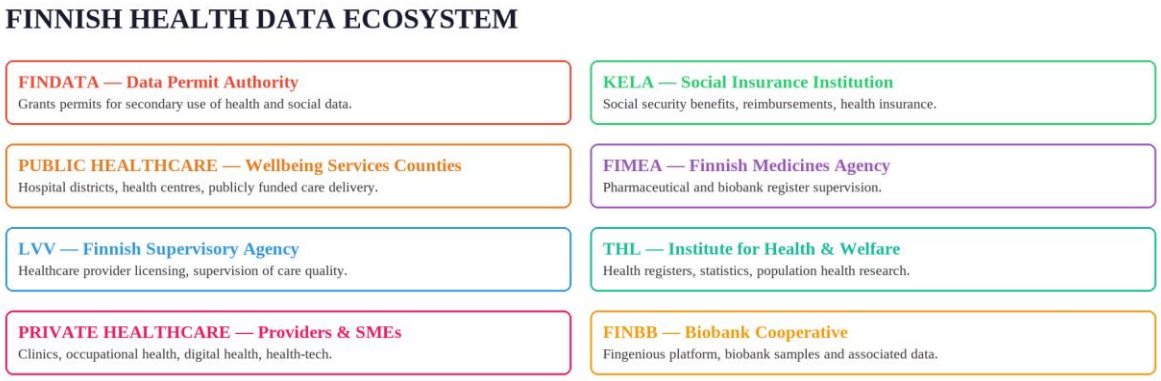
Wellbeing services counties and hospital districts are increasingly incorporating NIS2-aligned requirements into their procurement frameworks, and demonstrating compliance with recognised standards such as ISO/IEC 27001 may facilitate market access in the Finnish healthcare sector.

For SMEs, the practical takeaway is that cybersecurity in the health data context is a multi-layered obligation. The applicable requirements depend on the company's role, the nature of its product and the regulatory status of its customers. Companies should map which instruments apply directly and which apply indirectly through supply-chain obligations, identify gaps or conflicts, and make sure that their cybersecurity governance, incident-response procedures and contractual arrangements address each applicable layer.



7. Key Organisations in the Finnish Health Data Ecosystem

This section identifies the key organisations in the Finnish health data ecosystem and their respective roles, providing a practical reference for companies seeking to understand which authority is responsible for which aspect of the regulatory framework discussed above.



National Health Data Infrastructure

- **Finland's Wellbeing Service Counties** act as the primary data controllers for regional health and social care data. They must ensure lawful and secure processing under the GDPR and Finnish data protection law, compliance with the Secondary Use Act for research and innovation uses, and compliance with NIS2 obligations as essential entities.
- **Private health and social care providers** also act as independent data controllers for the personal data they collect and process in providing their services. They are subject to the same

GDPR obligations discussed above and, where they deploy medical devices or AI systems, to the MDR and AI Act requirements addressed in the product-safety section. Where applicable, private providers must integrate with national data systems such as Kanta Services, and the interoperability obligations anticipated under the EHDS will apply to them in the same way as to public-sector providers once the Regulation is fully implemented.

- **Kela** operates **Kanta Services**, Finland's national digital health infrastructure, including electronic prescriptions, patient records, and citizens' access to their own health information.

Health Data Governance & Secondary Use

- **Finnish Institute for Health and Welfare (THL)** Maintains national health registers, produces health statistics, and conducts public health research.
- **Findata** Grants permits for the secondary use of health and social data for research, innovation, statistics, and policymaking. Operates under THL.
- **Fingenious® service** is a national service that provides a single access point to Finnish biobank data and samples. It allows companies and researchers to apply for access to biological samples and associated health data collected by **Finnish biobanks**. Fingenious® service also provides access to datasets generated in large-scale research initiatives, such as the FinnGen study, enabling further research and development based on existing data resources. Access is subject to biobank consent, project approval, and ethical and legal requirements.

Regulation & Supervision

- **Finnish Supervisory Agency (LVV)** — Supervises healthcare and social welfare providers and professionals in Finland. LVV is responsible for licensing, national guidance and ensuring patient safety and service quality. In the context of the regulatory framework discussed above, LVV oversees the activities of healthcare providers and professionals, including the deployment of health technologies in clinical settings. This is relevant for companies whose products are used by regulated healthcare organisations.
- **Regional State Administrative Agencies (AVI)** — Regional authorities responsible for supervising healthcare and social services at the regional level. They work together with Valvira to ensure consistent national oversight and may be involved in the supervision of Wellbeing Counties' compliance with data protection, service quality and cybersecurity obligations discussed in the preceding sections.
- **Finnish Medicines Agency (Fimea)** — Regulates medicines, clinical trials, and pharmacovigilance in Finland. Fimea is also the competent authority for medical devices and in vitro diagnostic devices under the MDR and IVDR, responsible for market surveillance of medical devices placed on the Finnish market. In this capacity, Fimea may, as noted in the product-safety section, determine that a product has been incorrectly classified by its manufacturer and require reclassification. Fimea also participates in EU regulatory cooperation through the European Medicines Agency and the Medical Device Coordination Group.

