D1.5 SAFETY AND PRIVACY FOR DIGITAL TWINS IN THE CONSTRUCTION INDUSTRY

João Gonçalves, María Palacios Barea & Iris den Hollander, EUR

@AshvinH2020
ASHVIN H2020 Project
www.ashvin.eu

ASHVIN has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 958161. This document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.

Project Title	Assistants for Healthy, Safe, and Productive Virtual Construction Design, Operation & Maintenance using a Digital Twin
Project Acronym	ASHVIN
Grant Agreement No	958161
Instrument	Research & Innovation Action
Topic	LC-EEB-08-2020 - Digital Building Twins
Start Date of Project	1st October 2020
Duration of Project	36 Months

Name of the deliverable	Safety and privacy for digital twins in the construction industry
Number of the deliverable	D1.5
Related WP number and name	WP 1 IoT driven digital twin platform
Related task number and name	T1.4Cybersecurity & data protection
Deliverable dissemination level	PU
Deliverable due date	30-09-22
Deliverable submission date	30-09-22
Task leader/Main author	João Gonçalves (EUR)
Contributing partners	MFX, CERTH, DTT
Reviewer(s)	MFX, CERTH

ABSTRACT

The deliverable reports privacy and security requirements of the industry and describes how these requirements have been detailed for implementation into the ASHVIN platform and how these may be generalized to the broader construction industry. It suggests an integrated approach to cybersecurity and privacy, urging practitioners to consider technical and human aspects in tandem to identify vulnerabilities and privacy risks, while also proposing integrated solutions to these risks. The final part of this document provides some key privacy and security recommendations for implementation of digital twin technology in the construction sector.

KEYWORDS

Digital Twin, Cybersecurity, Privacy, Data Protection, Safety

REVISIONS

Version	Submission date	Comments	Author
V0.1	01/09/2022	Internal review	EUR
V0.2	20/09/2022	Coordinator review	EUR, MFX, CERTH, DTT
V1.0	28/09/2022	Submission Version	EUR, MFX, CERTH, DTT

DISCLAIMER

ACRONYMS & DEFINITIONS

CERTH	Ethniko Kentro Erevnas Kai Technologikis Anaptyxis
DPIA	Data Protection Impact Assessment
DTT	Digital Twin Technology GMBH
DPIA	Data Protection Impact Assessment
EUR	Erasmus University Rotterdam
FAS	Przedsiebiorstwo Robot Elewacyjnychfasada Sp Zoo
GDPR	General Data Protection Regulation
IAM	Identity and Access Management
IoT	Internet of Things
ISB	Information Security Behaviour
MFX	Mainflux Labs
mTLS	Mutual TLS authentication
NCC	NCC Sverige AB
SBP	SBP GMBH
SSO	Single Sign On
TUB	Technische Universitat Berlin

ASHVIN PROJECT

ASHVIN aims at enabling the European construction industry to significantly improve its productivity, while reducing cost and ensuring absolutely safe work conditions, by providing a proposal for a European wide digital twin standard, an open source digital twin platform integrating IoT and image technologies, and a set of tools and demonstrated procedures to apply the platform and the standard proven to guarantee specified productivity, cost, and safety improvements. The envisioned platform will provide a digital representation of the construction product at hand and allow to collect real-time digital data before, during, and after production of the product to continuously monitor changes in the environment and within the production process. Based on the platform, ASHVIN will develop and demonstrate applications that use the digital twin data. These applications will allow it to fully leverage the potential of the IoT based digital twin platform to reach the expected impacts (better scheduling forecast by 20%; better allocation of resources and optimization of equipment usage; reduced number of accidents; reduction of construction projects). The ASHVIN solutions will overcome worker protection and privacy issues that come with the tracking of construction activities, provide means to fuse video data and sensor data, integrate geo-monitoring data, provide multi-physics simulation methods for digital representing the behaviour of a product (not only its shape), provide evidence based engineering methods to design for productivity and safety, provide 4D simulation and visualisation methods of construction processes, and develop a lean planning process supported by real-time data. All innovations will be demonstrated on real-world construction projects across Europe. The ASHVIN consortium combines strong R&I players from 9 EU member states with strong expertise in construction and engineering management, digital twin technology, IoT, and data security / privacy.

TABLE OF CONTENTS

INDEX OF FIGURES

INDEX OF TABLES

1 INTRODUCTION

Privacy and cybersecurity are key concerns for increasingly digitized sectors, with digital twin technology introducing a set of new vulnerabilities and privacy concerns. Cyberattacks are becoming more complex and the range of targeted sectors is expanding, with attacks like ransomware targeting a wide variety of industries for which data plays a key role. Importantly, 95% of such attacks exploit vulnerabilities that depend on human factors. A robust and resilient cybersecurity strategy therefore requires an integrated approach between technical components and user awareness and behaviours.

While privacy and cybersecurity are interrelated, the former also encompasses the rights described in the European Charter of Fundamental Rights, such as protecting personal data and freedom of information. In current contexts, privacy tends to be immediately connected to compliance with the General Data Protection Regulation (GDPR). However, focusing on compliance may imply that broader, more innovative forms of incorporating privacy in sociotechnical solutions are ignored. Thus, ASHVIN implements a comprehensive privacy-by-design approach requires constant interaction with practice and technical partners to foresee privacy-sensitive points and their implications for design, construction, and maintenance.

1.1 SCOPE AND OBJECTIVES

The goal of this deliverable is to identify requirements for security, privacy, and detail how these are implemented within the ASHVIN project. It outlines the requirements that resulted from a set of interviews, meetings, documentation, and sociotechnical analysis. The report then explains the implementation of these requirements on ASHVIN, in the context of an IoT platform, the digital twin platform, as well as on demonstration cases and aspects that go beyond the technical infrastructure. This is in line with the integrated approach to security described above.

