

THE LEGAL CHALLENGES OF PROPTech

(V) ACCESS TO AND SHARING OF DATA GENERATED BY CONNECTED PRODUCTS IN THE REAL ESTATE SECTOR: THE BINDING LEGAL REQUIREMENTS OF THE DATA ACT

November 18, 2025

*The term **PropTech** (a contraction of "Property" and "Technology") refers to the use of technology and digital tools in the real estate sector at all stages of the value chain, from construction to asset management and property portfolio management, including market transactions to sell or rent property (or even potential financing rounds).*

As in other fields (health, law, insurance, etc.), well-established players in the property management and asset management sectors, as well as numerous start-ups, have understood the value of leveraging constantly evolving technologies to automate existing processes or offer new services to all stakeholders, particularly end users.

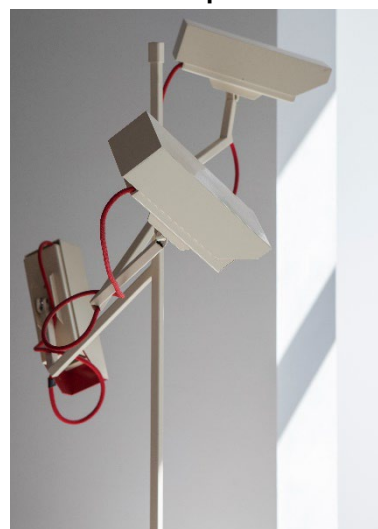
Examples include 3D printing and virtual (or augmented) reality at the construction stage, estimating the value of buildings using artificial intelligence (AI) tools, online sales or rental advertising platforms, and even "smart" management of real estate portfolios based on the Internet of Things (IoT) or collaborative tools that maximize the use of coworking spaces or parking lots.

Lime offers an analysis of the main legal issues surrounding PropTech, the fifth part of which is devoted to users' rights over data from connected products¹.

Recognizing the risks and opportunities of the emergence of a data market, resulting in particular from the proliferation of connected products among individuals and professionals, European legislators have adopted the Data Act, applicable since September 12, 2025.

Its purpose is to ensure fairness among the main players when accessing data (whether personal or not), using it, or sharing it with third parties. In the real estate sector, services related to this data open up some very interesting prospects: home automation applications for individuals (with value-added services), predictive maintenance tools for professionals to extend the life of products, etc.

All stakeholders must now ensure that they comply strictly with the Data Act. Companies must therefore verify that the contracts they enter into with their users or data recipients are strictly compliant with the new regulatory framework (as well as with the GDPR and the AI Act, where applicable). At the same time, measures must be taken to protect their digital assets,



¹ For previous notes on (I) data valuation in accordance with the GDPR, (II) artificial intelligence, (III) ecological transition, and (IV) the digitization of procedures, see <https://www.lime.law/en/latest-thinking>.

using the mechanisms in place in the field of trade secrets or intellectual property rights.

1. Opportunities of the Internet of Things (IoT) in the real estate sector and legal issues

➤ Growing use of connected products

In the real estate sector, as in other areas, connected products are becoming increasingly common. Connected to the network via Wi-Fi or an integrated SIM card, they can collect data relating to their use or their environment and process this data, while communicating various information to the product user or a professional (e.g., the manufacturer).

There are many applications for both consumers and professionals.

In the real estate sector, individuals can use them to check the pH level or temperature of their swimming pool, monitor the security of their home (using surveillance cameras), or optimize the lighting level in certain rooms. They can also be informed of their energy consumption and, in doing so, adjust it (in the event of excessive costs) or detect anomalies (a water leak, for example). In general, the information is made available to them in real time in applications downloaded to their smartphone, through which they can take various actions (lower the heating thermostat or release chlorine into the pool, for example).

For professionals, this data is useful in several ways. It allows manufacturers of goods and building managers/owners to quickly identify any malfunctions in key components (electrical installation, heating, sanitary equipment, etc.) and, as part of predictive maintenance, to remedy them as quickly as possible. These technologies can thus help to extend the life of products, with a view to sustainable development². Office space managers can also monitor parameters such as energy consumption and, in this context, optimize heating or lighting according to space occupancy. Finally, the data collected and processed anonymously enables professionals to better understand customer habits, with a view to improving their products and offering new features.

➤ Risks and legal issues surrounding the processing of data from connected products and associated services

The processing of data collected through connected products and related services, or generated by their use, may give rise to risks and, in this context, violate the fundamental rights of the individuals concerned.

When it comes to personal data, **the provisions of the GDPR** must be strictly complied with³. The use of artificial intelligence tools to process the considerable volume of available data or interact autonomously with users may also be subject to specific rules, such as the AI Act⁴. Similarly, as a result of hacking or other cybercrime offenses, data may be stolen or the functioning of certain connected products may be altered or even completely paralyzed.

➤ Focus on data access and sharing: the Data Act

For several years now, operators have understood that data is a valuable asset. The data market is therefore experiencing constant growth. However, not all companies are on an equal level, and for some of them it is very difficult, if not impossible, to obtain the data generated by connected products on fair and transparent terms. Similarly, some users, particularly consumers, may experience difficulties when accessing their data or sharing it with a new service provider.