Digital Infrastructure & Cybersecurity

- **Finnish Transport and Communications Agency (Traficom)** — Hosts the National Cyber Security Centre (Kyberturvallisuuskeskus, NCSC-FI), which serves as Finland's general

cybersecurity authority responsible for situational awareness, incident coordination and technical guidance. Under the Finnish cybersecurity legislation implementing NIS2, however, supervisory competence is allocated to sector-specific authorities rather than centralised under Traficom. For the healthcare sector, matters handled by Valvira until the end of 2025 transferred to LVV from 1 January 2026. Traficom and the Kyberturvallisuuskeskus retain a coordinating role across sectors, maintain the national incident-reporting infrastructure and provide technical cybersecurity guidance that is relevant to all entities, including those in healthcare. Companies operating in the health data space should therefore engage with LVV for sector-specific NIS2 compliance from 2026 onward, and with the Kyberturvallisuuskeskus for technical cybersecurity resources and incident coordination.

8. Why Finland Is an Attractive Environment for Health Data Innovation

Despite the regulatory complexity, Finland offers a structured and accessible environment for health data research and innovation in the EU. Key advantages for SMEs include:

- a highly digitalised, publicly funded healthcare system and strong political support for e-health, which enable national coordination and deployment;
- decades of health-IT investment, extensive electronic patient data and a long track record of using data for care, research and innovation;
- Kanta Services, which provide interoperable health records, e-prescriptions, patient repositories and citizen access through My Kanta;
- high public trust, a clear legal framework and policy support for prevention, patient empowerment and cost-effective care;
- high-quality national registers and longitudinal datasets that support real-world-evidence research and product development;
- an early-mover advantage in adapting to the EHDS, AI Act and other EU-level rules.

For SMEs, Finland combines regulatory rigour with digital, institutional and research strengths that support health-data innovation. Companies that engage early with the legal framework and relevant partners will be better placed to access data, validate products and bring solutions to market in Finland and across the EU.

Startup Quick Guide:
Using Health Data in Finland

1. What Are You Doing?

A: Patient Care	Development / Analytics	Clinical Study
Primary Use	Secondary Use	Ethical Review
No Findata Permit	Findata Permit	Ethics Approval

2. Can You Access Data Directly?

YES	NO
Part of Care Delivery	External Company
Internal Use Only	Apply via Findata

3. What Do You Get?

- Secure Environment
- Aggregated Results
- Anonymized Outputs

Step 4: Before You Start

Secure Environment | Aggregated Results | Anonymized Outputs

Operating Models:

- DPIA Assessment
- Security Audit
- Legal Agreement
- Use Case Defined

1 Controlled Access

- ✓ Findata Permit
- ✓ Secure Environment

2 Research Collaboration

- ✓ Partner with Hospital / University

3 Synthetic Data

- ✓ No Personal Data

Key Takeaway:

Health data is available for innovation – ***but access is controlled and regulated.***

9. REGULATORY SANDBOXES

Regulatory sandboxes are an emerging innovation tool. Under Article 57 of the AI Act, Member States must ensure that at least one national AI regulatory sandbox is operational by 2 August 2026. A sandbox is a controlled, time-limited environment in which providers can develop, test and validate innovative AI systems under a competent authority's supervision, with guidance on regulatory requirements and risk mitigation. The framework also provides for written proof of sandbox activities and exit reports that may support later conformity-assessment and market-surveillance processes. In the MDR/IVDR context, the same logic could be adapted to medical devices and IVDs, including, where appropriate, clinical investigations, performance studies and other real-world testing activities.

More broadly, sandbox frameworks in the health-technology field would likely be linked to the wider innovation infrastructure being developed around the AI Act rather than built as wholly separate systems. In practice, that could involve structures such as European Digital Innovation Hubs (EDIHs), Testing and Experimentation Facilities (TEFs), data spaces such as the EHDS and AI Factories, alongside research infrastructures, university hospitals and other specialised actors with medical-device expertise.

From an MDR/IVDR perspective, the value of sandboxes would lie in providing a controlled setting in which to test innovative solutions and generate evidence for regulatory decision-making, particularly where novel products raise difficult borderline or cross-regime questions.

