Smart buildings

LEGAL ASPECTS OF CONNECTED CONSTRUCTIONS

DLA PIPER

Think outside the building

What will buildings of the future look like? You may think of sustainable, cost-efficient and extremely user-friendly environments that incorporate technologies to make life more convenient and productive. Whether you are a constructor, I(o)T service provider, potential occupant or individual user, the added value these technologies may bring to your business and the support they could offer in reaching your objectives should not be too hard to envision.

The word "smart" is an overused term these days with smartphones, smart home assistants, and the slow but steady emergence of connected cars and other smart devices. Smart buildings are part of the internet of things (IoT) evolution that began several decades ago. As the dust settled and the buzz faded, we now want to take a look at the real business opportunities and challenges this transformation presents to the construction industry.

The future could be closer than we think. Startups in Belgium and abroad are offering innovative market-ready products that can be implemented in building projects. As these technologies are becoming more affordable and accessible, the products might soon reach the long-anticipated wide-adoption phase.

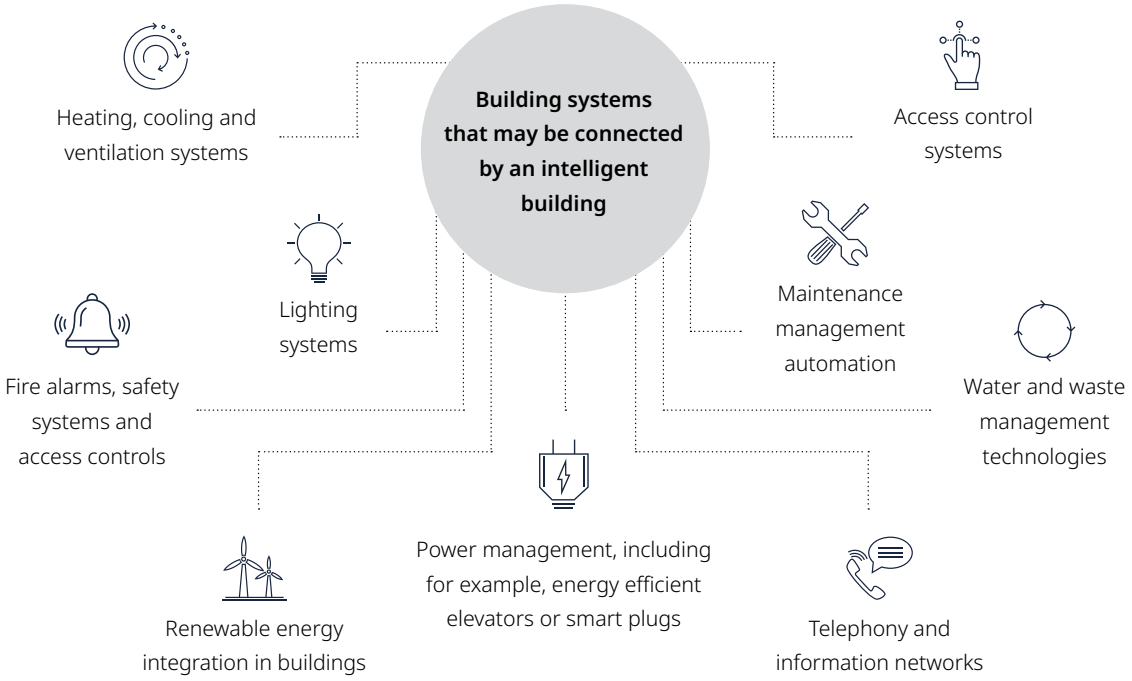
Integrating these technologies in construction plans to create truly connected and data-driven buildings also introduces new regulatory and data protection challenges. It raises numerous questions as to the implications of these developments for the responsibility of all parties involved in the construction industry.

Contents

What is a smart building?

In smart buildings, occupants are integrated into a dynamic, self-contained and self-adaptable ecosystem based on in-house smart devices such as sensors, routers, gateways, switches, printers, smart meters that can capture, store, and analyse data for facilitating user safety, comfort or user physical activity but also reducing cost with energy and maintenance.

Smart buildings integrate or connect multiple building systems, and automatically and autonomously respond to situations and events. A building can be labelled as "smart" when many such systems are merged and integrated into a construction. The smart building subsequently provides information to the owner or occupant that enables them to manage the building more efficiently, provide more comfort to its users, to optimise space and allow for flexible use, lower costs and also aims to increase working performance of users.[2]



[1]M. Barati, I. Petri, O.F. Rana, "Developing GDPR Compliant User Data Policies for Internet of Things", *Proceedings to the ACM International Conference on Utility and Cloud Computing* (UCC 2019, New Zealand).

