Project acronym	B4B
Project full name	Brains for Building's Energy Systems
Grant no.	M00I32004
Project duration	4 year (Starting date May 1, 2021)

Deliverable 4.1

Literature and market study of existing regulations and approaches regarding data privacy, ethics, and security, including GDPR constraints

Lead authors: Rizal Sebastian, Elena Chochanova (TNO)

Co-authors: Ekaterina Petrova, Lasitha Chamari, Pieter Pauwels, (TU/e)

Contributors: Sanne Jansweijer (NEN), Nico Mutsaers (Philips), Berno Veldhuis (RVB), Simon Hopkins (Simaxx), Niels de Jong (Cloud Energy Optimizer), Joep van der Velden (Kropman), Jan-Willem Dubbeldam (Kropman)

Work package	4
Result no.	7
Lead beneficiary	TNO
Due Date	31 January 2022
Deliverable Status	Final
File name	B4B WP4 D4.1_Study on data privacy security and ethics
Reviewers	Laure Itard (TU Delft), Mirjam Harmelink (TU Delft), Mike van der Heijden (Strukton)

This project received funding from Dutch Ministry of Economic Affairs and Climate Policy and Ministry of the Interior and Kingdom Relations under the MOOI program

SAMENVATTING

"Brains for Buildings" (B4B) is een meerjarig innovatieproject dat is gericht op de ontwikkeling van methoden met betrekking tot big data van slimme energie meters en Internet of Things (IoT) en beheersystemen in gebouwen. Het project heeft als doelen: het energieverbruik te verminderen, het comfort te verhogen, flexibel in te spelen op gebruikersgedrag en energievraag en aanbod, en de onderhoudskosten van gebouwinstallaties te verlagen. In het project worden snelle en efficiënte Machine Learning / Artificial Intelligence algoritmen – als 'hersenen' van slimme gebouwen– ontwikkeld, getest, gevalideerd en gedemonstreerd in een aantal utiliteitsgebouwen.

Dit rapport is een deliverable van Werkpakket 4 (WP4) onder het B4B project. Het werkpakket behandelt data-integratie vraagstukken in slimme gebouwen, in het bijzonder de data connectiviteit tussen de gebruikte softwareapplicaties in slimme meters, gebouwbeheersystemen, en IoT apparaten. Deze aspecten hangen samen met data beveiliging, open data standaardisatie, informatie, privacy en ethiek.

Een resultaat van WP4 dat in dit rapport is beschreven (Resultaat 7 in het B4B Werkplan) draagt bij aan de ontwikkeling van een gestandaardiseerde aanpak voor het waarborgen van privacy en ethiek bij het verzamelen, opslaan, delen, beheren of gebruiken van data in slimme gebouwen. Dit resultaat ondersteunt de andere beoogde resultaten van WP4, te weten: systemische data-integratie oplossingen (Resultaat 8) en een methodologie om bestaande gebouwen om te vormen tot slimme gebouwen, afgestemd op de Smart Readiness Indicators (SRI) (Resultaat 9).

Dit rapport heeft als hoofddoel een overzicht te geven van bestaande regelgeving, benaderingen en beperkingen met betrekking tot gegevensbeveiliging, privacy en ethiek in de context van slimme gebouwen. Op hoofdlijnen bevat dit rapport:

- Bevindingen uit literatuurstudie en deskresearch uitgevoerd door TNO, NEN en TU Eindhoven;
- Inzicht in de behoeften en beperkingen van vastgoedeigenaren en facility managers voor het verzamelen en beheren van data voor hun gebouwen of faciliteiten; en
- Een beschrijving van de huidige maatregelen voor gegevensbeheer zoals geïmplementeerd door de systeem-, platform- en softwareleveranciers.

Ethiek en datamanagement protocollen zijn bestudeerd in relatie tot de gebruikelijke procedures voor data eigenaarschap en de Europese privacywetgeving General Data Protection Regulation (GDPR) oftewel Algemene verordening gegevensbescherming (AVG). Dit rapport beschrijft ook de aspecten van toegankelijkheid (authenticatie en autorisatie) en de beveiligingsprotocollen.

In conclusie zijn de gebieden waar B4B persoonsgegevens zou betrekken in kaart gebracht. Dit zijn: 1) bij registratie van de gebouwbezetting ten behoeve van optimalisatie van energieverbruik en onderhoud; en 2) bij het inventariseren van het gebruikersgedrag ten behoeve van optimale comfort en binnenmilieukwaliteit. Op beide gebieden verwerkt B4B niet noodzakelijkerwijs persoonsgegevens. Desondanks zijn de maatregelen met betrekking tot privacy, ethiek en veiligheid belangrijk, met name: a) het waarborgen van de naleving van de GDPR door middel van Privacy-Aware Smart Buildings; en b) het waarborgen van gegevensbeveiliging bij gebouwbeheersystemen, on-premise en off-premise (cloud) dataplatforms, en IoT-apparaten om de risico's van diefstal en misbruik van (persoons)gegevens, systeeminbreuken en storingen te minimaliseren.

Dit rapport levert input voor het vervolgonderzoek naar een gestandaardiseerde methode voor het verifiëren van de compliance van de data-integratie oplossingen zoals voorgesteld in het B4B project. Deze methode zal dan bijdragen aan het versterken van het vertrouwen van de eindgebruikers en het verbreden van de marktacceptatie voor de projectresultaten.

SUMMARY

"Brains for Buildings" (B4B) is an innovation project focused on developing methods for smart building, especially to harness big data from smart meters and Internet of Things (IoT) devices and Building Management Systems (BMS) to reduce energy consumption, increase comfort, respond flexibly to user behaviours and local energy supply and demand, and reduce maintenance costs of building utilities. The 'brains' in B4B are faster and efficient Machine Learning / Artificial Intelligence algorithms that are developed, tested, validated, and demonstrated in a number of public buildings.

This report is a deliverable from Work Package 4 (WP4) in the B4B project. The work package deals with data integration in smart buildings and addresses data connectivity between the software applications used in smart meters, building management systems, and IoT devices along with the aspects of data security, open data standardization, information privacy and ethics.

The result from WP4 as presented in this report contributes to the development of a standardized approach for guaranteeing privacy and ethics when collecting, storing, integrating, sharing, managing, or utilizing data in smart buildings (Result 7 in the B4B). This result also supports the other results from WP4, i.e., systemic data integration solutions (Result 8) and a methodology for transforming existing buildings aligned with the Smart Readiness Indicators (SRI) (Result 9).

This report provides an overview of existing regulations, approaches and constraints related to data security, privacy and ethics in the context of smart buildings. It presents the findings from:

- literature study/desk research performed by TNO, NEN and TU Eindhoven;
- interviews with real estate owners and facility managers into the needs and constraints to collect and manage person-related data for their buildings or facilities; and
- current measures for data management as implemented by the system, platform, and software providers for smart buildings.

This report examines the data ethics and management protocols in relation to the common procedures for data ownership and the EU-wide implemented General Data Protection Regulation (GDPR). Regarding the data management measures as implemented by the system, platform and software providers, this report examines the accessibility, including authentication and authorisation), and the security protocols to prevent data leaks and privacy breaches.

In conclusion, the areas where B4B might be concerned with person-related data are: 1) at registering the occupancy of the buildings in relation to optimization of energy consumption and maintenance; and 2) at understanding the end-users' behaviour in relation to customizing the comfort and indoor environmental quality in relation with energy performance. In both areas, B4B does not necessarily process the personal data; however, relevant measures related to privacy, ethics and security are still important, especially with regard to: a) assuring the compliance to the General Data Protection Regulation (GDPR) through Privacy-Aware Smart Buildings measures; and b) assuring the data security at the Building Management Systems (BMS), the on-premise and off-premise (cloud) data platforms, and the IoT devices, including the end-users' mobile devices and wearables in order to mitigate the risks of theft and misuse of (personal) data, system breaches and failures.

This report gives input for the follow-up research to develop a standardised method for verifying the compliance of the data integration solutions as proposed in the B4B project. This method will contribute to emboldening the confidence of the end-users and widening the market acceptance for the project results.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Goal and scope

1.1.1 Rationale: The importance of ethics, privacy, and security for data integration

Technological advances in recent years have brought many benefits to society but we have also seen how negative impacts of these advances can play out. With the unregulated and unlimited collection and exchange of personal data, large companies can gain unprecedented control over people's lives. Many argue that information and knowledge sharing/exchange is beneficial for society regardless of the use and context, nevertheless. However, information can easily be misused or unknowingly used in indirect but harmful ways. Therefore, clear concepts of ethics, privacy and security are needed as a framework to be applied in the context of information sharing in relation with the following questions:

- What kinds of principles should guide the actions of individual users and of companies when using data and how do their actions affect society?
- What are the threats to personal privacy and how do we protect against them?
- How can access to sensitive information be controlled and how can we secure hardware and software?

A glance at the basic reasoning: what are privacy and ethics, and why are they important? The United Nations defines privacy as:

> "the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others, free from state intervention and excessive unsolicited intervention by other uninvited individuals. The right to privacy is also the ability of individuals to determine who holds information about them and how that information is used." [1]

This concept has been recognized as a basic human right under the Universal Declaration of Human Rights (Paris, Dec 10, 1948)[2] under Article 12, which states that:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Privacy and ethics are needed because personal information can be misused if it falls into the wrong hands. The concept of privacy cannot be seen as separate from the concept of security, which can be further divided into physical security and cyber security.

1.2 Goal and scope of this study

Smart buildings need to collect and use large amount of data from different sources. This data is owned by different stakeholders and should only be used in a controlled, ethical, and correct way. For that purpose, a standardized methodology with a focus on smart buildings is required.