This deliverable is targeted at professionals involved in the design, construction, and maintenance of buildings, as well as professionals developing digital twin technologies. Besides detailing work in ASHVIN, this deliverable uses the requirements and experiences from ASHVIN to provide broader recommendations for the industry and for digital twin technology development and deployment. One should note, however, that specific aspects of data flows and storage will not be discussed here, since these are already covered on the ASHVIN data fusion aspects (D3.3) and the data management plan (D9.3). Likewise, a thorough exploration of human factors and privacy aspects will be reported in D6.5, therefore aspects such as a broader ethical reflections and stakeholder (e.g., worker) involvement in the development process fall outside the scope of this deliverable.

1.2 STRUCTURE

The report first describes key concepts and methods that are relevant for requirement identification and implementation, outlining the actual work that occurred within T1.4. It then presents the requirements in a contextualized manner, not only providing the requirements, but also explaining the rationale behind them. Section 4 details the technical implementation of the main aspects that address the requirements, while section 5 looks at implementation from a user awareness perspective, accounting for the social and cultural factors of cybersecurity and

privacy. Finally, section 6 summarizes the main findings of the report and distils them into a set of recommendations that may be used by professionals in the construction industry or in digital twin development.

2 METHODOLOGY

Implementation of cybersecurity and privacy measures on ASHVIN is characterized by an iterative and incremental process that integrates technical and social dimensions of data protection, privacy preservation and preventive cybersecurity.

To this effect, an initial set of requirements were identified in formal interviews between EUR and practice partners NCC, FAS and SBP in June of 2021. This set of requirements was then discussed with technical partners in WP1, namely MFX, DTT and CERTH to assess feasibility of implementation. From September 2021 onwards the discussion was then expanded to other partners that had an interest in these issues, such as TUB and UPC, and stakeholders beyond project partners, namely construction workers, other construction companies and demo site owners, through online and in-person meetings and interviews. This effort of engaging with multiple stakeholders resulted in a comprehensive and multifaceted set of requirements described in section 3 of this deliverable.

2.1 PRACTICE THEORY APPROACH

Work on privacy and cybersecurity in the scope of ASHVIN departs from the assumption that technologies and material resources are indissociable from the humans that operate them and the contexts in which they are operated (Pridmore & Oomen, 2020). Therefore, in conjunction with T6.4, the approach to requirement implementation includes not only considerations on how these are technically deployed in the IoT and Digital Twin platforms, but also focus on the key actors that engage with and are affected by these technologies.

In this scope, the choice to identify requirements through semi-structured interviews instead of other, more formal, procedures, makes sense since it allows the exploration of the needs, contexts and individuals that underlie the requirements. This has been a trend in cybersecurity (Pollini et al., 2022) and privacy (Nissenbaum, 2004) research to mitigate the vulnerabilities generated by a mismatch between technical and procedural aspects and the actual behaviour of stakeholders.

2.2 CONTEXTUAL INTEGRITY

Regulation (EU) 2016/679 General Data Protection Regulation (GDPR) is naturally a strong foundation for requirement definition and implementation of privacy and data protection measures on ASHVIN. However, considering the project's ambitions of going beyond compliance, principles of contextual integrity (Nissenbaum, 2004) will be a key aspect in assessing privacy and security risks and mitigation strategies. According to this framework, contextual integrity is maintained when information is shared consistent with contextual norms, which are described by five parameters: actors (senders, receivers, data subjects), the circumstance (transmission principle) under which the information is shared, and the type (attribute) of information.For a schematic overview of this process, see Figure 1.

Unlike traditional privacy and cybersecurity models, ensuring contextual integrity entails more than just protecting communication between sender and receiver from unwanted and unauthorized access, disruption, or manipulation. It also considers that

different data types have different requirements and that data exchange transmission principles, both formal and informal, are a key component of privacy and cybersecurity. These parameters also manifest themselves in key components of GDPR, but by abstracting them beyond GDPR, ASHVIN is guided by a more holistic and integrated view of privacy and (cyber)security.

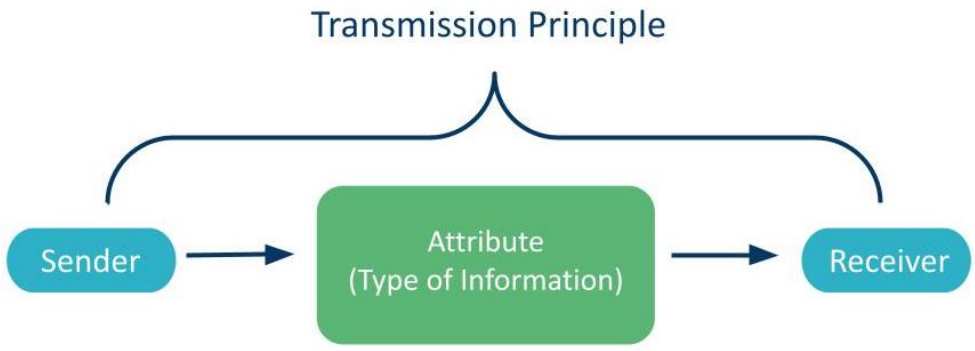

Figure 1: Contextual Integrity model with key components

3 INDUSTRY REQUIREMENTS

Section 3 identifies the key cybersecurity and privacy requirements relevant to ASHVIN whereby a distinction is made between those relevant to workers and non-workers, respectively. Non-workers include site owners, companies, and partners or third parties. This distinction is made to provide a structured overview of the requirements and recommendations as these then serve different interests and needs accordingly. Several aspects relevant in the context of ASHVIN are then named for each group. An overview of the structure of section 3 is provided in Figure 2.

