Roma Tre

Reuse of health data between contract law and data protection law

PRIMA – PRivacy Infringements Machine-Advice
12 January 2026

Prof. Giorgio Resta – Dott.ssa Sara Roccu

Roma Tre

Wellness applications

370.000

health apps currently available on the market

250

new apps are added every day

22%-41%

of European citizens who use at least one health app

Roma Tre

Wellness applications

User's Contribution

- High willingness to share data
- Health, biometric, and location data
- Implicit trust in the service

Policy Barrier

- Long documents
- Complex legal-technical language
- Non-granular and often implicit consent
- Exploitation of the user's vulnerability (e.g., accepting terms to access a necessary service during a moment of fragility)

Roma Tre

Critical analysis of 4 E-health Privacy Policies: common violations of the GDPR

Companies claim “maximum transparency”, but the structure of their privacy policies prevents real understanding and effective control by the user over the data being processed and transferred.

App	Trasparency (Artt. 12-14 GDPR)	Informed Consent (Art.6,7,9 GDPR)	Purposes and Recipients (Art.13 GDPR)	Extra-EU Data Transfers (Artt. 44-50 GDPR)
Fitbit	☒ Excessive length	☒ Implicit/based on actions	☒ Generic recipients	☒ Transfer of risk to the user
Garmin	☒ Complex language	☒ Vague language	☒ Generic recipients	
Kardia	☒ Complex language	☒ Consent not freely given	☒ Generic recipients	
mysugr	☒ Complex language	☒ “All or nothing"		

Roma Tre

The consent collection strategies are designed to maximize data acquisition, not user understanding.

Action-based consent (Fitbit)

Considering device pairing as a form of consent for the processing of health data violates the requirement for a positive and unequivocal action.

> *"We obtain this consent separately when you take actions leading to our obtaining the data, for example, when you pair your device to your account, […] or use the female health tracking feature."*

Power imbalance (mysugr)

The user (diabetic patient) is effectively forced to accept in order to access an essential service for their health.

Roma Tre

The flow of data to unknown recipients

Users cannot exercise meaningful control over their data if they do not know who is processing it.

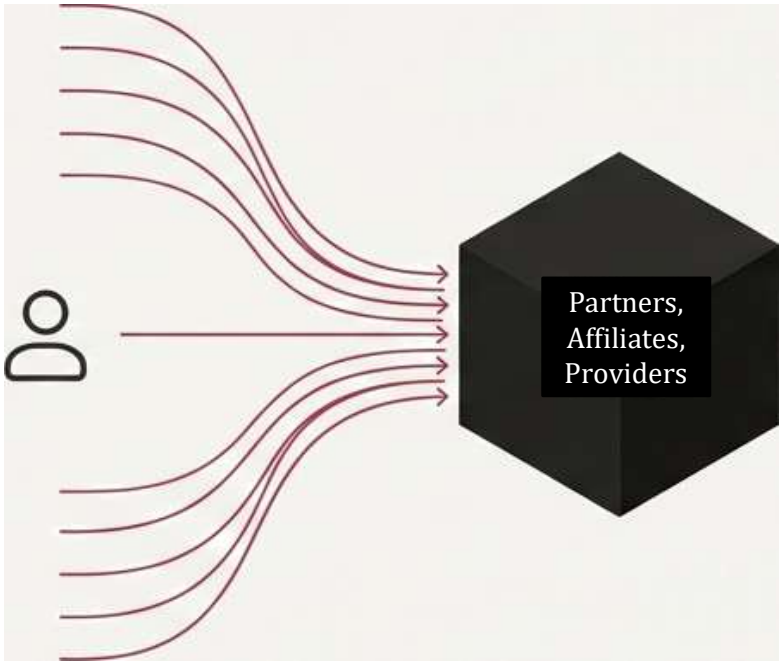
The policies of Fitbit, Kardia and Garmin mention sharing data with broad and undefined categories.

Generic Categories used:

- Corporate affiliates
- Service providers
- Other partners

This vagueness makes it impossible for the user to trace the actual path of their health data and assess the associated risks.

> *"We transfer information to our corporate affiliates, service providers, and other partners who process it for us, based on our instructions ..."*



Roma Tre

Extra-EU data transfers

The protections of the GDPR are bypassed by transferring data to less protective jurisdictions, with the user's explicit (but coerced) consent.