[2]V. Angelakis et al. (eds.), *Designing, Developing, and Facilitating Smart Cities*, Springer, 2017.

Legal pitfalls

Smart building projects may come in many different shapes and sizes. Depending on vital operational decisions such as the envisage business models of the parties involved in the construction of a smart building, preferred post-construction ownership structures and service delivery set-ups during the exploitation of the facility, plenty of legal challenges arise that require dynamic, business-oriented and inventive solutions.

Highlights of some relevant aspects in:

DATA PROTECTION

CYBERSECURITY

ICT CONTRACTING AND CLOUD COMPUTING

PROPERTY LAW

Data protection

Regarding processing of personal data, all GDPR obligations apply to smart building systems. The controller will, for example, need to ensure that data protection principles are adequately implemented, every processing activity has a valid legal basis at all times, a Data Protection Impact Assessment (DPIA) is performed and kept up-to-date and transparency obligations are complied with. However, some topics may require particular attention.

DO DATA PROTECTION LAWS APPLY?

The legal challenges related to data protection – as discussed below – of course only apply when smart building data generation comes within the scope of data protection laws.

From a GDPR perspective, not all generated data would be considered personal data. Sensors might, for example, keep track of the building's temperature, carbon dioxide levels, and light intensity and sound levels. In many circumstances, this data would not be considered personal data. Especially in flexible and modular workspaces, where people come and go, such data would not always identify individual users. Whether data is personal data is a highly contextual assessment that – in a big data environment – will need to take into account other available data sets and developments in technology.

On the other hand, the evolution towards a smart building environment will also convert many traditional devices or user functions into digital counterparts. All of a sudden, all of these will start processing (personal) data, so many more activities will involve processing covered by the GDPR.

BLURRING ROLES AND RESPONSIBILITIES

The providers of IoT-based services may be considered processors for the benefit of the owner(s) of the property, who can be considered controllers for the information collected by the services. However, data protection roles and responsibilities will correlate with the purposes for which generated data is to be used.

Obtaining a clear view on purpose determination may prove to be a challenge of its own. On completion of construction works, constructors or developers can offer continuous service and maintenance support to occupants and provide them with various smart building features. Smart building user data will help to deliver these services in better, more efficient and highly personalised ways and significantly reduce associated costs. As a result, many parties will be interested in smart building user data. This generated data can be extremely valuable, not only to occupants or their service providers, but also to be exploited for optimisation of other construction projects or to fuel entirely new big data business models.

Example: Belgian Data Protection Authority's decision on video surveillance

A basic analogy may be drawn from a recent decision of the Belgian Data Protection Authority. The decision concerned a dispute between the constructor of a building and the association of co-owners with regard to video surveillance equipment installed in and around the property. In essence, the Belgian Data Protection Authority held that a distinction needs to be made between the initial construction phase and a second phase that begins on execution of the notarial deed of sale. In the first phase, the constructor takes all the decisions in relation to the installation of the video surveillance and thus needs to be considered the controller of the data generated by the building's equipment. In the subsequent phase, the association of co-owners should be entitled to decide on the purposes and the means of the processing, regardless of any contractual obligation the constructor may have to install the equipment. The constructor needs to permit the association of co-owners to determine the purposes and the means of the processing and is therefore under an obligation to transfer the plans related to the installation and hand over the access codes of the related systems.

Correctly assigning data protection roles will be of significant relevance, as it will bring responsibility and liability for compliance with data protection obligations. Even if the constructor or project developer cannot be considered to qualify as a controller or processor under data protection laws, they may nonetheless be confronted with various data protection obligations – and obliged to abide by them in the construction of smart buildings – to ensure the commercial viability of the building insofar as data protection obligations are (indirectly) contractually imposed by the (future) owner of the smart building. Such contractual arrangements might be a prerequisite for future occupants of the building to be able to use the property in compliance with data protection laws.

DATA OWNERSHIP

Personal data generated by smart buildings (eg on the use of energy consumption) can have a huge value for the constructor, building owner or third parties. An important question that arises is whether the owner can use, resell, share or transfer this data to third parties. Contractual arrangements between the parties involved regarding the ownership of the data will be crucial in this regard.

Even if adequate arrangements have been made, the interaction with data protection law may set limits to the parties' contractual freedom. The decision of the Belgian Data Protection Authority of 9 July 2020, also contains interesting indications in this regard. It held that "the [constructor/project promotor] was indeed responsible for providing the physical infrastructure for the installation of security cameras, but this cannot lead to ongoing access to the video footage after the property rights have been transferred in his same capacity as constructor and project promotor."