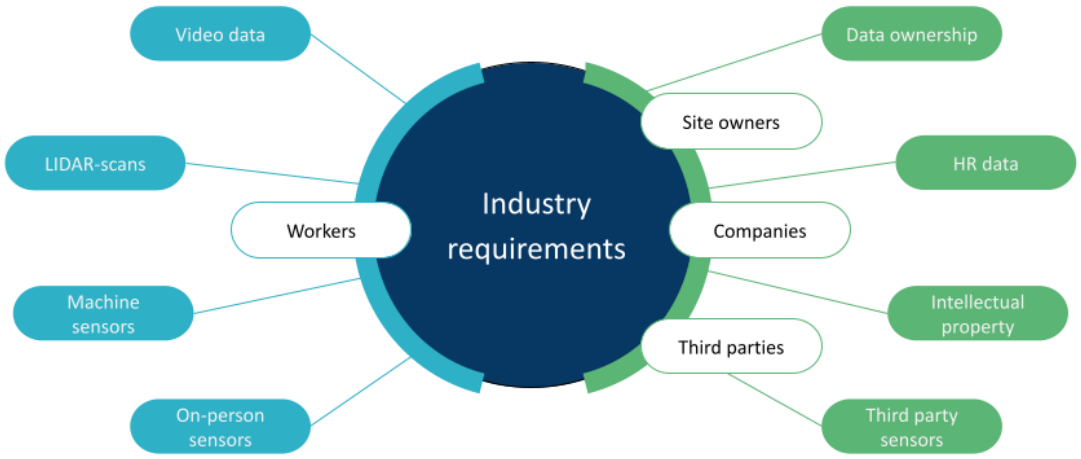

Figure 2: Key Privacy and Security Aspects for ASHVIN

3.1 CONSTRUCTION WORKERS

This section addresses a series of worker privacy issues that arise from tracking and monitoring practices through IoT-enabled technologies, including sensors, cameras, machines, and 3D-scans. When data collection or processing practices involve personal data, the GDPR must be adhered to. However, some data may still reveal sensitive aspects of individuals' identities, even though it is not considered personal data in strict terms. Specifically, measures need to be implemented to ensure that construction workers are not disadvantaged because of unethical monitoring practices. This section summarizes relevant requirements and how these might apply within ASHVIN, and recommendations that extend beyond the GDPR by addressing ethical concerns.

The European legal framework primarily stipulates the establishment of legitimate grounds for data collection and processing, clear purpose specification, and the minimization of data retention. Because of the asymmetrical relationship between employer and employee, the notion that personal data is legally processed based on the data subject's consent does not apply. Workers' consent for an employer to process their personal data is not seen as given freely, since employees financially depend on employers and are subject to the employer's authority (Ball, 2021). For this reason, the legal basis for processing personal data of employees is based on necessity and proportionality, rather than consent. The proportionality principle must

be applied to ensure the use of proportionate technology and operationalization standards to prevent unnecessary personal data collection. Translated to practice, this means that the purpose of personal data collection must serve a legitimate interest of the employer, while minimizing the impact on employees' privacy. This is an important aspect of requirement identification in the context of ASHVIN, because requirements that are unfair to employees cannot be detailed for implementation, even if they formally comply with the legal framework.

Another key principle of the GDPR is that of integrity and confidentiality, which deals specifically with cyber security aspects of personal data. Article 5(1)(f) states that personal data must be:

"…processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

Article 32(1)(a) of the GDPR stipulates that using algorithmic encryption of personal data is an appropriate security technique (European Union, 2016). In addition to industry requirements, international industry standards predicate best practices for information security. The ISO/IEC 27000-series contain recommendations for information risk management. The European Union Agency for Cybersecurity (ENISA) also recommends a set of security good practices specifically for IoT and smart infrastructures (source). Notable technical standards for securing IoT-enabled systems include IEC 62443 (industrial automation and control systems), CEN/CENELEC/JTC 13 (cybersecurity and data protection), and ISO/IEC JTC 1/SC 27 (information security, cybersecurity, and privacy protection).

3.1.1 Video data

On ASHVIN demonstration sites, video footage often is collected through several devices, including CCTV, drones, and machine cameras. For instance, on the Barcelona office building demonstration site, drone test flights were conducted to give an overview of the construction site and its workers. This footage is often used as a tool to prevent and identify illicit trespass on construction sites. Within ASHVIN, the utilisation of CCTV extends beyond monitoring and trespass prevention as it allows data-driven improvements to safety processes and efficiency. This equips construction site owners with the tools to develop measures, procedures, and guidelines that are directly informed by data that was collected on-site. For example, the most used routes of heavy machinery can be determined by analysing video footage of vehicle movements around the construction site. This data can then help to identify and improve inefficiencies or identify dangerous overlaps between machinery and worker movements. When looking at the drone footage collected at the Barcelona demo site, this could also be useful to detect workers wearing or not wearing harnesses and helmets.

The GDPR specifies the legal grounds for video monitoring workers without requiring explicit consent beforehand. It states that there must be legitimate interest and subjects need to be informed. However, CCTV cameras may capture identifiable data about workers at the site, such as individual faces or ID-tags. Because this data

could unintentionally reveal information about individual worker performance, it is key that employee privacy and security are not leveraged during these processes.

This section also addresses the requirements and recommendations for video data captured by drones, as special EU regulations apply.

3.1.1.1 Ethics and data protection

From an ethical perspective, it is key to align purpose specification with the actual usage of data. CCTV allows for image data collection for legitimate purposes, but the data should be stored and treated securely to ensure that any potential risks to the subjects are minimal. To this end, workers should always be informed of the data collection and usage, even when it concerns secondary usage. D10.1 includes a privacy notice that was displayed on ASHVIN demo sites where secondary data is being used. When possible, anonymity should be accounted for, and filmed subjects should be allowed to review and delete footage that contains them on request.

Use of secondary data for research purposes is allowed if due care is taken regarding data storage and purpose specification. If, due to individual or corporate initiative, video data is used beyond the legitimate purposes specified in GDPR, individuals captured by the footage may be subjected to an unfair situation.

The ASHVIN IoT-platform is developed to minimize privacy and security risks that emanate from this. Because data processing of IoT devices occurs at the edge of the network, unprocessed personal data does not enter the cloud environment. Instead, information is presented as a visualisation or dashboard. As a result, the volume of personal data entering the cloud should be minimized, reducing the likelihood that identifiable information from video data is used for purposes other than those specified.

Beyond ASHVIN, CCTV footage in digital twins should keep in mind the goals of enhancing safety, improving efficiency, and reducing costs. Furthermore, these goals should not be achieved at the expense of unfair and invasive worker monitoring. Involving workers or their representatives when developing or implementing digital twin technologies contributes to this goal, and 7 interviews with workers and site managers were conducted in the scope of ASHVIN to ensure these perspectives were incorporated.

