KNOWLEDGE BASE
English edition

Patient data under the EHDS and the Data Act: a new equilibrium without ownership

Joris Bijvoets, CIPP/E | AVG Compleet B.V.

AVG Compleet knowledge base | 23 August 2026

https://avg-compleet.nl/patientgegevens-ehds-data-act/

Three new regulations, one question

Between May 2022 and March 2025, the European Union adopted three regulations that fundamentally reshape the position of data in the digital economy: the Data Governance Act (Regulation (EU) 2022/868), the Data Act (Regulation (EU) 2023/2854) and the European Health Data Space (Regulation (EU) 2025/327, published in the Official Journal on 5 March 2025). For the data protection officer (DPO) at a healthcare provider, and more broadly for anyone who works with patient data, this is no marginal development. The framework in which the electronic health record, the processor agreement with the cloud provider and the governance of scientific research operate has changed substantially.

What is conspicuously absent from these new frameworks is the vocabulary of property. None of the three regulations speaks of an "owner of data" or of a saleable personal data record. The Union legislature consistently chose a different set of concepts: access, use, sharing, opt-out, permits, supervision. In that choice, the line the GDPR set out in 2016 is recognisable: personal data are treated as the object of fundamental-rights protection, not as merchandise (Bijvoets, 2026a).

For DPO practice this creates clarity, to begin with: the old question "who do the patient data belong to?" receives a more precise answer. Under the law as it stands, they are not treated as property in the civil-law sense, but as the object of a layered structure of access and use, in which primary and secondary use each carry their own safeguards. At the same time, the complexity increases: the rules pile up (GDPR, Dutch Medical Treatment Contracts Act (WGBO), Dutch GDPR Implementation Act (UAVG), EHDS, Data Act, Data Governance Act) and the elaboration of the EHDS in national law is still under way. This blog sketches those layers, with the DPO role as its compass.

The three regulations at a glance

The **Data Governance Act** created the European infrastructure for data sharing in 2022: intermediaries ("data intermediation services"), rules for altruistic data use ("data altruism") and public data spaces. Its relationship to personal data is modest: the DGA adds no legal basis for processing and is expressly complementary to the GDPR (Article 1(3) DGA). For the DPO, the DGA is mainly relevant to data-altruism arrangements and the assessment of data intermediaries.

The **Data Act**, adopted on 13 December 2023 and largely applicable since 12 September 2025, regulates access to and use of data generated by "connected products": Internet of Things devices, vehicles, smart systems and medical devices that produce data themselves. Two core rights are central: the right of the user to request their data from the manufacturer (and to have them provided to a third party), and rules on data transfer when switching between cloud services. Under Article 50(2), the design duty in Article 3(1) applies to connected products and related services placed on the Union market after 12 September 2026.

For personal data, the Data Act explicitly reiterates that the GDPR retains priority: where the requested dataset contains personal data, the GDPR's legal bases and data-subject rights continue to apply in full (Article 1(5) Data Act). The Data Act thus creates no new property regime over personal data. What it does regulate is related to the idea behind Article 20 GDPR, but worked out in its own, broader regime of access and sharing for device-generated data (on the limits of the GDPR right, see Bijvoets, 2026b).

The greatest change for the healthcare sector lies in the **EHDS Regulation**. It pursues two aims at once: better access to and exchange of electronic health data for care (primary use), and regulated access for purposes outside care, such as research, policy and public-health monitoring (secondary use). Its general application date is 26 March 2027. Many core duties follow later: primary use for the first priority categories and Chapter IV on secondary use largely from 26 March 2029, further categories from 26 March 2031, and a limited number of elements from 2035 (Article 105 EHDS).

Primary use: control, not ownership

For primary use, the EHDS provides above all for rights of access and restriction (Articles 3 and 8 EHDS): the patient can exercise access to their electronic health data and can indicate which specific data they do not wish to make available to healthcare providers, or only to a limited extent. A directly applicable, uniform opt-out regime for primary use is not part of the regulation; the continuity and quality of care leave little room for an unbounded opt-out. Member States may, however, introduce such an opt-out nationally on the basis of Article 10 EHDS, provided it is reversible. The Dutch legislature has announced its intention to make use of that possibility (Letter to Parliament on the implementation of the EHDS, 20 January 2026).

These rights are structurally different from property rights. They rest on control (taking part or not, granting or restricting access), not on alienation. They are revocable and must be read alongside the existing GDPR rights (access, rectification, erasure) and WGBO rights (access, copies, supplementation, destruction; see Bijvoets, 2026d). A property model would enable the patient to surrender their record definitively in exchange for some benefit; the EHDS does not provide for that and thereby stays in line with the existing approach under the GDPR.

A third element deserves separate attention: the rights of control are subject to exceptions protecting vital interests. Article 10 EHDS provides that, under a national opt-out, access remains possible where the vital interests of the data subject or of another person so require. Think of a patient who has requested shielding but ends up in a life-threatening situation in which the healthcare provider nevertheless needs access to certain data (*P&I* 2024/5). Member States elaborate that exception in national law. The design of the care process therefore cannot stop at "patient has set a restriction, so no access"; there must be a procedure for vital-interest exceptions, combined with logging that will later withstand scrutiny.