This argument may hinder the possibilities of parties involved in the construction of a smart building to set up a business (eg for the optimisation of other construction projects or for selling data related to energy consumption) which requires ongoing access to the IoT-generated building data after the property has been transferred.

DATA PROTECTION BY DESIGN AND BY DEFAULT

To facilitate compliance – and because adjustments to incorporate IoT systems may come at a high cost – data protection by design and by default should be part and parcel from the start of the building design and development process.

In a smart building environment, this obligation can be particularly challenging. IoT-based systems, for example, have the ability to act, react and adapt based on the information gathered by sensors and devices. Therefore, it may be difficult to foresee what information will be captured, including sensitive information. When such devices are continuously connected, this data may be automatically shared and transferred.

Another challenge for data protection by design and by default in this context may be the difficulty to understand when and where IoT data is collected and for what purposes. In addition, IoT-generated data is often deployed for multiple purposes and new purposes may emerge over time.

TRANSFER OF DATA TO THIRD COUNTRIES

Many IoT vendors are not located in the European Economic Area. Very often, they do not have large local storage facilities and make use of cloud infrastructure to store massive amounts of generated data. Using cloud infrastructure can involve multiple data transfers to third countries that require thorough assessment under the current legal landscape.

EPRIVACY (AHEAD)

In a data-driven building, an additional layer of regulatory complexity is added by ePrivacy rules.

Under the current ePrivacy Directive and its national implementations, several types of IoT applications are already subject to additional transparency obligations and even to end-user consent. In most cases, it will be difficult for the controller to meet all GDPR conditions for consent in the context of processing by IoT-based systems. The Working Party 29 Opinion on Internet of Things also refers to the quality of consent as a point of attention.

In the (near) future, the upcoming ePrivacy Regulation may – once adopted – also significantly affect the construction and development of smart environments. The current proposal seeks to regulate a wide array of metadata (or data about data). In addition, machine-to-machine communication data collection would be explicitly limited to a restrictive number of legal grounds and conditional on the application of appropriate security measures.

Cybersecurity and I(o)T infrastructure

ROBUST SECURITY IS KEY

Due to the interconnectedness of smart devices, the impact of security (including data) breaches can be particularly severe as organisations are likely to become more dependent on their expanding IT infrastructure. Incidents could have catastrophic consequences and many real-life examples have shown they may paralyse an organisation for a long time.

The entity acting as a controller of the smart building's processing activities will, under data protection law, bear the responsibility of ensuring that robust security measures are in place that are aligned with the risks caused by high volumes of generated data. Agencies and industry groups have been taking action to set industry security standards for IoT devices, an example of which are the ENISA guidelines on Good Practices for Security of IoT and Industry 4.0 – Cybersecurity Challenges and Recommendations.

INCIDENT MANAGEMENT

In case of an incident, notification obligations can be triggered. Security and notification obligations may result from the GDPR and also from other cybersecurity legislation, such as the NIS Directive, depending on the type of organisation occupying the smart building.

ICT contracting and cloud computing

Any use of technology in smart buildings will undeniably require third-party licenses and the performance of third-party services. Depending on the size and complexity of the project, the set-up and negotiation of an appropriate contractual framework for smart buildings may be challenging and typically requires the involvement of legal and technical experts in the subject matter to avoid any common pitfalls.

A smart building project involving the use of multiple technologies and software may, for instance, be problematic if no adequate contractual safeguards are put in place to ensure interoperability or compatibility with the key systems of the project, the latter being subject to constant updates and upgrades. Similarly, opting for a Software-as-a-Service (SaaS) will expose a customer to significantly different risks than a traditional on-premises solution or any other delivery model (eg loss/corruption of data or downtime), taking into consideration the type of data and applications in a cloud environment.

From a contractual perspective, it is critical to be aware of the dangers that could have major impact on a smart building project and jeopardise the continuity or integrity of the smart system. This may require contract parties to set up detailed integration/implementation projects with rigorous testing and acceptance procedures, consider the use of realistic and measurable service levels that are enforceable and reportable, set up a governance model that allows efficient follow-up actions, establish an effective liability framework and establish a clear exit plan in case the services are terminated or transitioned to a different supplier.

When such sourcing of technology services takes place with the goal of delivering integrated smart services to building tenants, the interplay and potential gaps between the contractual provisions with the tenants and the service providers should also be considered.