This task attempts to map the constraints for data integration used in the automation processes of the specialistic domain models. These models are handled in work packages 1, 2 and 3 of the B4B project. Data integration, within the context of this project, is:

- A way to provide the expert models of the relevant disciplines as addressed in B4B with required data from the buildings' management systems (BMS), the associated IoT devices, and the related information systems, such as Facility Management (FMIS) in an automated fashion; and
- A framework of standards and processes that ensures that the data remains interoperable between the different systems and stakeholders involved.

[1] United Nations (ohchr.org) (UN General Assembly 2013:15).

[2] Universal Declaration of Human Rights | United Nations (UN General Assembly resolution 217 A)

The goal of this study is twofold:

1. To create an overview and awareness of the existing regulations, norms, and stakeholder approaches for ensuring privacy, ethics and security when collecting, storing, and handling person or building-related data. The outcome will be used as input to develop a standardized methodology as part of the data integration architecture for ensuring a safe and ethically correct collection, access, management, and use of data.
2. To sketch any technical or market constraints for data integration from the perspective of the stakeholders involved.

The stakeholders who are directly involved in this task are the real estate owners (also representing the needs of their tenants and building occupants) and the IT platform providers.

The real estate owners are the owners of the buildings, and as such, they oversee facility and asset management and the building performance. Usually, they are the main investors in the buildings' health and maintenance while at the same time being the main beneficiaries of the increasing value of their assets when the buildings are performing well.

The IT platform providers are the stakeholders involved in providing some or all required services for the collection, storage, sharing and use of the building data.

Finally, the occupants are the natural persons who interact directly with the buildings and whose needs around comfort and well-being remain central in the context in designing and operating smart buildings.

The assurance of data privacy, ethics and security will strengthen the trust of the real estate owners together with their tenants and occupants to adopt B4B solutions in their buildings and daily practices.

1.3 Methodology

1.3.1 Research approach

The approach to this study comprises two parts. First, a selection of academic and applied studies on data privacy, ethics and security in smart buildings is made, and a literature review is performed related to the objective of B4B. Second, interviews are performed with the stakeholders of smart buildings (i.e. the real-estate owners and IT solution/platform providers) about their policies and business operation related to data privacy, ethics and security.

The figure below sums up the steps taken in this study. Both literature review and stakeholder interviews have been conducted in parallel.

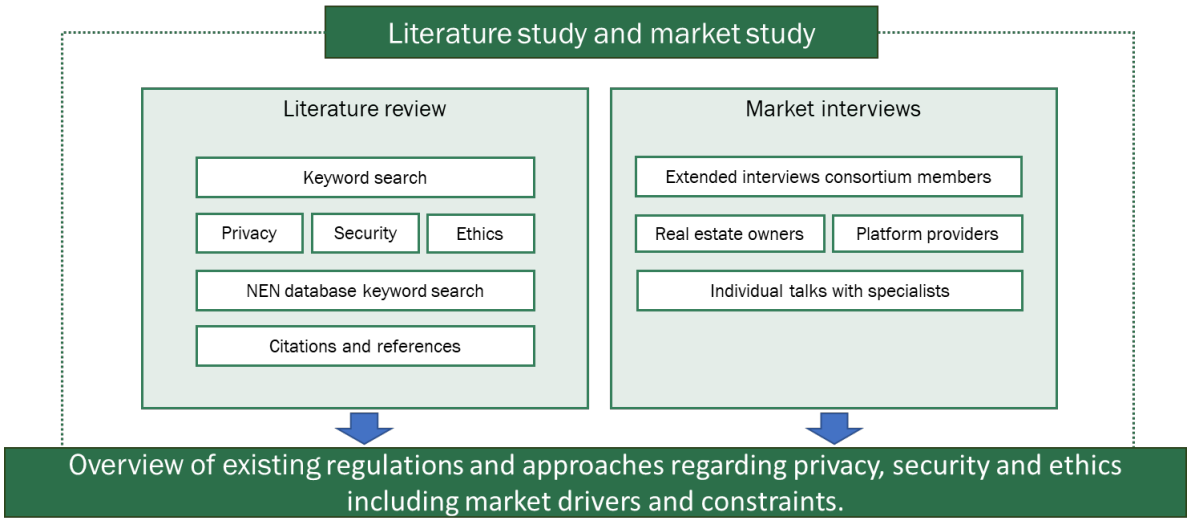

Figure 1 Research approach for this deliverable

a. Literature review

Since the introduction of the General Data Protection Regulation (GDPR) in 2016, a lot of (online) information materials have been available to help organizations to check for compliance. This information was used as a general reference to make an inventory of the constraints and challenges that companies might face when trying to adopt the regulation in their operations. There are high fines at failure to comply to the regulation constitute a significant risk for companies and organizations. There are also high incentives to adopt the

regulation; and this is part of the reasons why specialized new businesses have been formed around the need of GDPR compliance, and why many trainings are available. This reasoning holds not only for Europe where the GDPR is mandatory, but also for foreign companies which conduct businesses in Europe.[3]

Within Europe there have a been several scientific studies conducted to create a better framework for data management in the context of the built environment, Smart Cities and smart grids. In particular, the ever-increasing interconnectivity of devices (IoT) and emerging data dependent technologies such as AI and Machine Learning (ML) raise concerns about privacy, security and ethics.

b. Stakeholder Interviews

The second part of the information collection involved interviewing the consortium partners involved in WP4 of the B4B project to attain a better understanding of the norms and regulations that play a role from their businesses' perspective. A semi-structure questionnaire was used during the interviews. The interviews were conducted individually but the questions were tailored to two different groups, namely: 1) Real estate owners and 2) Platform providers.

1.3.2 Structure of the deliverable

Even though the two parts of the research (literature study and stakeholder interviews) were conducted in parallel, this deliverable presents the results in a sequential manner.

In chapter 1 we describe the goal and scope of the study in the context of the Brains4Buildings consortium and the methodology applied for collecting the information.

In chapter 2 we present the finding from the literature quick scan starting with an overview of the GDPR, how it has come into existence and why it is important in the current landscape of interconnected building systems and applications. Furthermore, we explain how this regulation relates to activities executed within the B4B consortium and in other work packages. This chapter also provides an overview of the state-of-the-art concepts and solutions based on literature reviews.

The analysis of the stakeholder interview outcomes is presented in chapters 3 and 4. The perspectives from two stakeholder groups are addressed, namely real estate owners (chapter 3) and the IT platform providers (chapter 4).

Finally, the conclusions from the literature study and stakeholder interviews, and recommendations for the follow-up tasks and deliverables are presented in chapter 5.

[3] GDPR: These companies are getting killed by Europe's new data protection law (cnn.com)

2 OVERVIEW OF REGULATIONS CONCERNING PRIVACY, ETHICS, SECURITY

2.1 General Data Protection Regulation (GDPR)

2.1.1 What is the GDPR?

The General Data Protection Regulation is a regulation within European Law that holds within the European Union (EU) and the European Economic Area (EEA). It was adopted and published in 2016, but only came into force on May 25th, 2018.

It gives individuals the power to control their personal data, which as we have already seen is internationally recognized as a basic human right.

In regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 it is stated:

> The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her. This right is also guaranteed under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms [4]

Along with the formation of the United Nations and the following declaration of human rights the GDPR has its origins in the aftermath of the Second World War. It is a known fact that the excellent registration systems in countries like the Netherlands, have made it possible to target with surgical precision ethnic groups around the country.

To avoid the mistakes of the past, a series of regulations were developed in the years following the formation of the United Nations and the issuing of the universal human rights declaration.

Privacy policies like the GDPR are guided by an underlying set of privacy principles that were first articulated during the 1960s and 1970s. The Fair Information Practice Principles (FIPPs) originated when computers began to increase their capability for information processing, and the public became concerned with the risks to privacy that these new technologies presented. (Lee at al., 2021). The GDPR supersedes the EU member states' national data protection laws based on the 1995 Data Protection Directive (DPD).[5]

An overview of data protection history is shown below. [Fig.3]

[4] Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725

[5] Source: https://www.itgovernance.eu/en-ie/eu-general-data-protection-regulation-gdpr-ie

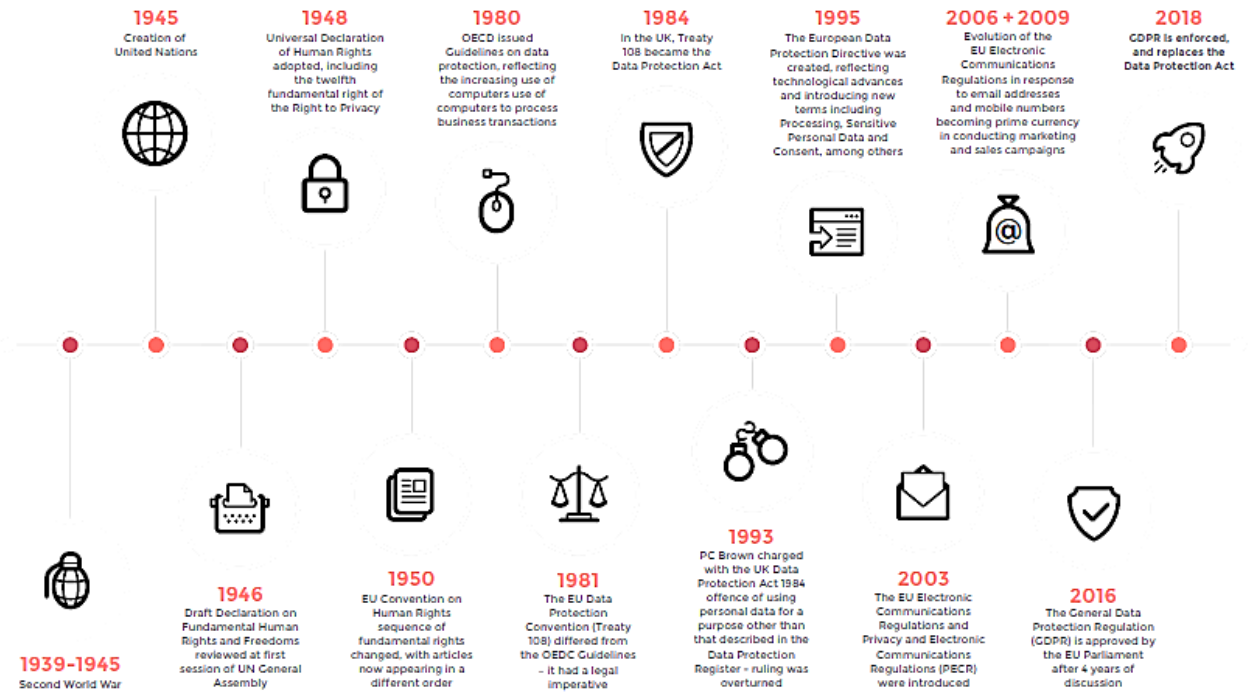

Figure 2 A historical overview of the development of data protection legislation (source: Sytorus)[6]