Secondary use: governance through permits

For secondary use, the EHDS opts for a system that does not rest on consent per individual. Data become available in anonymised form where the purpose can be achieved that way; only where the user demonstrates that it cannot, is pseudonymised data used (Article 66 EHDS), within a secure processing environment (Article 73 EHDS). Data are moreover made available only for exhaustively defined purposes and after a national *Health Data Access Body* (HDAB) has issued a permit (Articles 53 and 68 EHDS). In addition, Article 71 EHDS gives data subjects a right to object to secondary use of their health data; the precise modalities are elaborated in national legislation (*P&I* 2025/3).

Member States may include exceptions to that right to object in national law, under the strict conditions the regulation attaches to them, such as a task in the general interest of public health (Article 71(4) EHDS; *P&I* 2024/5). Additional safeguards may apply to particularly sensitive categories, such as genetic data and data from wellness applications (a category the regulation itself addresses separately).

For the DPO at a healthcare provider there are two practical points of attention. First: according to reporting in *P&I*, existing data-source holders in the Dutch landscape (think of Vektis, Dutch Hospital Data, Nivel and the Netherlands Comprehensive Cancer Organisation) are exploring with the Ministry of Health how the coordinating role around the future HDAB will be organised; for the individual healthcare institution, the question is how its internal registration will relate to that (*P&I* 2025/6). Second: secondary use requires data suitability, not just data availability. An electronic

health record that is not coded in a standardised way yields no usable datasets; without that quality, an HDAB permit is meaningless.

The relationship with the GDPR and the WGBO

Does the EHDS set the GDPR aside? No. The GDPR continues to apply, while the EHDS lays down specific rules for access to and use of health data and itself creates statutory duties, public-interest tasks and safeguards. Depending on purpose and legal framework, Article 9(2)(g), (h), (i) or (j) GDPR may apply to special-category data; in the Netherlands Articles 24 and 30 UAVG may also be relevant. The WGBO continues to govern the treatment contract and record-keeping duty (Article 7:454 of the Dutch Civil Code), as does medical professional secrecy (Article 88 Wet BIG; Article 7:457 of the Dutch Civil Code).

A common misconception is that an HDAB permit automatically supplies the complete GDPR basis for every actor. The EHDS is itself part of the normative foundation: the holder's duty to make data available may correspond to Article 6(1)(c) GDPR and the HDAB's task to Article 6(1)(e) (see recital 52 EHDS). The user must nevertheless demonstrate its applicable Article 6 basis in the application. The data permit is therefore a necessary EHDS access condition, but not automatically the user's complete GDPR basis (Bijvoets, 2026e).

For the DPO this yields an operational check. In the case of secondary use, the organisation must be able to demonstrate which GDPR legal basis it relies on, which exception to the processing prohibition of Article 9(1) GDPR applies, and how the EHDS regime (HDAB permit, objection register, any Member State exception) is anchored alongside them. In the DPIA and the record of processing activities, that layering deserves explicit mention.

What is missing: the concept of ownership

The EHDS Regulation does not know the concept of an "owner of data". It speaks of a *health data holder*, a *health data user* and the *data subject* (the patient). The holder is the healthcare provider or other entity that manages the data in practice; the user is the research institution or policy maker that obtains access to them on the basis of a permit; the data subject is the natural person to whom they relate. None of these roles encompasses ownership (Bijvoets, 2026e).

The same holds for the Data Act. Whoever reads Articles 1 and 4 of the Data Act encounters "user", "data holder", "third party" and "recipient"; the regulation employs no concept of ownership of data. The civil-law qualification of data is, moreover, not settled across the EU Member States, and a property regime over data has been criticised extensively in the literature (cf. Purtova, 2017; Bijvoets, 2026a). The Data Act aligns with that by speaking exclusively in terms of access rights.

For the healthcare context this means that patient data are not allocated as property under the EHDS: not to the patient, not to the healthcare provider and not to a national data bank. They are treated as the object of a regulated chain of access, in which each link (patient, practitioner, healthcare institution, HDAB, user) has its own rights and obligations. For legal qualification, that offers more to hold on to in practice than a property model.

What changes for DPO practice?

DPO practice changes on the following points, among others.

Record of processing activities. First map the actual operations and purposes. Secondary use may be a separate processing activity or may materially change an existing entry. Assess per process whether a separate entry or an update is required under Article 30 GDPR; in all cases record purpose, basis, categories, recipients and retention periods in an auditable way.

DPIA. Before implementation, assess whether the new or changed processing is likely to create a high risk and update an existing DPIA when the risk picture changes (Article 35 GDPR). Large-scale processing of health data will often require a DPIA. Address pseudonymisation and anonymisation, logging, secure processing environments and objection procedures explicitly.

Roles and contracts. A research or analytics partner is not automatically a processor. Determine first who decides purposes and means: controller, joint controller or processor. Article 28 and a processing agreement are appropriate

only in the last case; joint control calls for an Article 26 arrangement. In addition, document the data permit, security conditions, handling of objections and permitted purposes.