The following are recommended technical measures that aid in maintaining proportionality and privacy preservation of employees:

- Blur faces and other forms of identifiable information (e.g. ID tags), preferably on the edge, to reduce identification of workers to external/outside third parties in case of a data breach.
- Generate access logs to raw video/image footage to control unauthorised or abusive access.
- Implement anomaly detection unsupervised machine learning algorithms to detect unauthorised or unusual access to raw video data.
- Implement edge or in-platform opaque data processing so that access to raw data image data is not required. (e.g., if the purpose of image collection is to assess the position of a machine in the construction site, pre-process the video feed so that only the machine position output is accessed).

- Implement automated and/or simplified file/data deletion and archiving processes so that image data that has been processed and is no longer necessary is deleted.

3.1.1.2 Drones

The use of drones is restricted by EU regulations in terms of safety and privacy requirements. As established by regulation (EU) 2019/947, in effect since December 2020, drone flying is subject to a classification strategy in accordance with their operational risks, whereby three main categories are highlighted: open, specific, and certified (EASA, 2021).

The *open* category encompasses lower-risk drone operations where safety is ensured if compliance with the relevant requirements for its intended operation are adhered to. In this case, given that the operationalization risks are considered low, no operational authorization is needed prior to the use of the drone. The *specific* category refers to drone operations which are considered riskier, entailing that an operational authorization is required which must be issued by the national competent authority prior to the utilization of the equipment. Lastly, the *certified* category includes high-risk drones where it is required for the drone operator, the drone itself, and remote pilots, to attain adequate certification and licensing.

Prior to the utilization of drones, compliance with EU regulations begins with a registration of the equipment within the country where it will be operated and where the business is found. To efficiently register and to acquire further details on the type of regulations that apply to the equipment, please refer to drone department of the National Aviation Authorities (EASA, 2022) website, in which an overview of specific national regulations within the EU territory can be acquired. It is important to note that the utilization of drones is forbidden in certain areas, and therefore appropriate consideration should be drawn to country-specific regulations.

Drone footage was collected on ASHVIN in the scope of demo sites 1 (railway bridges in Spain), 3 (Zadar Airport) and 6 (office buildings in Barcelona). Some privacy risks may arise during the processing of drone-collected sound, imagery and geolocational data relating to identified or identifiable individuals. Importantly, these are addressed if the raw data is securely and thoroughly encrypted via algorithmic applications on edge-computing components because the data is then anonymized before it enters the platform environment. The raw data should be deleted directly after processing. When AI-enabled tools allow for automated anonymization of identifiable information, drone-collected video data within ASHVIN falls outside of the GDPR.

In cases where technical measures cannot prevent the collection of identifiable information, several requirements apply. Both construction workers and potential bystanders may become data subjects and their respective rights must be respected.

Additional recommendations are incorporated in Article 29 Working Party (WP29) and encompass the adoption of *privacy by default* and *privacy by design*, ensuring that privacy preservation mechanisms are engrained in the drone's operating capacities (Data Protection Working Party, 2015). Moreover, the DPIA is considered a valuable tool in this context, as it enables an evaluation of the impact of the implementation of drone technologies on the right to data protection and privacy.

The following technical recommendations apply to drone usage:

- Implement data deletion procedures after drone footage is processed;
- Devise minimally intrusive flight plans for drones, not only in terms of avoiding bystanders and private spaces, but also protecting construction site worker from monitoring.

3.1.2 Machine sensor data

Sensors in machinery and equipment collect real-time data to gain insights in numerous aspects of the construction or maintenance process. For example, they may measure temperature, moisture levels, of fuel usage of machinery. Although these sensors do not collect data about individual workers directly, data analysis may reveal aspects of worker activity including performance-related information.

Important categories of sensor data are accelerometers and GPS-systems, which collect geodata and movement speed of machinery. Because machines and equipment are operated by construction workers, their movements across construction sites and how quickly they complete their work are also tracked indirectly. Thereby, the performance of individual workers can be extrapolated from the collected sensor data. This raises ethical concerns on worker surveillance.

For this reason, it is recommended to carefully consider how sensor data collection can best be protected, while still enabling parties to make data-informed decisions to improve construction safety and efficiency.

3.1.2.1 Ethics and data protection

Article 6 of the GDPR states “processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party” and that “the existence of appropriate safeguards, which may include encryption or pseudonymisation” should be considered. The requirements associated with the GDPR only apply to instances where personal data is collected. Examples of sensor data are measurements of carbon dioxide, sound, heat, or light intensity; in many cases, these datasets would not be considered personal data and data protection regulations would not apply. However, what data is regarded as personal data is not always as straightforward and should be seen in its context. As noted above, the multitude of sensors can together give insight in individual worker performance, especially when sensorics are combined with other available datasets.

An important exception is the geofenced GPS-tag worn by construction workers. These tags collect geospatial data and are activated when workers enter specific, predetermined areas. In some cases, geodata is combined with information generated by accelerometers. Because location can be an identifier, this is considered personal data. Consequentially, the GDPR states several requirements that must be followed.

First, the purpose of personal data collection must be specified and recorded. The legal ground for processing this kind of data is specified in Article 6 of the GDPR, which allows processing for the purposes of legitimate interests. In this case, these interests are efficiency and safety; for example, ASHVIN D4.6 explores this by implementing a safety tool. Efficiency is valuable for construction site owners, while the interest to improve construction safety is in the interest of both owners and construction workers. Importantly, this data must not be used for other purposes than

those provided. Personal data must not be retained longer than necessary to achieve the provided purposes. Additionally, construction workers must be informed about the purpose of geospatial data collection and processing.

In the toolset created for ASHVIN, measures are already implemented to minimize the risk of data traceable to individual workers. The data that sensors collect is sent to the cloud environment of the platform. It is used to generate insights shown on the platform dashboard, which provides information through interactive visualisations of aggregated data. The raw data is stored to be algorithmically processed. During the processing, automated software creates generalizations, aggregations, and models from the data. This is information is then shown to users on the platform dashboard. After processing, all raw data with potentially identifiable information is deleted from the servers. This means that platform users cannot access raw datasets that contain measures of individual sensors, workers, and operators.