The GDPR states that the protection of natural persons in relation to the processing of personal data is a fundamental right. That includes every part of a citizen's personal information, such as name, contact data and location and anything that can describe their physical, physiological, mental, economic, cultural, or social identity, such as age, sex and religion. [Fig.4]

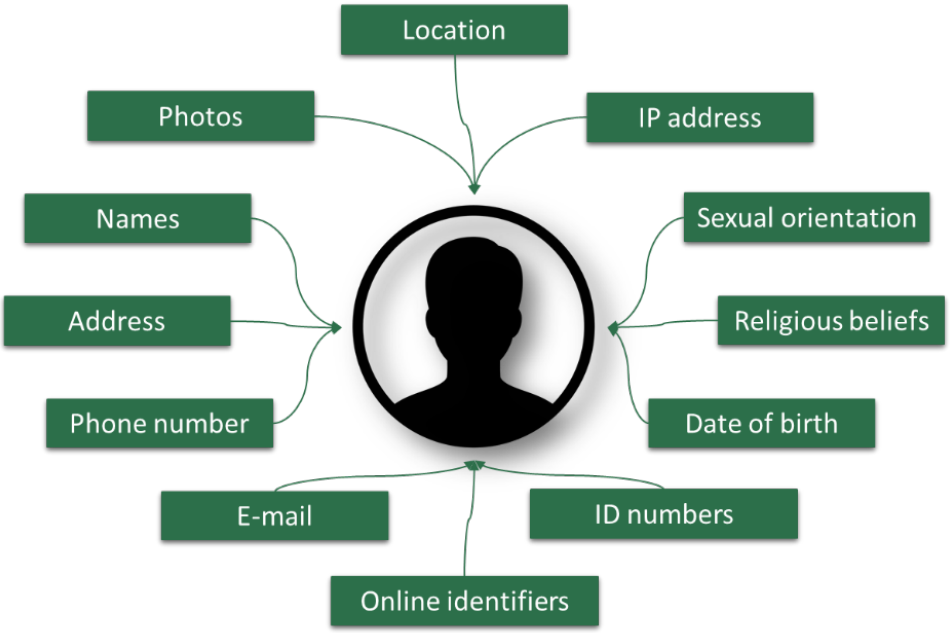

Figure 3 Types of personal information that the GDPR protects

Organizations who fail to comply with the GDPR can face serious penalties for infringements of any of the data protection principles, described further below. They could carry the maximum penalty up to 20 million EUR, or in the case of an enterprise, up to 4 % of the total worldwide annual turnover of the preceding financial year,

[6] Source: https://blog.privacyengine.io/article/176/destination-gdpr-how-did-we-arrive-here-0

whichever is higher.[7] In addition, if a data breach or other violation of data subjects' rights occurs then that could seriously damage the company's image, affecting its customers' perception and trust. On the other hand, pursuing full compliance with the GDPR could also be seen as an opportunity to practice good data hygiene and traceability, which will in turn improve relationships and trust between companies and their customers.

To illustrate the relationships between stakeholders the GDPR defines the 3 main roles involved in the collection and processing of personal data.[8]

- Data controller (organization) - "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".
- Data subject (individual) - means an identifiable natural, living person "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier".
- Data processor (service providers) - "a person, public authority, agency or other body which processes personal data on behalf of the controller".

When the stakeholders of the B4B project are considered, these 3 roles are fulfilled by the real estate owners, the building occupants, and the IT platform providers respectively. In the research and demonstration context in the B4B project, researchers are also considered as 'data controllers' and/or 'processors'. However the distinction between data controller and data processor is not always very well defined; depending on the type of contract the real estate owner can delegate some of the authorities of the data controller function to the platform providers or another stakeholder, such as a building manager or a sub-contractor.

The GDPR outlines six data protection principles. These principles summarize the GDPR requirements and give a good overview to businesses of how to comply. The principles are:

Lawfulness, fairness, and transparency – Data should be processed according to the law, in a fair and transparent manner in relation to the data subject.

Purpose limitation – Personal data should only be collected for specified, explicit and legitimate purposes. The purposes must be clearly stated, and the data should only be processed in ways that are compatible with these purposes.

Data minimization – The personal data collected should be adequate, relevant and limited to what is necessary in relation to the processing purpose.

Accuracy – All reasonable steps should be taken to update or remove data that is inaccurate or incomplete. Individuals have the right to request that data related to them be erased or that erroneous data be rectified.

Storage limitation – Personal data should only be collected for as long as it is necessary for completing the stated purposes and not longer. Data should be deleted when no longer needed.

Integrity and confidentiality - The collected personal data should be kept safe and protected against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

The ability of the data controller to demonstrate compliance of these Data Protection principles is called Accountability.[9] This principle applies to the 6 principles. The 6th principle, "integrity and confidentiality", demonstrates that there is a strong link between privacy regulations and security measures when it comes to implementation within companies.

[7] GDPR, Article 83. Source: https://gdpr-info.eu/art-83-gdpr

[8] Source: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

[9] Source: https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles

- Enabling data protection authorities (DPAs) to make binding decisions and issue administrative sanctions including fines
- The right to object to processing based on controller's or public interests
- An obligation to notify DPAs and data subjects about data breach
- Stronger consent requirements
- Including biometric and/or genetic data in the definition of sensitive data
- Introducing data protection officers (DPOs) as a mandatory role in organizations that process personal data

In addition, if an organization wants to collect and process personal data, it needs to comply with the lawful bases described by the regulation. According to Chapter 2, article 6 of the GDPR:

> Processing shall be lawful only if and to the extent that at least one of the following applies:
> 1. the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes.
> 2. processing is necessary for the performance of a **contract** to which the data subject is party or to take steps at the request of the data subject prior to entering a contract.
> 3. processing is necessary for compliance with a **legal obligation** to which the controller is subject.
> 4. processing is necessary to protect the **vital interests** of the data subject or of another natural person.
> 5. processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;
> 6. processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, where the data subject is a child.

In its core the GDPR is about the principles of **consent** and **transparency** between the data subjects and the organizations that collect and use the former's personal information. Part of the data protection regulation mandates that such data cannot be collected or traded between organizations and governments without the prior consent of the person whom this data concerns. To implement these principles, the regulation outlines the rights of natural persons in chapter 3 (Art.12 – Art.23)[10]. These rights can be roughly summed up into 3 main principles:

1. **Data Awareness:** Data subjects have the right to be informed about what data is being collected, who is collecting the data, what it will be used for, for how long, whether the data will be shared, with whom and for what purposes. In addition, the data subjects need to be informed about those rights, and the methods for raising a complaint or exercising those rights.
2. **Data Control:** Data subjects have the right to access their information via a subject access request and companies must provide this within a month. If any data is inaccurate, companies must correct it. In addition, the data subjects have the right to have their data deleted (also known as the right to be forgotten) or restricted, so that it is stored but not used. They also have the right to object to data uses, for example for direct marketing or for profiling.
3. **Data portability:** Data subjects have the right to move or copy their personal data from one system or source to another. This is known as data portability.

The GDPR constitutes an unprecedented advance in the protection of privacy of European citizens and has been used as a reference for the development of similar regulations outside Europe as well. For example, the CCPA (California Consumer Privacy Act) in the USA and the PDPA (Personal Data Protection Act) in Singapore.

Even though it's based in Europe, it affects the rest of the world. The GDPR might have sparked a new global movement since its initial publication in 2016. There to this date (2021) about 9 other state-wide (3 in the USA) and national privacy regulations around the world.[11] [Fig.5].

[10] DGPR, Chapter 3. Source: https://gdpr-info.eu/chapter-3/

[11] Source: https://piwik.pro/privacy-laws-around-globe/

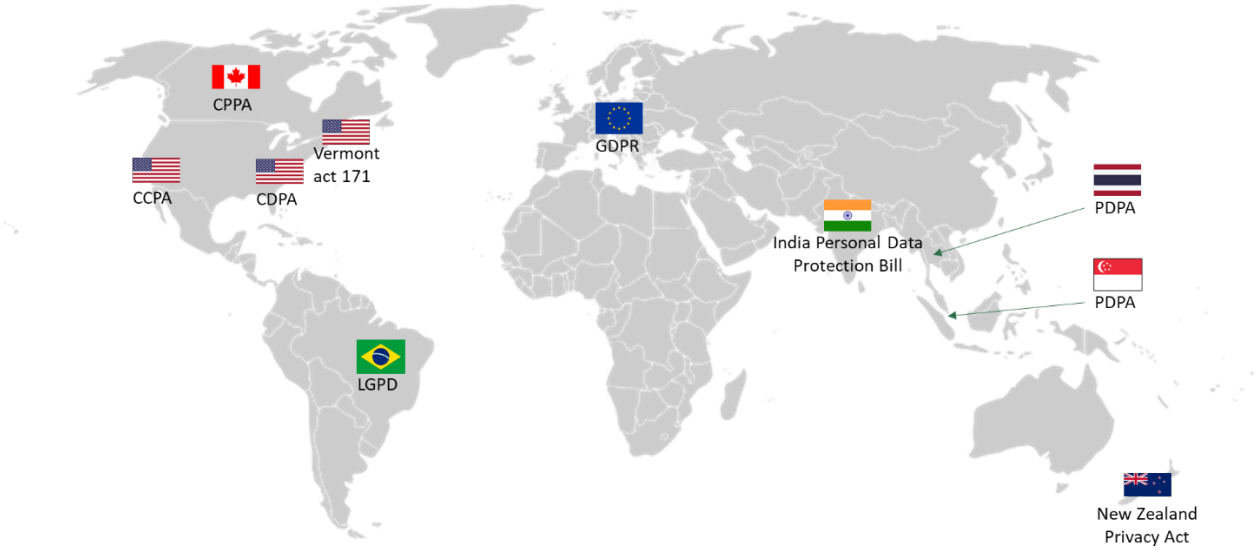

Figure 4 Overview of the 9 recognized privacy regulations worldwide as of 2021.