Communication with the patient. The right to object is effective only if the patient knows about it. Clear information on primary and secondary use (Articles 13-14 GDPR, supplemented by EHDS transparency mechanisms) deserves a visible place in patient communications. A deficiency may breach transparency duties, but does not automatically make every secondary-use operation unlawful: Article 14(5) GDPR contains exceptions and the EHDS builds its own information infrastructure. Document the applicable duty, exception and safeguard for each data flow.

Governance. Under the EHDS, the healthcare provider must engage with new actors: the national HDAB, secondary data users and, where applicable, a data-altruism organisation under the DGA. Allocate executive ownership, decision-making and oversight lines. The DPO advises and monitors independently under Articles 38-39 GDPR; accountability for purposes, means, risk acceptance and compliance remains with the controller and its management.

Closing remarks

The three new European frameworks (DGA, Data Act, EHDS) are anything but a return to the ownership debate about data. They work out, instead, what it means to make data available without assigning them to anyone as property. For the healthcare sector, the EHDS is the most far-reaching example: the regime of primary and secondary use, with restriction rights, objection, HDAB permits and Member State exceptions, forms a complex architecture that seeks to regulate care, research and protection in conjunction, and in which patient data become usable without becoming tradable.

For DPO practice, this framework confirms the GDPR's basic principles: control runs through data-subject rights, lawfulness through legal bases, and protection through governance rather than possession. The elaboration is layered and the Dutch implementation of the EHDS is not yet complete. The coming period calls for timely, independent DPO advice and monitoring on role allocation, DPIA updates, records of processing and objection procedures.

The old distrust of the "data is the new oil" metaphor is not dispelled by the EHDS but confirmed. Patient data are not allocated as property. They form the object of a regulated architecture of access and use in which patient, healthcare provider and society each play a part. The DPO advises and monitors within that architecture; the organisation itself must achieve and demonstrate lawfulness, transparency and accountability.

References

1 Bijvoets, J. (2026a) *Persoonsgegevens zijn geen eigendom: waarom de AVG kiest voor zeggenschap* [Personal data are not property: why the GDPR opts for control]. AVG Compleet. Available at: https://avg-compleet.nl/persoonsgegevens-zijn-geen-eigendom/.

1 Bijvoets, J. (2026b) *Dataportabiliteit onder de AVG: zeggenschap zonder eigendom* [Data portability under the GDPR: control without ownership]. AVG Compleet. Available at: https://avg-compleet.nl/dataportabiliteit-onder-de-avg/.

1 Bijvoets, J. (2026d) *Patiëntgegevens, WGBO en AVG: waarom het medisch dossier geen verkoopbaar bezit is* [Patient records, the WGBO and the GDPR: why the medical record is not a sellable possession]. AVG Compleet. Available at: https://avg-compleet.nl/patientgegevens-wgbo-en-avg/.

1 Bijvoets, J. (2026e) *De European Health Data Space: waarom ook de nieuwste EU-datawet geen eigenaar kent* [The European Health Data Space: why even the newest EU data law knows no owner]. AVG Compleet. Available at: https://avg-compleet.nl/de-european-health-data-space/.

1 Dutch Civil Code, Book 7, Articles 7:454 and 7:457 (Medical Treatment Contracts Act, WGBO).

1 Minister of Health, Welfare and Sport, *Stand van zaken implementatie European Health Data Space Verordening* [State of play of the implementation of the EHDS Regulation] (Letter to Parliament), 20 January 2026, Parliamentary Papers II 2025/26, 27 529. Available via zoek.officielebekendmakingen.nl.

1 *P&I* 2024/5 'Het Kamerlid, de ministers en de EHDS' [The MP, the ministers and the EHDS] (on rights of control and exceptions in primary and secondary use).

1 *P&I* 2025/3 'Actualiteiten' [Current developments] (on the Dutch opt-out choice and the positioning of the HDAB).

1 *P&I* 2025/6 'Actualiteiten' [Current developments] (on EHDS data availability and data suitability; letter Vektis-DHD-Nivel-IKNL).

1 Purtova, N. (2017) 'Do Property Rights in Personal Data Make Sense after the Big Data Turn? Individual Control and Transparency', *Journal of Law and Economic Regulation*, 10(2), pp. 64-78.

1 Dutch GDPR Implementation Act (UAVG), Articles 24 and 30.

1 Regulation (EU) 2016/679 (General Data Protection Regulation), in particular Articles 6, 9, 13-14, 26, 28, 30, 35 and 38-39.

1 Regulation (EU) 2022/868 (Data Governance Act), OJ 2022 L 152, in particular Article 1(3).

1 Regulation (EU) 2023/2854 (Data Act), OJ L 2023/2854, 22 December 2023, in particular Articles 1(5), 3(1) and 50.

1 Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space (EHDS Regulation), OJ L 2025/327, 5 March 2025, in particular Articles 66, 68, 71, 73 and 105 and recital 52.

1 Individual Healthcare Professions Act (Wet BIG), Article 88.

This English edition corresponds to the Dutch online article published by AVG Compleet. Legal information reflects the position stated on the publication date.