In cases where performance of individual workers can be extrapolated, extra measures should be taken to protect abuse of inferred data about their performance. This may for instance occur in situations where only few workers are licensed to operate special heavy machinery. For this reason, it is recommended that different data aggregation levels are implemented for human versus non-human operated machinery. This would allow the organization of information in distinct piles depending on their function, while avoiding the linking of datapoints concerning performance to specific individuals.

The analytical outputs included in reports should not contain details of specific events or individual workers but generalized conclusions and overall findings that can inform decisions to increase efficiency. To this end, data should be aggregated and anonymized whenever possible. In cases where personal data is collected and full anonymization is not possible, a second general recommendation is to allow workers to access and review their personal data.

The GDPR also stipulates appropriate safeguards should be considered. These are recommended:

- Implement easy-to-use data aggregation procedures, either in the platform or as an edge computing component;
- Implement automated measures to anonymise the data collected where subjects are present (e.g., where a human is operating a construction equipment).

3.1.3 LIDAR scans

LIDAR cameras use lasers to generate a detailed 3D scan of a construction site, based on a point-cloud map. This technology can be used to create high-definition geospatial data and can be used to inform decision-making during construction design, planning, or building. Point cloud data may also be combined with other sensor data to generate advanced insights, such as moisture levels.

3D-mapping can be generated by using standalone scanning devices, but LIDAR-cameras can also be built into smartphones or other hand-held devices. While capturing faces or bodies is not the main purpose of this data collection, it could still happen incidentally. Since a 3D scan of a person's face is highly personal data and

can be used for biometric identification, it may be subjected to higher processing requirements.

3.1.3.1 Ethics and data protection

From an ethics point of view, it should be assured that LIDAR data that potentially includes human subjects is only collected when needed, and that appropriate steps are taken to avoid collection of facial data whenever possible.

This point cloud-data should be subject to high protection and access controls, not only for potentially including biometric data, but also because it holds detailed representations of buildings that may present privacy and intellectual property risks if shared. As the speed of 3D-data capturing sensors increases, the data volumes increase rapidly. For this reason, it is important to delineate a clear strategy on how long-term storage and future access to point cloud-data are secured.

Whenever possible, only collect LIDAR data when no humans are present in the room. If the collection of personal data in the form of facial features cannot be avoided, it is recommended to implement automated methods for facial feature removal from point cloud-data. Using facial recognition, a suitable AI/ML application consistently identifies and then obfuscates human faces of entire datasets.

Usage of lidar scans should account for the following technical recommendations:

- Implement automated methods, preferably on edge, to detect and remove human features from pointcloud data;
- To ensure transparency, implement methods to grant access to pointcloud data of spaces to all stakeholders who are directly invested in the space (e.g. workers, residents) upon request.

3.1.4 On-person sensors

This subcategory pertains to a range of internet-connected sensors that can be worn by workers, including hardhat cameras, heartrate monitors, and mixed vision glasses. These wearable devices can be built into the fabric of employee attire, such as jackets or shoes, or integrated with accessories, including watches, helmets, or badges. They are key tools for improving the occupational safety of construction work through real-time data gathering.

It is critical to determine whether individuals can be (accidentally) identified from the sensor data collected because this would classify the information as personal data. Within the scope of ASHVIN, some sensor data is analysed and encrypted locally through edge-based computing before it is sent to the platform environment. A previous study on construction workers' attitudes towards IoT-based safety monitoring devices shows that employees have most privacy and security concerns about wearable sensors in the work environment (Häikiö et al., 2020).

3.1.4.1 Ethics and data protection

Heartrate data may be considered health data, and therefore subjected to special rules under GDPR. Because there is health data involved, site owners should ensure special provisions for workers, so they are able to access the collected data. Workers should be informed about how their personal data is used, for what purpose it is being collected, and for how long the data is being retained. They should be informed

about their right to have their personal data removed if they so wish, and such wishes should be granted.

Heartrate data, classified as health data, should under the strictest protection and individual data should only be accessible to the individuals themselves.

Extra attention should be paid to the language used in the privacy notice that is presented to employees. To ensure people of all educational levels and cultural backgrounds can read and understand the privacy policy, clear language should be used, sentence length limited, and jargon should be avoided. A suitable alternative for areas where low literacy rates may apply is to present key privacy policy information in a video that employees can watch in the workplace.

The purpose of saving lives and ensuring the safety of workers may justify the collection of this highly intrusive data. However, very careful treatment of the data should be provisioned to ensure that potential risks do not outweigh the benefits for data collection subjects.

“Not-wearing” may also reveal aspects of worker activity. For example, sensor/wearable may be turned off when worker takes breaks. This can be addressed by adding a degree of noise and/or uncertainty to the collected data. This process relies on the transformation of the numerical attributes within the data to the extent that it cannot be linked to any natural individuals, therefore granting a reliable degree of confidentiality (Mivule, 2013).

If wearable sensors or other forms of invasive data collection are implemented, there should be special care put into informing those involved, gathering consent, and allowing transparent access to the data and its uses by the subjects of data collection. Purpose specification for this type of data must be ensured and adhered to, using it for no other purpose than to increase worker safety.

The following additional technical measures are recommended:

- Similarly to machine sensor data, implement easy-to-use data aggregation and anonymization procedures, either in the platform or as an edge computing component.
- Any wearable should have key privacy controls embedded in its hardware components. In doing so, workers are given more control in data collection activities through on-body sensors.
- It is also advised that sensors have visible indicators, such as a blinking light, that show the device is activated. This is best done in such a way that only the wearer can read this indicator.

3.2 NON-WORKERS

The IoT-enabled platform requires the integration of datasets from multiple different sources. Combining these datasets gives rise to several issues in terms of access authorisation for datasets containing company-sensitive or confidential information.

Specifically relevant is the risk posed by access to raw data, given that third parties could make inferences about proprietary techniques, models, processes, or materials. These assets need appropriate protection considering that stakeholders may otherwise have concerns about losing their competitive advantage. This section establishes guidelines for protecting the interests of site owners and third parties in

terms of data protection and security, going over legal requirements as well as best practices.