Despite the wide acceptance of the GDPR and its inspiring effect around the world through raising awareness about citizens' fundamental rights and the increasing efforts to reduce unlawful processing of personal data, there is still a lot of work to be done to ensure privacy in today's ever more data-driven world. For example, today there are companies that manage to subvert the GDPR by manipulating user's behaviours through "dark" design patterns whilst technically still being compliant to the privacy regulations in their countries.[12]

2.1.2 Why is the GDPR important for smart buildings?

In short, the GDPR is about the right of a person to control their own data. It is a consent driven regulation meaning that for all purposes collecting data should be consensual, this concept is a good enabler for ethical data collection.

Within the B4B project there is a possibility to collect personal data for the purpose of gaining more insights on either of the following:

1. Occupancy - In the case of occupancy information collection, usually anonymous information is collected, for example the amount of people occupying a room at any given time. But when that information is crossed referenced with the owner of the room or the use of a personal access pass then the occupancy data can become traceable to individuals and as such be subject to GDPR regulations.
2. Occupants' behaviours and comfort requirements – in case of occupant detection the GDPR is applicable only in personal information / preference storage. For example, personal preferences could provide information that could be used to optimize energy use inside the building

2.1.3 Data Protection Impact Assessments (DPIA) under the GDPR

In certain circumstances, the GDPR mandates conducting a DPIA. When implementing new technologies or processing operations, organizations must assess whether the processing presents a "high risk" to the rights and freedoms of data subjects, and whether this risk can be reduced or avoided, such as by pseudonymisation. A DPIA is "in particular" required where there is automatic processing (including profiling) and processing of special categories of data on a large scale.

A DPIA is required under the GDPR any time a new project begins that is likely to involve "a high risk" to other people's personal information as stated in Article 35 of the GDPR.

The DPIA is a new requirement under the GDPR as part of the "protection by design" principle. It is, for example, compulsory to perform a DPIA for smart city data applications. The Dutch Authority for personal data: "Authoriteit Persoonsgegevens" is actively encouraging municipalities in the Netherlands to perform these assessments in the initiation phase of any data-driven smart city applications[13]. Logically, smart buildings applications should also follow this principle like smart cities.

[12] Source: https://piwik.pro/blog/how-dark-patterns-conflict-with-gdpr-ccpa/

[13] Source: https://www.autoriteitpersoonsgegevens.nl/

This organization acts as an independent supervisory authority that monitors and regulates the protection of personal information of Dutch citizens in relation with the various existing laws, decrees and regulations that regulate the processing of personal data in the Netherlands.

For Smart Grid and Smart Metering systems, the European Commission has published a standard template for DPIA[14]. The GDPR foresees the DPIA as a key instrument to enhance Data Controllers' accountability as it helps controller not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the GDPR. In other words, a DPIA is a process for building and demonstrating compliance. The Template will guide Data Controllers in conducting a thorough DPIA which describes the envisaged Data Processing, an assessment of the Risks to the rights and freedoms of data subjects, the measures, safeguards, controls, and mechanisms envisaged to address the Risks, ensuring the protection of Personal Data.

2.2 State-of-the-art of relevant concepts and measures

Several studies have been dedicated to data privacy concerns in smart buildings. These studies and their findings are recorded in literature (see literature list in the references).

At the level of **data on energy grids**, Wesselingh et al. (2015) discussed the key concepts of the Privacy-by-Design model as proactive measures and integration of technical principles in the design of the system and default settings to enhance privacy. **Privacy-by-Design** model can be effectively integrated into the design of energy networks where transparency and user-centred implementation can be achieved by providing the option to manage the system in-house only (more privacy-friendly) or with the optional use of a smartphone over the Internet connection (more user friendly, less privacy friendly without additional measures).

Regarding **data from smart meters** in buildings, several studies investigated the data privacy concerns related to smart meters. A smart meter is an electronic device that records energy consumption and exchanges consumption data with energy suppliers, which is used for monitoring and billing (EDPS, 2019; Ząbkowski et al., 2013; Cejka et al., 2019; Lee at al., 2021). The monitoring of the energy consumed in short intervals can help to increase the efficiency and safety of electricity distribution, but also allows those who have access to the data to draw conclusions about the behaviour of energy consumers. For example, Beckel et al. (2014) found that fine-grained electricity consumption data can lead to identifying specific characteristics that may reveal information about a home's socio-economic status, dwelling, and appliances, with an accuracy of more than 70% for all households. Privacy concerns can also be linked to security risks because criminals may be able to access the data and use the information to enable inferences about what people are doing in their home or if they are away from home (McDaniel and McLaughlin, 2009).

In 2012, both the European Data Protection Supervisor (EDPS) (Opinion on smart metering systems) and the former Article 29 Working Party of Data Protection Supervisory Authorities (Opinion 12/2011) identified certain risks to the protection of personal data that were previously unknown to the energy sector. Since then, researchers, policymakers and regulators have systematically assessed and addressed privacy risks, both at EU and at national level. The EU's 2019 amended electricity Directive specifically requires smart meters to comply with the EU's data protection rules. Article 25 of the GDPR on 'data protection by design and by default' requires that controllers implement appropriate technical and organisational measures – both at the time when the means for processing is determined and at the time of the processing itself. Consumers could also be given the option to disable and enable certain smart features of their smart meter in some circumstances. However, the possibility for users to choose large measurement intervals could reduce the accuracy of conclusions drawn using smart meter data. Deploying Privacy-by-Design and Privacy-Enhancing Technologies (PETs), like cryptographic algorithms and Data masking techniques, may reduce the risks originating from drawing conclusions from the data without changing the measurement interval. More information on this topic can be found in the guidelines and publications of the European Union Agency for Cybersecurity (ENISA).[15]

On the subject of **occupancy sensor or occupant tracking** in smart buildings, Lee et al. (2019) and Kessler et al. (2020) pointed out to the importance of tracking people in buildings, including locating and accounting for people in case of emergency (e.g. lost children in a building and making sure all people are evacuated in case of a natural disaster); identifying threats (e.g. making sure that unwanted people are prevented from being in restricted areas); as well as maximizing occupant comfort, increasing energy efficiency, and collecting data for research (e.g. collecting building simulation data). Unfortunately, tracking can lead to the gathering of information that can be used to violate the privacy and confidentiality of the people being tracked. Kessler et

[14] Source: https://gdpr.eu/data-protection-impact-assessment-template/

[15] https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies

al. (2020) proposed a method for tracking people in a building while preserving their privacy by using 'windowed floor vibration data' so that the individual's anonymity is preserved while sacrificing little localization accuracy. Lee et al. (2019) focused on possible privacy breaches in case of attack/hack and proposed mitigation strategies by the principle of 'least privilege' that can be used as a governing principle in providing the right level of information to various applications. The exact details of implementing the mitigation strategies will differ from application to application. Differential privacy and deletion of past occupancy data could also be used to enhance the privacy of the building occupants.

Pappachan et al. (2017) discussed **privacy threats in relation with Building Management Systems (BMS).** BMS are cyber-physical systems that are used to manage buildings by monitoring different utility services. BMS capture a digital representation of a dynamically evolving building at any point in time for purposes such as comfort and security. But this representation might contain distinct patterns which can reveal the absence or presence of people and their activities, potentially resulting in the disclosure of data that people might not feel comfortable disclosing (e.g., where they go, what they do, when and with whom they spend time, whether they are healthy and more). Pappachan et al. (2017) proposed a framework for smart buildings which includes three main components:

- First, IoT Resource Registries (IRRs) which broadcast data collection policies and sharing practices of the IoT technologies with which users interact.
- Second, IoT Assistants which selectively notify users about the policies advertised by IRRs and configure any available privacy settings.
- Third, Privacy-Aware Smart Buildings, which publish building policies, receive the privacy settings of users, and enforce them when collecting user data or sharing it with services.

The **Privacy-Aware Smart Buildings** measures comprise a set of building policies and user preferences:

- A **building policy** states requirements for data collection and management set by the temporary or permanent owner. Building policies can be related to the infrastructure of the building, the specific sensors deployed in the building, the events taking place inside the building, and the communication policies to the building users. These policies (in most cases) have to be met completely by the other actors in the pervasive space. Some examples of building policies: A building administrator defines that either an ID card or fingerprint verification is needed to access meeting rooms; the building management system stores your location to locate you in case of emergency situations.
- A **user preference** is a representation of the user's expectation of how data pertaining to her should be managed by the pervasive space. These preferences might be partially or completely met depending on other policies and user preferences existing in the same space. Some examples of user preferences: Do not share the occupancy status of my office in after-hours; Do not share my location with other occupants.