² In this regard, see the note on [ecological transition in the PropTech sector](#).

³ In this regard, see the note on [complying with the GDPR in the PropTech sector](#).

⁴ In this regard, see the note on [the use of AI in the PropTech sector](#).

European legislators are aware of these obstacles and, as part of their data strategy, adopted a **regulation on data⁵ (or "Data Act")** in 2023, the provisions of which have been applicable, with some exceptions, since September 12, 2025. This instrument introduces harmonized rules, directly applicable in Member States, with the aim of ensuring the availability of data for the benefit of users of connected products or related services, for the benefit of data recipients or, for exceptional purposes, for the benefit of public sector bodies or certain public authorities. Data portability is also regulated, as is the adoption of harmonized technical standards, which are essential to enable data transfers.

We will focus on **users' rights** in terms of data access and sharing, and on the possible obligation to make data available to third parties.

First and foremost, potentially affected companies must ensure that they are subject to the provisions of the regulation. Certain SMEs (micro, small, or medium-sized enterprises) may be exempt from certain data sharing rules.

2. User rights to access data

In accordance with the Data Act, users—whether professionals or consumers—have the right to access data relating to connected products (e.g., an electricity meter) and related services (e.g., dedicated mobile applications). Where possible, they must be able to access this data directly or, with some exceptions, by simply sending a request by email. The principle of access *by design* is thus enshrined in Article 3 of the regulation.

Information obligations are imposed on users' co-contractors. These relate in particular to product data and how to access it. Manufacturers or lessors/lessees of products and service providers are therefore advised to ensure that their information notices and contractual terms and conditions are up to date.

This right of access is not absolute. Product safety requirements that could lead to "*serious adverse effect on the health, safety or security of natural persons*" may therefore restrict or prevent access (Art. 4 (2) of the Data Act). Trade secrets must also be protected. Not all uses of the data are permitted: it is clearly stipulated that "*the user shall not use the data obtained [...] to develop a connected product that competes with the connected product from which the data originate, nor share the data with a third party with that intent and shall not use such data to derive insights about the economic situation, assets and production methods of the manufacturer or, where applicable the data holder*" (Art. 4 (10) of the Data Act).

The Data Act applies to both personal data and non-personal data. The latter includes, for example, technical information relating to the performance of the connected product and any bugs affecting it. In practice, the distinction between these two categories of data could prove difficult, and a detailed and thorough analysis will need to be carried out. With regard to personal data, the requirements of the GDPR must be strictly observed. With regard to non-personal data, the regulatory framework is much less detailed. In addition to Regulation 2018/1807⁶, Article 4 of the Data Act must now be complied with, which requires a contract to be concluded between the user and the data holder in order for the latter to use non-personal data, on the understanding that they are prohibited from doing so "*to derive insights about the economic situation, assets and production methods of, or the use by, the user in any other*

⁵ Regulation (EU) 2023/2854 of the European Parliament and of the Council of December 13, 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L of December 22, 2023.

⁶ Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ, L 303 of November 28, 2018.

manner that could undermine the commercial position of that user on the markets in which the user is active" (Art. 4 (13) of the Data Act). The sharing of this data with third parties must also comply with the contractual provisions.

3. Data sharing and disclosure to third parties

➤ User rights

The data user - the manager of an office space, for example - has the right to share this data with third parties.

These third parties may be the provider of an integrated home automation solution whose services they wish to subscribe to, or another predictive maintenance provider they wish to use (and who therefore needs the data).

The data holder — the current service provider of the office space in the above example — must make the data available to the third party without undue delay. Where necessary, measures must be taken to protect the confidentiality of the data and trade secrets. As for the third party, it may only process the data for the purposes and under the conditions agreed with the user. Article 6 of the Data Act also contains a list of prohibited practices, including using *"the data it receives to develop a product that competes with the connected product from which the accessed data originate or share the data with another third party for that purpose"* or preventing *"the user that is a consumer, including on the basis of a contract, from making the data it receives available to other parties."*

➤ Rules to be followed when data holders make data available to third parties

When a data holder discloses data to a third party, at the request of a user or pursuant to an applicable legal provision, the Data Act establishes as a guiding principle that the terms and conditions of such disclosure must be fair, reasonable, non-discriminatory, and transparent.

Several aspects are thus regulated by the Data Act, such as the compensation that may be agreed between the data holder and the recipient, dispute resolution, technical protection measures put in place to prevent unauthorized access to data or to regulate access to data, and the prohibition of unfair terms. For the most part, these rules apply only to relationships between enterprises.

In addition to the internal policies to be put in place, it is important in any case to contractually regulate these aspects in relations with the various parties involved.

For more information, please contact:

Hervé Jacquemin
h.jacquemin@lime.law

Julie-Anne Delcorde
ja.delcorde@lime.law

Thierry Tilquin
t.tilquin@lime.law