The mechanism (e.g., Fitbit)

- The policy informs that data is transferred to the United States.
- It specifies that U.S. laws may be “potentially less protective”.
- The responsibility for this risk is transferred to the user upon account creation.

«You agree to this risk when you create a Fitbit account and click “I agree” to data transfers, irrespective of which country you live in.»

Roma Tre

The intervention of the EHDS in wellness apps

In this context of uncertainty, the new Regulation on the European Health Data Space (EHDS) introduces for the first time a specific regulatory framework for wellness apps.

Key definition (Art. 2(2)(ab) EHDS)

"**Wellness app**": any software or any combination of hardware and software, intended by the manufacturer to be used by an individual, for the processing of electronic health data, specifically to provide information about an individual's health or to provide care services for purposes other than the provision of healthcare.

Roma Tre

Mandatory labeling for interoperability

The EHDS introduces a mandatory label for wellness apps that claim to be interoperable with electronic health records (EHR). The goal is to inform users about compliance with specific interoperability and security requirements.

DECLARATION

The app manufacturer declares interoperability with EHRs and compliance with the essential requirements (Annex II).

SELF-DECLARATION

The manufacturer independently declares that the app meets all the requirements.

REGISTRATION

The manufacturer registers the app in the EU public database.

LABEL

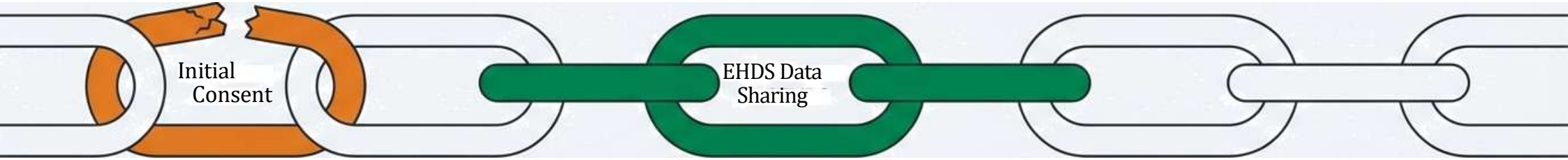
The manufacturer issues and places the label on the application.

Roma Tre

One step forward, but the challenge of the power imbalance remains

The EHDS significantly improves the user's control over data sharing with the EHR system.

However, it does not fully address the root issue: the power imbalance between app manufacturers and users during the initial data collection phase.



Focus on interoperability

The EHDS primarily focuses on the security and interoperability of data transfer, but does not thoroughly verify the validity of the original consent.

Manufacturer's self-certification

Labeling is based on a declaration by the manufacturer, not on empirical verification or certification by an independent third-party organization.

A false sense of security for the user

Users might perceive the EHDS label as a seal of GDPR compliance, lowering their level of awareness, even if the app's data collection practices remain problematic.

Roma Tre

Roadmap: integrating “Privacy by design” into labelling

Using delegated acts (Article 49(4) EHDS) and implementing acts (Article 47(3) EHDS), the Commission can integrate the fundamental principles of “Privacy by Design” directly into the requirements for obtaining the EHDS label.

1. Proactive Approach

Incorporate these safeguards before an app receives the label, rather than relying on reactive checks afterwards.

2. Privacy by Default / Granularity of Consent

Make it mandatory for users to give separate consent for each processing purpose. The EHDS already requires this for sharing with the EHR system; this principle must be extended to the initial collection of data.

3. Visibility and Transparency

Require that terms of use are understandable and that information relevant to consent is not hidden. Withdrawing consent must be as simple and accessible as granting it.

Roma Tre

Transforming principles into mandatory requirements

- **Verification of initial consent**
  Include proof of GDPR-compliant consent mechanisms (e.g. no pre-ticked boxes, granular choice) in the list of data required for registration.
- **Pop-up notifications**
  Promote or require mechanisms such as pop-up notifications that require users to actively confirm their consent for each purpose, making the choice an informed one.
- **Simplification of terms**
  Establish minimum standards of clarity and accessibility for privacy policies as a prerequisite for labelling.
- **Role of digital health authorities**
  Leverage their role (Art. 19 EHDS) to contribute to the development of common specifications that directly address issues related to users' fundamental rights.

Roma Tre

Thank you for your attention!