For example, when a user connects to a **WiFi Access Points (AP)** for Internet connectivity in a building, the event is logged for security purposes (the information logged includes the MAC address of the device and AP, and a timestamp) as part of the building policy. Using background knowledge (e.g., the location of the AP) it is possible to infer the real-time location of a user. Therefore, it is important to understand user preferences and expectations with respect to the information collected and used by a system like BMS (Pappachan et al., 2017).

In 2016, Sir Tim Berners-Lee introduced the **web decentralization project known as Solid**[16]. Solid is a specification that lets people store their data securely in decentralized data stores called Pods. Pods are like secure personal web servers for your data. The project aims to radically change the way Web applications work today, resulting in true data ownership as well as improved privacy by developing a platform for linked-data applications that are completely decentralized and fully under users' control rather than controlled by other entities. The goal of Solid is to allow users to have full control of their own data, including access control and storage location. On the possible implementation of this concept for building data, Werbrouck et al. (2019 and 2021), presented a view on the federated Linked Building Data and a decentralised Common Data Environment reflecting on the ongoing research and a proof-of-concept for the setup of a web-service for creation and management of Linked Building Data generated with the Solid-React generator.

In a wider scope with certain relevance for smart buildings, the following norms and regulations can be considered next to the GDPR, such as the **ISO 27000** series that provide the framework for organizations to perform good information security management and the IEC62443, initiated in 2005 by the International Society for Automation (ISA)

[16] About Solid · Solid (solidproject.org)

In its core, the ISO 27000 series on information security standard upholds three aspects of information namely:

1. Confidentiality - information should not be available or disclosed to unauthorized persons or entities.
2. Integrity – ensured that information is complete and accurate and protected from falsification or corruption
3. Availability – ensures that the information is accessible and usable upon request from the authorized persons.

The ISO 27002 described the normative data control measures that need to be in order before a certification can be issued. These are the normative measures, in other words, these are the minimum requirements that must be in place before ISO certification is granted. The Annex A of this standard describes 114 best practices, including but not limited to:

1. Physical access control
2. Firewall policies
3. Security staff awareness programs
4. Procedures for monitoring threats
5. Incident management processes
6. Encryption

In addition to these measures, a risk assessment (e.g. carried out in accordance with ISO27005) is required to determine whether additional control measures are necessary.

The IEC 62443 cyber security management standards is a series of standards that provide a standardized approach for ensuring the cyber security of Industrial Automation and Control Systems (IACS). As such, their main goals is to provide assurance to the asset owners about the security of their systems. The IEC 62443 standards series were initially developed for the industrial process sector but have been slowly finding their way on other sectors as well. The reason why a specific standard had to be developed to secure IACS is because "traditional" IT standards have different performance requirements due to the different magnitude of risks involved in case of a cyber-attack: only economic consequences for IT systems versus the risks of economic, environmental, or public health catastrophe in the case of essential IACS.[17]

From the industry's view, Davis (2020)[18] summarized the four essential pillars of **cloud security** that include:

1. Visibility and compliance that enable ongoing insight into the entire cloud environment and thereby creating the opportunity for ongoing improvement
2. Compute-based security that covers automated vulnerability management and operational security of the compute engine or compute workload
3. Network protections
4. Identity security

The subject of cloud security is important in the Brains4Buildings project in relation to the cloud solutions used for Building Management Systems (BMS) and data analytics platforms as described in chapter 4 in this report.

[17] Understanding IEC 62443 | IEC

[18] The 4 essential pillars of cloud security – GCN

3 NEEDS AND CONSIDERATIONS FROM THE REAL ESTATE OWNERS' PERSPECTIVE

This chapter reports the findings from the discussions with the real estate asset owners and managers in the B4B project consortium. For these stakeholders, the main issues related to data privacy, ethics and security can be identified in two groups: 1) the necessities with regard to data sovereignty, ownership and liability; and 2) the client/user requirements to select and apply the IT and data solutions which are available on the market (i.e. market offers).

3.1 Data sovereignty and ownership

The International Data Spaces Association (IDSA) defines data sovereignty as the ability of a natural person or a corporate entity for exclusive self-determination regarding its economic data goods. In other words, data sovereignty is the ability for each stakeholder to control their data by making decisions as to how digital processes, infrastructures, and flows of data are structured, built, and managed, based on an appropriate governance scheme enabling specification of terms and conditions. While GDPR grants individuals the right to decide what data collectors are allowed to do with their personal data and what not, European data spaces will provide the tools to exert these rights and stay in control over that data (Nagel et al., 2021).

Data sovereignty is related to, and sometimes identified with, claims to ownership of data. Take for example, the sovereignty of medical records. The doctor creating the medical data or the hospital storing them are not the owners of this information. Indeed, all medical information belongs to the patient. Consequently, patients have control over their data and access to this information (Plateaux et al., 2013). In terms of ownership, the following situations apply:

- The real estate owners in the B4B consortium are the owners of building-related data (e.g. building specifications, maintenance status) and the data that is collected or generated by on-premise measurement devices (e.g. sensors, energy meters, and BMS in and on the buildings). The data from these devices/systems can be stored on cloud platforms managed by the service providers; however, at completion or termination of the contracts, the real estate owners get all data from the BMS and other providers.
- The real estate owners are usually not the owner of the energy data of the grid or off-premise systems unless contractually agreed with the energy and/or system providers.
- The real estate owners are not the owners of person-related data although this data is collected within or in-relation-to the buildings. For person-related data, the real estate owners must comply to the GDPR.

The real estate owners in the B4B consortium understand the necessity to ensure data sovereignty, and therefore, the following measures are put in place:

- Data security: Security certificates, in particular the ISO 27001, are known and applied for data collection and storage services. The representatives from the IT departments of the real estate owners emphasize that good security, including access control, is essential to prevent data loss and to ensure optimal performance. The highest measures on data security are applied when person-related data is collected as the real estate owners aim to prevent data leaks.
- Data storage: Most building data is stored in the cloud platforms, such as Microsoft Azure and Amazon. Along with the building data, information on building legislations is also stored. APIs are used for the connection between the different data sources and the cloud platforms.

3.2 Considerations for applying market solutions

With the rise and further development of technologies that propagate IoT, smart buildings and smart cities, data privacy, ethics and security are becoming ever important. Real estate owners and managers are responsible to ensure data privacy, ethics, and security with the market solutions that they select and implement for their buildings. Therefore, the following considerations are taken:

- Real estate owners that rent out parts of or the entire office buildings or facilities to other companies expect that their clients will demand that the data collection, storage and use is handled responsibly. Such a demand drives the inclusion of the GDPR and the ISO 27000 series in the contractual agreements to give assurance to the (potential) clients.
- System and service providers together with the real estate owners are expected to act in an ethical and responsible way when collecting any data whether or not that data is person related.

- Much data is supplied by various systems and providers, for example electricity network providers and water companies, which have their own APIs to connect to the data platforms. Compliance to open standards becomes more and more important in selecting and implementing smart building solutions.
- Predictive capabilities of the smart building solutions are gaining increasing interest from the real estate owners, for instance: smart solutions that could help building occupants, managers, and owners to anticipate or timely identify problems regarding indoor comfort and ventilation (especially in offices, also related to COVID-19 health measures), relative humidity (in factory buildings), and energy cost projection.
- Aligned with this, the real estate owners and managers also anticipate the emergence of digital twins for practical applications and to accommodate more sensors for higher accuracy. Take for example the application for setpoints: such setpoints are currently done manually; using digital twins it should be possible to learn and optimize the setpoints more adaptively to the energy generation and storage facilities, heating/cooling installations, building use, end-user preferences, and indoor/outdoor conditions.

4 NEEDS AND CONSIDERATIONS FROM THE IT PROVIDERS' PERSPECTIVE

This chapter reports the findings from the discussions with the developers and providers of digital platforms and services for Building Management Systems (BMS) in the B4B project consortium. For these stakeholders, the main issues related to data privacy, ethics and security can be identified in two groups:

1. the technical implementation of the privacy, ethics and security policies on the digital platforms; and
2. the privacy/ethics/security considerations in exploring new business or operational models

4.1 Technical implementation of privacy, ethics, and security policies

A BMS (Building Management System) is in its core a computer-based control system that collects data and monitors and controls a building's mechanical and electrical equipment. It often operated behind the scenes to ensure optimal performance of those systems. With the increase of smart devices and systems within buildings the communications between them grow ever more complex. Data communication between digital devices and platforms is illustrated in the following example.

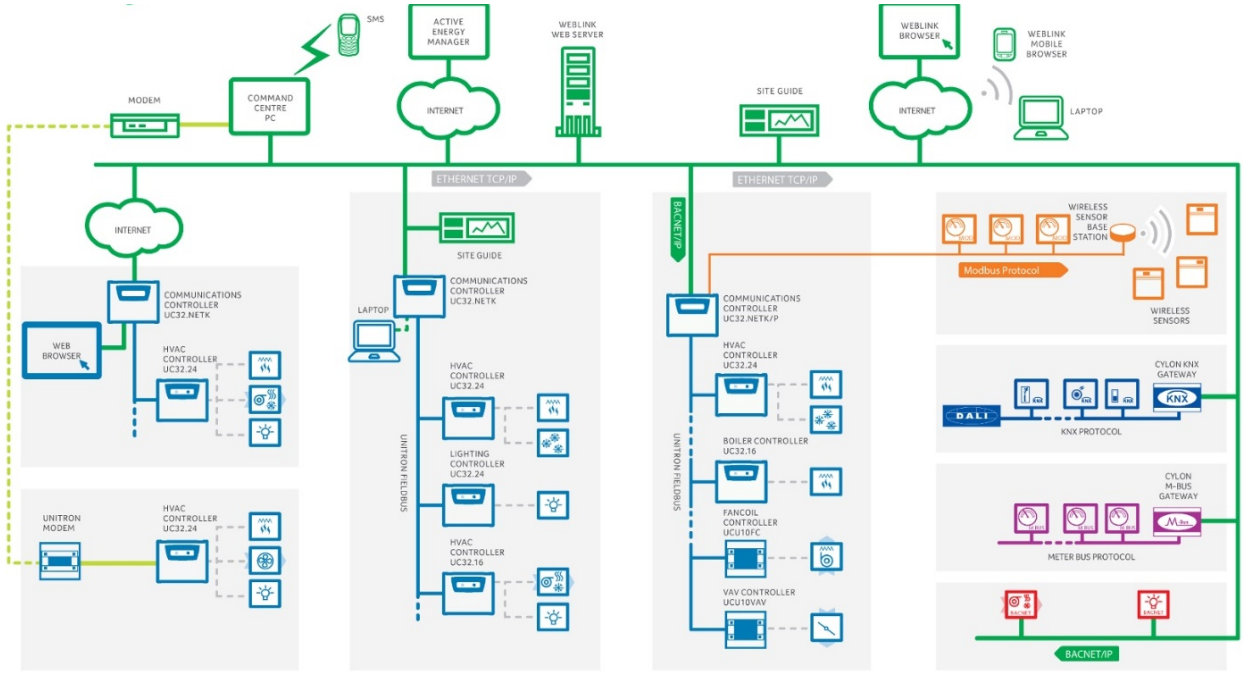

Figure 5 Example of BMS architecture from Cylon systems[19]