3.2.1 Data ownership

Given that the construction process tends to involve multiple stakeholder with different backgrounds and interests, parties may fear that a digital twin platform highlights flaws and liabilities in their procedures and practices, or exposes intellectual property assets to others. Research-generated insights that may go against the direct interests of stakeholder(s) need to be addressed accordingly. For this reason, it is recommended to regulate access and to minimise the retention period. In the scope of ASHVIN, formal agreements were signed between the demo site owners or companies and researchers to ensure that data was protected from misuse.

The purpose of data collection and processing should be delineated clearly in the platform structure and metadata. This is in line with the GDPR, which places a strong emphasis on purpose specification. In principle, contractually agreed purposes for data collection and processing are binding and serve as a legal ground to determine liability. In other words, data owners should be protected by the fact that other parties with access to the digital twin platform cannot use collected data for purposes other than the ones specified. An exception may hold for extreme cases when a flaw that directly puts human lives in danger is exposed by the data, in which case it would be required to notify site owners and/or report to the relevant authorities. This kind of circumstance is, however, very unlikely.

Further protection is provided by establishing access logs which store the access history of all users who access information on the platform that is deemed more sensitive. This allows security monitoring, assisting incident responders and developers in quickly spotting malicious activity. Important to note is that access logs should only be accessed by admins, considering they contain information linked to IP addresses which may allow the identification of individuals.

Regarding data ownership, the following technical recommendations should be implemented:

- Clearly and transparently define access levels that distinguish between access to data and ownership of data;
- Create secure access logs to control access and protect against cyberattacks;
- Minimize automatically defined retention periods to prevent unwanted use of data.

3.2.2 Intellectual property, HR, and extra sensitive data

Operations in the construction industry may mean that particularly sensitive data may be integrated within complex environments. This includes, but is not limited to, accounting records, budgeting information, HR data, and intellectual property. While ASHVIN does not directly handle most of these data types, the possibility of reverse engineering processes that are protected as intellection property should still be considered. This kind of data require compliance to high levels of technical and legal protection. In general, it is key to clearly specify the purpose for data collection and processing practices.

If personal data is involved, such as employee records, the GDPR applies. If this kind of data is to be integrated in the platform, not only a high level of transparency and information are required, but access should also be very well controlled with restrictions. For instance, accessing HR data should be restricted to HR staff and admins.

Integration of highly sensitive or personal data in the platform should only be done if: there is a clear benefit in doing so; there are guarantees that the data can be protected from undue access and is only used for the purpose specified in its collection.

HR, financial and IP data were identified by practice partners on ASHVIN as the most critical pieces of information to be safeguarded in case of a data breach. Therefore, they should benefit from additional degrees of protection. Any tool development or integration should be carefully considered if HR, financial, or IP data are involved, for example by means of a cost analysis. Additional layers of protection should be created for sensitive data that do not only rely on access permission (e.g., specific passwords and authentication methods for sensitive data).

Technical recommendations regarding sensitive data categories include:

- Configuring additional layers of protection for sensitive data types;
- Implement anomaly detection for access to sensitive data;
- Deidentifying databases of financial, HR and other sensitive information, securely storing the keys that ties persons and organizations to data records.

3.2.3 Third-party platform sensors

ASHVIN or other digital twin technology may integrate sensors in construction sites that involve third party platforms. While some data may not seem particularly sensitive on itself, it may reveal more when cross-referenced with other datasets. Therefore, considerable security measures should be implemented because protected intellectual property, including proprietary procedures and methods, could be inferred from detailed sensor data.

When introducing a sensor on a construction site that sends data to a third-party platform, it should be ensured that the platform itself complies with GDPR requirements. In particular, the terms of service should be scrutinized for data sharing policies, and data storage should take place in EU servers.

If digital twin implementation introduces potential data leak risks or cybersecurity vulnerabilities in a construction site, these measures should be executed:

- Ensure that there are no feasible alternatives that would eliminate the need for data sharing
- Data sharing and security policies of any third parties involved should be scrutinized.
- Implement secure message encryption and transfer protocols for data transfers between third-party platforms and ASHVIN IoT.