Property law

The so-called platform economy (economic activity facilitated by digital platforms that allow the public to connect, share resources or sell services and/or products) has already forced many businesses to transform from purchase to rental models. In the future, the evolution towards more smart devices and applications may only add more "something-as-a-service" packages to our daily lives. In these models, the producer, owner or lessor offers functionality to the user, who rents or leases the goods that are being used. In return, the service provider commits to continuously maintain the infrastructure. A task supported by the data generated by the smart building. Essentially, smart buildings use tech-platforms to facilitate the management and operation of buildings in more efficient ways. In this regard, questions regarding property law arise.

A DIFFERENT APPROACH TO PROPERTY – PROPTECH AND SMART BUILDINGS

What is proptech?

The real estate sector has been marked by the emergence of proptech (or property technology). Proptech is a hot topic. Generally speaking proptech can be defined as technology designed specifically for real estate. Proptech aims at creating solutions to make planning, managing, trading, and using real estate more efficient and easier at every stage of a building's lifecycle. The term covers both software and hardware.

Property law hurdles for implementing proptech

Property law establishes many obstacles to the extension of proptech and "as-a-service" business models to the construction and building industry. For example, the right of accession (*recht van natrekking/droit d'accession*) could lead to a loss of ownership for the producer/owner/lessor of proptech appliances and impede the use of this model.

As a solution, one could propose a ground lease (*recht van erfpacht/emphytéose*) or a right of superficies (*opstalrecht/droit de superficie*). However, the cost to establish these rights may make them unsuitable for practice and these rights were neither conceived nor designed for the type of technologies and solutions we are currently looking at.[3]

Volumes – the deus ex machina?

The Belgian legislator has recently made an attempt to overcome some of these constraints. The recent reform of the Belgian Civil Code includes a fairly comprehensive revision of property law whereby the goal of the new legislation involves adopting a functional approach to property law and modernising antiquated legal concepts for use in a contemporary context. As confirmed in the preparatory works of the new legislation, the legislator specifically took into account new technological developments.

Specifically, the new legislation includes the introduction of three-dimensional real estate property, through a novel legal concept referred to as "volumes." This new legal figure, allowing the stacking of volumes above and below each other, without time limitation, creates the potential to make separate volumes for proptech, without the obstacle of accession. In a smart building, one could imagine a separate volume for a specific proptech appliance (eg smart speakers or voice-activated assistance systems, or a building operating system or a tool aimed at improving energy efficiency), which could then be managed remotely by the property manager. As such, the new "volumes" figure creates the potential for technologically interlinking buildings, allowing property professionals to "communicate" with buildings.

Another question that arises is the distinction between moveable and immoveable property and how to categorise new proptech solutions (software and hardware). In the new book on property law, the legislator adopted open categories, aimed at better withstanding the test of time. Depending on technological developments and scientific progress, "objects" (including objects that are currently unknown) can then be included in one or the other category.

Proptech – the way forward in day-to-day legal practice

Proptech is already disrupting the real estate sector, but we are clearly only at the beginning of the proptech revolution. The question is how legal practitioners will implement these solutions in practice and whether they will embrace "volumes" as an all-encompassing solution. Exciting times clearly lie ahead. It remains to be seen how the legal sector and the notarial profession will tackle these developments in their day-to-day practice.

[3]Read also: Ton Hartlief, "Het Huis van de toekomt," *Nederlands Juristenblad*, afl. 25, 2019, 1429

Conclusion

The breadth of the impact of the digitalisation of real estate on day-to-day operations (and investor-developer and landlord-tenant relations) cannot yet be fully appreciated, but it is already clear these developments will benefit the community at large in the long run: everyone will benefit from buildings that use technology and processes to protect the health and wellbeing of occupants, improve employees' productivity, allow buildings to become more operationally efficient and reduce environmental impact.

As discussed above, smart buildings clearly present both opportunities and challenges for the legal industry; from a data protection, cybersecurity, ICT contracting and a property law perspective. Navigating these legal aspects will not always be easy, especially in the early phases. Exciting times clearly lie ahead. Should you have any legal questions on smart buildings and proptech, we are readily available and happy to assist.

Key contacts

DATA PROTECTION & CYBERSECURITY

Heidi Waem
Counsel
+32 2 500 16 14
heidi.waem@dlapiper.com

Simon Verschaeve
Lawyer
+32 2 500 15 85
simon.verschaeve@dlapiper.com

ICT CONTRACTING & CLOUD COMPUTING

Kristof De Vulder
Partner
+32 2 500 15 20
kristof.devulder@dlapiper.com

Florian De Rouck
Lead Lawyer
+32 2 500 16 51
florian.derouck@dlapiper.com

REAL ESTATE

Joseph Spinks
Partner
+32 2 500 15 56
joseph.spinks@dlapiper.com

Luana Huybrechts
Lawyer
+32 2 500 15 94
luana.huybrechts@dlapiper.com