The developers and providers of digital platforms and services for smart buildings are aware of the threats to data privacy, ethics and security, which can be recognized in the 3 types of risks:

- Access risks, i.e., compromised access, denial of service, credential/identity theft, phishing.
- Data risks, i.e., incomplete or loss of data, damages or inaccurate data, data theft during transfers.
- Platform risks, i.e., not secured or not isolated data on the platform, not restricted access, physical security risks of the connected devices.

In general, measures are taken regarding data encryption, open or closed source software, and mitigation of risks, threats, and vulnerability. ISO27005 gives some guidelines how risks can be defined and mitigated. Periodic penetration tests are carried out as part of the security measure to detect the weakest link in a connected network of systems. Addressing these risks depends on the types of concepts and systems used by the platform developers and providers. The most common concepts, which can be divided into local and building level controls and can be used in combination with each other, are:

[19] Source: https://www.nykeenergy.com/about-us/bms-explained/

1. **Room-level controls:**

- Local wired network (BUS), dedicated protocol, limited capacity, not direct accessible from outside.
- The BUS system is a local wired network with a dedicated protocol and limited capacity. It is not directly accessible from the outside, but it does enable a two way communication system that allows for connecting multiple systems with each other and for the transfer of data between the Input/Output (I/O) devices. Examples of such protocols include: modbus, LON, BACnet/mstp, Dali and KNX. Several examples of I/O devices are: Priva controllers that allow for manual override through their intervention modules (manual override can be physical or digital, on-site or remote) and Schneider standard devices in buildings with common functionalities.
- Wireless local network, dedicated protocol, mostly limited capacity.
- The wireless local network and the pertaining connections and protocols have dedicated protocols and usually limited capacity. It provides access to and remote-control systems through a secure connection. Within buildings there are a lot of wired communications between devices. The common wireless communication protocols and technologies that these devices use include: BACnet ; Lora (from "Long Range") protocol which is in essence a low energy and relatively small distances (of a few kilometres) of wireless communication; Zigbee; EnOcean; Bluetooth; Mesh networks and gateways; Modbus, MQTT , OCPI, KNX, WiFi-based, etc. The BMS platforms usually consume the data through a middleware platform. The B4B stakeholders use existing solutions for this, such as Niagra platform by Honeywell, and establish a contract for API updates, drivers' updates, etc.

2. **Building-level controls:**

- Local networks using TCP/IP as transport protocol, large capacity. Examples: BACnet-IP, LON-IP, Modbus-IP, MQTT, OCPI, KNX-IP. Made safe and secure via standard IT-solutions (such as VPN), made safe and secure via standard IT solutions. Most GBS relies on / uses the standard IT security concepts and solutions to implement instead of BMS supplier dependent solutions.
- One frequently used security measure for a two way communication between the building systems and the cloud services is to have all connections initiated from within the building. This can be done by setting-up a unique **Virtual Private Network (VPN)** service with a local VPN client inside the building. It ensures that communication can never be initiated from external sources. A VPN is A virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks.[20]

The subjects with a high importance for developing and applying data integration solutions for the B4B project are described in the following.

- Data about building energy and indoor environment quality, such as data on energy sources and consumptions, air quality and CO_2 concentration, regards the building as a whole or the specific building spaces. Usually, no direct data about natural persons is collected and processed. As such, the building energy data is considered low risk for privacy considerations, and although data encryption is used for all data transfers (in the communication streams), an end-to-end encryption as a security measure is not urgent.
- The main challenges when discovering and extracting information from different systems in an existing building are as follows.
    - Many existing buildings are provided with non-open BMS systems. Closed BMS systems form a problem in many existing buildings. There are technical and non-technical challenges with reporting using BMS systems. For instance, the BMS suppliers claims that their systems are "open", but there is no consensus on what "open" system means, and as such, certain data points are hidden and transported on scrambled way through back-end protocol; and in that case, BACnet points can be integrated, but other points are not accessible.
    - When a BACnet datapoints can be read, it is essential to know the purpose/meaning/use of the datapoint within the building. This is the area were open standards, such as Haystack or Brick, can be of help. However, there are still some constraints, for example: Haystack is currently not sufficient as an open standard to store data, and therefore, a translation/conversion should still be done using connectors from individual databases.

[20] https://doi.org/10.6028/NIST.SP.800-113

- In the cases when standard protocols are used, the implementation approach varies from building to building. In the Dutch market more than 50% of all installed systems are by Priva. On one hand, this kind of 'standardise' the approach, but on the other hand, the consequence is that the platforms ar depending on the possible connections with Priva.
- On the non-technical aspect, there is a challenge related with the lack of knowledge on IT solutions from the facility managers.
- There are also contractual issues. Large international market players, like Honeywell, Siemens, Schneider, do not share data to allow them to manage the systems by themselves. When cloud solutions are used, robust contractual agreements are crucial, for example an agreement with Microsoft to transfer data from West European Azure environment to North American environment in case of bugs; however, in this agreement only the metadata is transferred.
- The common security features used by the platform developers and providers in the B4B project are: the so called Technical-VLAN setup (VLAN-virtual-LAN) which connects to external services via OpenVPN; keeping the technical networks separated from administrative networks; and the use of access rights linked to assigned users/groups.
- On the management of the levels of control that the different stakeholders have on data from the building, the following strategies are used:
    - The roles (as described in section 3), access rights and permissions, which are granted to the users and managed by the platform administrator, determine the level of data that can be used by each user. Solutions for automatic user access synchronization with Microsoft user control are also commonly used. As for Simaxx, its architecture comprises a site with several sub-sites, and Simaxx aims to give all the knowledge and tools to the customer (see Fig. 6 and 7).