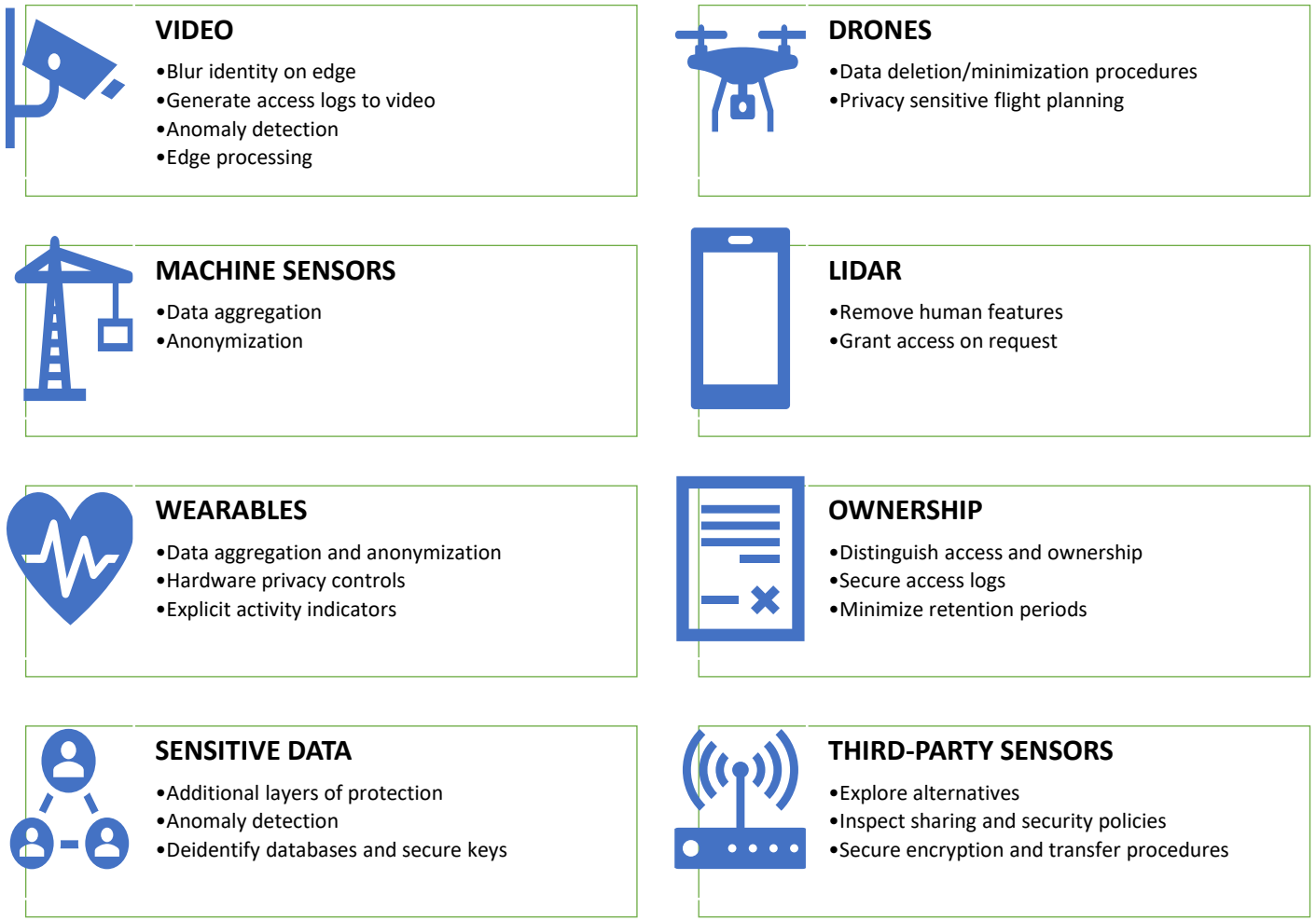

Figure 3: Technical privacy and security recommendations

4 TECHNICAL IMPLEMENTATION

This section details the ASHVIN implementation of some technical solutions that contribute to address the requirements identified in section 3.

4.1 SINGLE SIGN ON

ASHVIN implements Single Sign-on (SSO) as a key authentication method. This is a method that belongs to Identity and Access Management (IAM), facilitating the management of electronic or digital identities and network access rights for individuals, hardware and applications. Its most important components are user management services, directory services, and authentication and authorization services. ASHVIN opted for SSO with two-factor authentication because current best practices for cybersecurity advise against forcing users to create and remember multiple passwords, since this will often result in a simplification of these passwords which introduced vulnerability. Two-factor authentication also protects the ASHVIN platform from vulnerabilities emerging from careless handling of passwords online (phishing attacks) and offline (writing the password on paper).

SSO enables users to use one set of login credentials (e.g., a username and password) to access multiple applications and websites. When a user logs in to the IoT platform, for instance, they are automatically authenticated to other ASHVIN tools and services. In the IoT segment of the ASHVIN platform, a SSO service is implemented using a Keycloak solution with theOAuth 2.0 framework and the OpenID Connect authentication protocol SAML.

Keycloak is a SSO solution for web apps and RESTful web services. It was chosen for ASHVIN because it is tailorable to individual requirements and customizable user interfaces for login, registration, administration, and account management. Applications are configured to point to and be secured by this server. As a critical aspect for ASHVIN's cybersecurity and transparency, Keycloak uses open protocol standards like OpenID Connect or SAML 2.0.

OAuth allows accounts created under ASHVIN to be used by third-party services without exposing user credentials. OpenID Connect adds an additional authentication layer to further ensure security..

The OpenID Connect protocol manages authentication with JSON Web Token standards. These standards define an identity token in JSON format and enable methods to digitally sign and encrypt data in a compact, web-friendly way.

The login flow for the ASHVIN platform includes both password authentication and an app-based device SSO authentication using Keycloak for robust access control.

4.2 ENCRYPTION

To accommodate the data volumes generated by the ASHVIN project, the IoT infrastructure was migrated to AWS during the second year of the project. In order to protect data, databases make use of the industry standard Amazon RDS with Amazon EBS encryption relying on AWS KMS for key management.

AWS EKS cluster is made with encryption enabled for the cluster's encryption. Once configured, the encryption provider automatically encrypts a created Kubernetes secret with a Kubernetes-generated data encryption key, which is then encrypted

with the provided KMS master key. Kubernetes secrets enables storing and managing sensitive information, such as passwords, docker registry credentials, and TLS keys using the Kubernetes API. Kubernetes stores all secret object data within etcd.

Amazon EKS encrypts all etcd volumes at the disk level with AWS-managed encryption keys. Using encrypted storage class and S3 storage, where application backups are kept, application services employ volumes that are likewise encrypted.

By default, the TLS protocol only uses X.509 certificates to verify the identity of the server to the client; the application layer is in charge of authenticating the client to the server. Using client-side X.509 authentication, TLS also provides client-to-server authentication. It is rarely used in end-user applications since it necessitates provisioning of the certificates to the clients and has a less streamlined user interface. In business-to-business (B2B) applications, where a small number of programmatic and homogeneous clients are connecting to specific web services, the operational burden is minimal, and security requirements are typically much higher than in consumer environments, mutual TLS authentication (mTLS) is more frequently used.

Implementation of data encryption in ASHVIN is aimed at preventing common forms of digital attacks. Mutual authentication prevents man-in-the-middle attacks, ensuring that no parties are intruding between the sender and the receiver. This also prevents replay attacks, since mutual authentication verifies timestamps and terminates sessions if a time delay is exceeded. Robust SSO and authentication methods prevent identity attacks such as spoofing attacks and impersonation attacks. Mutual authentication ensures that parties involved are legitimate. To manage device certificates, ASHVIN uses the Hashicorp Vault service in conjunction with an in-house certificates service that integrates Vault with device data. is also trustworthy.

4.3 MACHINE LEARNING

A challenge for visual data obtained from different sources in construction environments is data privacy, ownership, and how the data can be used, as this framework remains unclear. It is evident that cameras may unintentionally capture their identifiable data, even for tasks where the goal of visual data collection is not to monitor workers. This may result in workers feeling under surveillance, increasing their stress levels, and reducing acceptance of such technologies in their working environment.