Such an approach could combine early regulatory guidance with a more closely supervised testing environment, helping innovators address qualification, classification and the interaction of overlapping regimes such as the MDR, IVDR, AI Act and EHDS. It would also raise practical questions about the roles of competent authorities, expert panels and notified bodies, and about how sandbox outputs should relate to later conformity-assessment processes. For Finland, an infrastructure-linked arrangement of this kind could reduce regulatory uncertainty for SMEs, improve readiness, make better use of existing public and research capacity and support faster market access without compromising patient safety.

10. REGULATION TECHNOLOGIES (REGTECH)

For many SMEs, the volume, complexity and pace of change of the applicable requirements present a significant operational challenge. Regulation Technologies (RegTech) is a developing field that seeks to address this challenge by using technology to help companies navigate the complex regulatory landscape and make technology-enabled progress without sacrificing compliance.

Examples of service providers in this area:

- **Lean Entries** is a Finland-based company that operates a subscription-based online platform providing tools and information to help medical device companies save time and effort in achieving compliance with global regulatory requirements. The platform offers solutions for

regulatory strategy, documentation management and submission readiness, with coverage spanning the MDR and related regulatory frameworks.

- **Data Privacy Designer** is a Finnish company, that provides a software platform and advisory services for data protection, information security and regulatory compliance. The platform enables organisations to map and visualise data flows, assess risks and manage compliance obligations across data protection, AI regulation and related frameworks such as the Data Act. Core functionalities include automated data mapping, Data Protection Impact Assessments (DPIA), risk assessment and documentation management. In addition to its software tools, the company offers consulting services supporting responsible data processing and regulatory readiness.
- **Leida.ai** is a cloud-based SaaS platform that provides AI-powered regulatory roadmaps, automated compliance documentation and real-time regulatory intelligence for the pharmaceutical and healthcare sector. The Service covers MDR, IVDR, ISO standards and global regulatory frameworks, offering features such as automated generation of technical files and declarations, dynamic classification roadmaps, centralised evidence management for audit-readiness, and continuous monitoring of regulatory changes. The Service does not provide legally binding advice, and outputs are for informational and decision-support purposes only.

11. Key Contacts and Resources for SMEs

- AIREGU Project
  - Website: AIREGU
- European Commission – AI Act Service Desk
  - Website: AI Act Service Desk
- Findata
  - Website: Findata
  - Email**:** info@findata.fi
- Fingenious® service genious®
  - Website**:** Fingenious
  - Email**:** info@fingenious.fi
- Healthtech Finland (industry associaton)
  - Website: Healthtech Finland
- Fimea (Finnish Medicines Agency)
  - Website: Fimea
  - Email: registry@fimea.fi
- Finnish Supervisory Agency LVV
  - Website: LVV
- Ministry of Social Affairs and Health (STM)
  - Website: MSAH
- Office of the Data Protection Authority (Tietosuojavaltuutetun toimisto)
  - Website: DPA
  - Email: tietosuoja@om.fi
- Sitra TEHDAS-project
  - Website: TEHDAS
  - Email: sitra@sitra.fi

- Traficom (Finnish Transport and Communications Agency – National Cybersecurity Authority)
  - Website: Traficom
  - Email: kyberturvallisuuskeskus@traficom.fi
- TUKIJA (National Committee on Medical Research Ethics)
  - Website: TUKIJA
  - Email: tukija@gov.fi
- Business Finland
  - Website: Business Finland
  - Email: info@businessfinland.fi
- CSC – IT Center for Science
  - Website: CSC
  - Email: servicedesk@csc.fi

Regulation

EU
Artificial Intelligence (AI) Act
Data Act
Data Governance Act (DGA)
European Health Data Space Regulation (EHDS)
General Data Protection Regulation (GDPR)
In Vitro Diagnostics Regulation (IVDR)
Medical Device Regulation (MDR)
NIS 2

Finland
Biobank Act
Data Protection Act
Medical Research Act
Patient Data Act
Secondary Use Act

HealthHub Finland EDIH

Co-funded by the European Union

Credits

The handbook has been prepared within the HealthHub Finland EDIH initiative, which is co-funded by the European Commission's Digital Europe Programme and Business Finland, the Finnish government organization for innovation funding and trade, travel and investment promotion.

HealthHub Finland EDIH is coordinated by Business Turku Ltd.

EDIH European Digital Innovation Hubs Network

BUSINESS FINLAND

Co-funded by the European Union

NOTICE: The handbook is only intended as guidance and should be considered advice only.

Published: March 2026