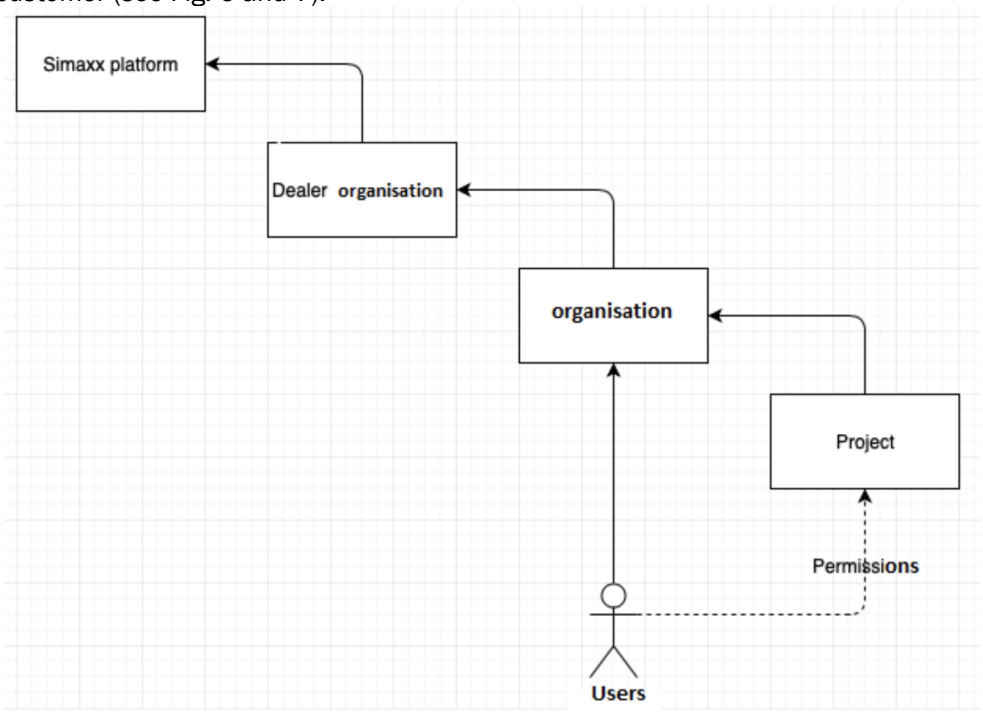

Figure 6 High-level example from Simaxx

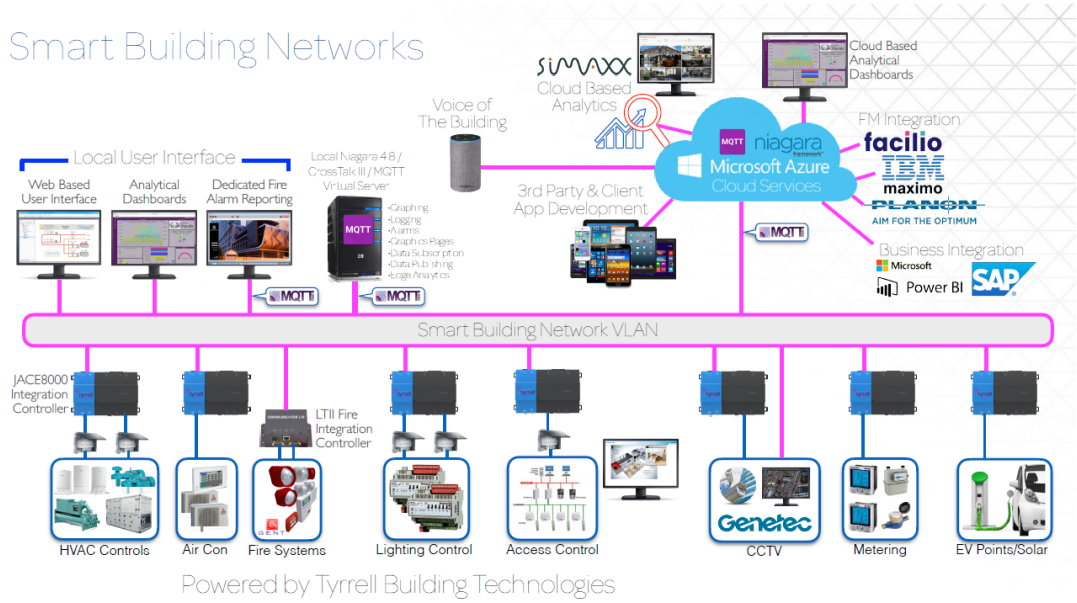

Figure 7 Elaborated example from Simaxx

- The levels of control on data also depend on the **system installations**. For products that run on-site (on-premise), the customer owns the database. When, based on the service contract, a third-party cloud platform is used, such as Microsoft Azure, the connection between the customer and this platform goes through a secure OpenVPN. To mitigate the risk of data loss, the customer is always able to download the entire dataset from the Azure database.
- Usually, it is contractually agreed that the real estate owner is the data owner, this real estate owner can also define the **data sharing policy and the periodic reviews** in case of needed improvements or changing policies.

– Reviewing the relevant guidelines related to energy data of buildings and utilities, such as:
  - the Dutch policy on Aquifer Thermal Energy Storage (ATES)[21];
  - the requirements for heat data in the social housing sector as regulated by the warmteWET
  - the ISSO 100 -107 series about sustainable maintenance of building energy installations
  - the references to BREEAM-NL and the new development of Radio Equipment Directive (RED) for secure IoT devices[22]
  - The International Energy Agency's Energy in Buildings and Communities programme (IEA EBC)[23] - Annex 81 Data-Driven Smart Buildings[24] with a.o. objectives to provide the knowledge, standards, protocols and procedures for low-cost high-quality data capture, sharing and utilization in buildings.

[21] https://dutch-ates.com/wp-content/uploads/2016/09/DutchPolicyOnATESSystems092016.pdf

[22] Nieuwe regels maken slimme producten slimmer (nen.nl)

[23] https://www.iea-ebc.org/

[24] https://annex81.iea-ebc.org/

4.2 Privacy, ethics, and security considerations for business models

The developers and providers of digital platforms and services for Building Management Systems (BMS) in the B4B project consortium indicated their future outlook and business models.

The acquisition of additional data that is targeted in the coming years include:

- BIM data (3D geometry in IFC models). Several B4B consortium partners are currently working on getting the samples from the TU Eindhoven. The BIM data can be used to improve the tenant experience and help the facility managers with automated fault detections.
- CO2, air quality, and fine particles data as well as apps for real time perceived comfort and measurement of user behaviours and interventions (such as opening windows, playing with blinds, changing thermostat values) to make improvements of indoor environmental quality, comfort and health.

Along with the additional data, extended functionalities of the digital platforms are also foreseen, such as:

- **Machine Learning** for making prognoses in software systems (like InsiteSuite from Kropmans among other examples) where future scenarios can be anticipated based on the data from IoT for more flexible energy systems.
- Software plugins on BMS and data buffering and predictive capability of the **viewing and reporting systems**, as enhancement of the current systems that collect data (historical and current data) and visualize it based on BMS .
- Extending the data models to incorporate **multiple digital facility management solutions**, such as Maximo, Planon, Ultimo and Topdesk.
- Expanding the coverage of energy management of buildings also to address the **surrounding facilities**, such as integration and analytics of data from the EV charging stations and demand-response/balancing systems for the grid operators.

The relevant considerations on privacy, ethics and security that go with the new outlook or business models regard the aspects that have been described in Chapter 2 of this report, in summary:

- The privacy, ethics, and security issues regarding smart energy meters in buildings and grids, and the occupancy data collected in the buildings.
- The security of cloud services, and the agreement with the clients whether the data can also be shared with third parties for optimization purposes.
- Specific (higher) security requirements for certain organizations, such as governments and pharmaceutical companies where the BMS also controls the laboratory facilities.
- The GDPR compliance is not only an obligation, but also gives an opportunity to promote structured data, data traceability and provenance, high ethics, and the attention to the users that will help to build more between the real estate owners and the platform providers.

5 CONCLUSIONS AND FOLLOW-UP RECOMMENDATIONS

5.1 Conclusions

Smart buildings in general, and projects like the Brains for Buildings (B4B) in particular, collect and process a large amount of data. When person-related data is part of it, adequate attention should be given to privacy and ethics. In the EU, this is regulated by the General Data Protection Regulation (GDPR) that came into force as of May 25th, 2018, in all EU member states to harmonize data privacy laws across Europe.

The literature study and the stakeholder interviews with the real estate owners and IT platform providers within the B4B consortium, as reported in this deliverable, point out the areas where B4B might be concerned with person-related data, namely:

- at registering the occupancy of the buildings in relation with optimization of energy consumption and maintenance; and
- at understanding the end-users' behaviour in relation to customizing ease of use, comfort, and indoor environmental quality in relation with energy performance.

For both areas, B4B does not necessarily process the personal data; however, the relevant concerns related to privacy, ethics and security are:

- Assuring the compliance to the GDPR through Privacy-Aware Smart Buildings measures wherein the building owners/administrators clearly communicate the 'building policy' on data collection and management (i.e., clarifying which data is collected, for what purpose, and how the data is managed); and b) the tenants/building occupants have rights for the 'user preference' in connection with the 'building policy'; and
- Assuring the data security at the Building Management Systems (BMS), the on-premises and off-premises (cloud) data platforms, and the IoT devices, including the end-users' mobile devices and wearables in order to mitigate the risks of theft and misuse of (personal) data, system breaches and failures.
- The outcomes of the current study highlight the crucial aspect of wireless and cloud platform data security as well as standardization regarding data management and IoT. As multiple devices, systems and (cloud) platforms are used in B4B proposed solutions, these aspects deserve a further investigation. The use of open standards will be addressed in the follow-up deliverable on standardization.

5.2 Follow-up recommendations

This deliverable is the first one of the two B4B deliverables on data privacy, ethics, and security. The overview of relevant aspects as well as technological and non-technological measures as presented in this deliverable will be further examined in relation with the development of the data integration architecture and API-oriented solutions in B4B. The second deliverable will thus specify the recommended measures to be implemented in the B4B proposed solutions.

This deliverable gives input for the follow-up research to develop a standardised method for verifying the compliance of the data integration solutions as proposed in the B4B project. This method will contribute to emboldening the confidence of the end-users and widening the market acceptance for the project results.

REFERENCES

Literature

- Berners-Lee, T. et al. Solid. [link]
- Beckel, C., Sadamori, L., Staake, T., and Santini, S. (2014). Revealing Household Characteristics from Smart Meter Data. Energy 78:397-410. DOI:10.1016/j.energy.2014.10.025
- Università della Svizzera Italiana (USI), Lugano, Switzerland
- Cejka, S., Knorr, F., and Kintzler, F. (2019). Privacy Issues In Smart Buildings By Examples In Smart Metering. In Proceedings of 25th International Conference on Electricity Distribution (CIRED), Madrid, 3-6 June 2019. [link]
- European Data Protection Supervisor (EDPS). TechDispatch #2: Smart Meters in Smart Homes. 16 October 2019. [link]
- Kessler, E., Masiane, M., and Abdelhalim, A. (2020). Privacy Concerns Regarding Occupant Tracking in Smart Buildings. [link]
- Lee, D. and Hess, D.J. (2021). Data privacy and residential smart meters: Comparative analysis and harmonization potential. Utilities Policy, Volume 70, 2021, 101188, ISSN 0957-1787, doi: https://doi.org/10.1016/j.jup.2021.101188. [link]
- Lee, P., Shin, E.J., Guralnik, V., Mehrotra, S., Venkatasubramanian, N., and Smith, K.T. (2019). Exploring Privacy Breaches and Mitigation Strategies of Occupancy Sensors in Smart Buildings. In Proceedings TESCA'19, November 13–14, 2019, New York, NY, USA. [link]
- McDaniel, P. and McLaughlin, S. (2009) Security and Privacy Challenges in the Smart Grid. IEEE Security Privacy, 7, 75-77. DOI:10.1109/MSP.2009.76.
- Nagel L., Lycklama D. (2021): Design Principles for Data Spaces. Position Paper. Version 1.0. Berlin. DOI: http://doi.org/10.5281/zenodo.5105744
- Pappachan P. et al., "Towards Privacy-Aware Smart Buildings: Capturing, Communicating, and Enforcing Privacy Policies and Preferences," 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), 2017, pp. 193-198, doi: 10.1109/ICDCSW.2017.52. [link]
- Plateaux, A, Lacharme, P, Rosenberger, C, et al. (2013) A contactless e-health information system with privacy. In: 2013 9th international wireless communications and mobile computing conference (IWCMC), Sardinia, Italy, 1–5 July 2013, pp. 1660–1665.
- Werbrouck, J., Pauwels, P., Beetz, J., and Mannens, E. (2021). Data Patterns for the Organisation of Federated Linked Building Data. In Proceedings of CIB W78 - LDAC 2021. [link].
- Werbrouck, J., Pauwels. P., Beetz, J., and Berlo, L. van (2019). Towards a Decentralised Common Data Environment using Linked Building Data and the Solid Ecosystem. In Proceedings of 36th CIB W78 2019 Conference, Northumbria University, Newcastle, United Kingdom. [link]
- Wesselingh, E.. Stokman, H. Willigenburg, P. van. (2015). DCCPP = Privacy by Design. Direct Current Communications & Privacy Protocol (DCCPP) Proposed for a Privacy Protective DC Smart Grid. SSRN (July 3, 2015). [link]
- Ząbkowski, T. and Gajowniczek, K. (2013). Smart Metering And Data Privacy Issues. Information Systems in Management (2013) Vol. 2 (3) 239−249. [link]

European directives

- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ 2000 L 178, p. 1)
- Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45, and corrigenda OJ 2004 L 195, p. 16, and OJ 2007 L 204, p. 27)
- European Union, Charter of Fundamental Rights of the European Union, 7 December 2000, OJ L C 364/01, available at: http://www.refworld.org/docid/3ae6b3b70. html [accessed 7 March 2014]

List of standards

- ISO/IEC 29134 (project), Informatietechnologie – Beveiligingstechnieken – Privacyeffectbeoordeling – Richtsnoeren, Internationale Organisatie voor Standaardisatie (ISO)
- NEN-EN-ISO/IEC 27001:2017+A11:2020 nl Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging – Eisen

- https://www.nen.nl/ict/digitale-ehtiek-en-veiligheid/cyber-privacy/informatiebeveiliging

Selection of internet links on GDPR information and discussions

- Ways GDPR will affect Tech and other Businesses - Wiredelta
- Data protection | European Commission (europa.eu)
- Data protection impact assessment (DPIA) | Autoriteit Persoonsgegevens
- Dataprincipes - Digital Society (thedigitalsociety.info)
- Dutch vision on data sharing between businesses | Report | Government.nl
- EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)
- Intelligent Buildings: Understanding and managing the risks (fm-house.com)
- IT Governance - Governance, Risk Management and Compliance for Information Technology Ireland
- Wetten | Autoriteit Persoonsgegevens

APPENDICES

We conducted several interviews with the consortium members involved within Work package 4 of the Brains4Buildings consortium (see Appendix A). In those interviews two sets of questions (containing marginal differences) were given to the two groups of interviewees: the real estate owners and platform providers. The interview questions are relevant for this and another deliverable, D4.3.

- Appendix A: list of interviewees (name, company name, date interviewed)
- Appendix B: interview questionnaires (Real Estate owners' questionnaire, Platform providers questionnaire).
- The questions that were specifically relevant for this deliverable are highlighted in green.

APPENDIX A

Name	Company name	Date Interviewed
Niels de Jong	Cloud Energy Optimizer	28.09.2021 and 1.11.2021
Jan-Willem Dubbeldam	Kropman	21.09.2021 and 01.11.2021
Joep van der Velden	Kropman	21.09.2021 and 01.11.2021
Simon Hopkins	Simaxx	14.09.2021 and 23.09.2021
Berno Veldhuis	RVB	7.10.2021 and 27.10.2021
Nico Mutsaers	Philips	28.09.2021 and 1.11.2021

APPENDIX B

Brains for Buildings – WP4 Data Integration

Questionnaire for building owners

Name :

Organization :

1	Question	Please describe your role in the company, how you are related to building sector and your experience?
	Answer	
2	Question	What are the types of buildings that you own? And who manages them?
	Answer	
3	Question	What are the issues you currently face in the operational phase of these buildings that leads you to seek solutions from this project?
	Answer	
4	Question	What data do you have about your assets and how (where) do you store, access and update that information?
	Answer	
5	Question	What are the naming conventions, classifications and procedures you use for accessing this information?
	Answer	
6	Question	What are the devices and systems that generate data about the building operation and the occupants?
	Answer	
7	Question	What data are usually monitored and collected?
	Answer	
8	Question	What is the purpose of collecting above data?
	Answer	
9	Question	Do you have all the data that you need, or what additional data do you think will be included in the future and why?
	Answer	
10	Question	Do you use naming conventions for the data? What are they?
	Answer	
11	Question	How is data stored? And for how long?
	Answer	
12	Question	In which formats the data is stored?

	Answer	
13	Question	There are many parties involved in building operation like platform providers, building owners, renters, occupants, etc. What level of control/ownership each party has on data?
	Answer	
14	Question	Do you perform data analysis? (If the answer is “yes”, skip Question 15 & 16 and go to Question 17. If the answer in “no”, answer Question 15, 16 and go to Question 25)
	Answer	
15	Question	Do you try to continuously improve any of the building performance aspects: operation cost, comfort, energy, user feedback? If yes, in what ways? If not, why?
	Answer	
16	Question	How do you measure or benchmark the performance of a building (for example in terms of its energy efficiency and occupant satisfaction)?
	Answer	
17	Question	What data do you analyze and what do you expect by doing it?
	Answer	
18	Question	What is the procedure for data analysis and who is responsible for this task?
	Answer	
19	Question	What platforms and solutions do you use for data analysis?
	Answer	
20	Question	Where do you apply the results from above data analysis?
	Answer	
21	Question	Do you perform the same analysis for each building that you own?
	Answer	
22	Question	What can you say about the visualization and reporting ability of the existing systems? What value do you extract from the visualizations?
	Answer	
23	Question	What limitations do you encounter when analyzing data using the platforms and solutions you mentioned?
	Answer	
24	Question	What do you think about the complexity of the data analysis procedure? Is it efficient and easy to use or cumbersome and needs lot of manual work?
	Answer	

25	Question	What are some critical requirements of occupants and how much control do occupants have over those requirements on the building systems?
	Answer	
26	Question	Do you collect and analyze occupants' feedback? How? If not, why?
	Answer	
27	Question	Do you operate more than one system (from different vendors) for managing your assets? If so, what are the challenges that you run in to when operating multiple systems from different vendors?
	Answer	
28	Question	What are the solutions that you currently use to solve above problems?
	Answer	
29	Question	What external constraints do you experience for data collection and analysis?
	Answer	
30	Question	What security features are used in your systems? How do you prevent data tampering or misuse?
	Answer	
31	Question	What other drivers are there for these security measures?
	Answer	
32	Question	How do you apply and maintain the General Data Protection Regulation?
	Answer	
33	Question	What functionalities would you like to have in a future smart building platform and how do you expect your buildings to perform differently in future by using such platform?
	Answer	

Brains for Buildings – WP4 Data Integration
Questionnaire for platform providers

Name :
Organization :

1	Question	Please describe your role in the company, how you are related to building sector and your experience?
	Answer	
2	Question	What types of services/solutions that you usually provide for buildings?
	Answer	
3	Question	What are the solutions that are mostly requested by building owners from you? And are you able to provide those solutions?
	Answer	
4	Question	Which systems and protocols available in buildings can be handled in your solutions?
	Answer	
5	Question	What issues do you encounter when discovering and extracting information from different systems, specially from an existing building?
	Answer	
6	Question	What data is usually monitored and collected?
	Answer	
7	Question	What is the purpose of collecting above data? Do you think all the data collected in buildings are utilized in some way or are there unnecessary data that never serve any purpose?
	Answer	
8	Question	Do you include building information in your solutions? How?
	Answer	
9	Question	In which formats you find the data? And what desired formats do you convert them in to?
	Answer	
10	Question	Do you use naming conventions for the data? What are they? How do you convert client's naming convention to your desired format?
	Answer	

11	Question	What are your data storage techniques? (Type of database, on-premises or cloud, retention period)
	Answer	
12	Question	What platform do you provide to the client for data consumption and how do you charge for it?
	Answer	
13	Question	What are the typical functionalities of the above platforms?
	Answer	
14	Question	How sensitive are your solutions for a certain upgrade in the building?
	Answer	
15	Question	What security features are used in your systems? How do you prevent data tampering or misuse?
	Answer	
16	Question	What other drivers are there for these security measures?
	Answer	
17	Question	There are many parties involved in building operation like platform providers, building owners, renters, occupants, etc. What level of control each party has on data?
	Answer	
18	Question	Do you have all the data that you need in buildings, or what additional data do you think will be included in the future?
	Answer	
19	Question	Do you perform data analysis? If so, what are the typical data analysis cases available in the solutions provided by you?
	Answer	
20	Question	What kind of data do you analyze? (Historical, live)
	Answer	
21	Question	What platforms do you use for data analysis?
	Answer	
22	Question	What is the normal procedure for data analysis?
	Answer	
23	Question	How do you validate whether the data that you collect is correct and how do you handle missing/ incorrect data?
	Answer	

24	Question	After analyzing, what kind of insights do you provide about the buildings and to whom?
	Answer	
25	Question	What benefits have you brought to the building owners and occupants from data analysis?
	Answer	
26	Question	Are your solution packages generic, specific for building category or different for each building?
	Answer	
27	Question	How easy or hard it is to reuse or scale one of your solutions from one building to another, given the variety of systems in different kinds of buildings?
	Answer	
28	Question	Do you provide solutions to collect and analyze occupants' feedback? If so, how do they work?
	Answer	
29	Question	Do you refer to any standards and/or regulations when you are providing solutions?
	Answer	
30	Question	What external constraints do you experience for data collection and analysis?
	Answer	
31	Question	What is your policy regarding privacy and ethical usage of occupant and other data in the building? How do you apply it in practice?
	Answer	
32	Question	Have privacy and ethical usage of data ever become a barrier to implement any of your solutions? How and where?
	Answer	
33	Question	What other functionalities would you like to add further in your solutions?
	Answer	