In ASHVIN T3.1, the goal is to run computer-vision algorithms to provide a higher level of understanding from the collected visual data (images and/or videos). As described in D3.1, there are three main tasks involved in ASHVIN work performed by CERTH, none of which is per se aimed at detecting people or their activities. Nevertheless, there is always the possibility of capturing identifiable human data during the data collection process, especially since this data collection comes from automatic or semi-automatic procedures performed by the managers of the demonstration sites and end-users.

When data processing for people-detection algorithm are involved, the methods developed by CERTH ensure that the training of the specific classes is performed using publicly available datasets, in a way that no reference is made in identifying

specific individuals in compliance with the ethics regulations. Thus, the deployed services are not to perform any face recognition aim, so no personal identifiers are collected or processed. Another important point during the training is to perform nonbinary classification to distinguish between men/women or categorize humans based on skin colour or appearance. Furthermore, for the evaluation and demonstration scenarios, footages are acquired from distant perception locations. Therefore, the possibility of capturing a personal identifier is significantly decreased. Additionally, for human detections CERTH's practices and consultation guidelines mandate an in-build blurring mechanism to hide personal information if it appears and to further comply with the GDPR.

As mentioned above, CERTH is leading T3.1, which relates to three different subtasks that are processing visual data from construction sites.

The first task aims for the deployment of the **3DRI** method. As quoted in D7.1: "This method will introduce a pipeline for estimating 3D structures from 2D imagery. The depth information is calculated from 2D data using common information that is present in overlapping parts between different images or videos". The capturing of human-identifiable data during this process is not only unnecessary, also it often deteriorates the final output since the 3D representation aims at the extraction of the point clouds for the building structures. The strategy followed in the deployment of the method for removing and not recording the human objects in the results is a segmentation technique, based on DeepLabV3 network to remove unwanted elements from the collected datasets, if existing.

Figure 4: Masking results of the DeepLabV3 CNN algorithm.

The output masks can serve various purposes. First, they can be used to speed up the reconstruction since they limit the number of features detected for solving the 3D representation problem. Secondly, they can be used to enhance the sparse and dense reconstruction by filtering outliers in the point clouds. This in turn results in significantly better dense point clouds with less noise. Finally, and most importantly in the context of this deliverable, the masking of people offer an extra level of security of people private info that may be present in the construction sites operating their daily tasks.

The second task deployed within the framework of T3.1 is the defect detection over runaways, which refers to the **DDCV** method. As noted in D7.1 (ASHVIN technology demonstration plan): "The AI-powered solution is used to detect damages, anomalies and objects on the runway surface and green areas around the runway. The aim is to integrate the automated damage detection into inspection and maintenance planning

process". The deployed service processes the visual input, acquired via UAV camera, and produces an annotated mask where the detected defects are segmented accordingly. Again, the intention of the module is not to process content with identifiable data from people. In addition, the data collection process is controlled by qualified personnel and occurs when there is no human presence on the runway. Data is collected remotely with the drone camera set on "top-view" in a restricted area by the authorities, as the facility is located approximately on a NATO base. The images below show some examples of the data collected.

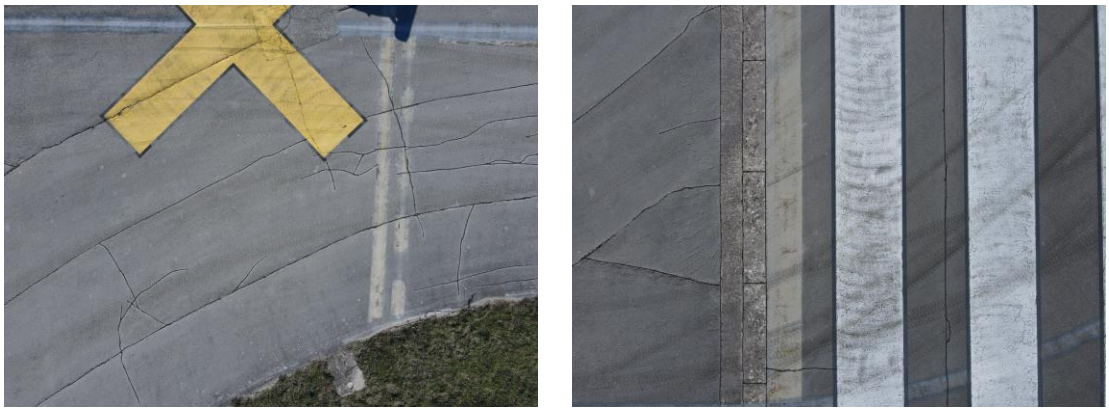

Figure 5: Data via UAV camera of Zadar airport

The third task related to computer vision and implemented under T3.1 concerns the monitoring of construction activities. An object detection algorithm was implemented to detect the installation of piles for ASHVIN demonstration project #4 (logistics hall construction in Germany). The service processes time lapse images to detect the duration of installation activities during the construction phase. This service runs as a black box and does not extract information about human subjects in the scene. The output of the module, which is the duration of activities, is forwarded to the DES tool, the use of which is to calculate the productivity rates of construction activities.

Finally, a tool was developed by EUR and TUB within T1.5 to verify that the personal protective equipment (PPE) is worn correctly by the workers (protective helmets and vests). CERTH's role in this activity was to consult and supervise the activity to ensure, based on experience, that good practices were being followed. Implementing such monitoring mechanisms involving human agents, entails many challenges associated with accuracy, timeliness, and transparency (Seo et al., 2015). The recommendations for the tool implementation where to set the service on edge, processing the raw data on a JETSON device. Object detection services should process video streams or images on edge and not store any information in a local database. Each time a detection is made, a JSON file is created and forwarded to a higher-level tool without any reference for identifying specific individuals, always in compliance with ethics regulations and the recommendations of section 3.

4.4 DASHBOARD AND VISUALISATIONS

The game engine-based Digital Twin platform (ASHVIN) is developed to enable connectivity, device management, and data acquisition. ASHVIN's digital twin platform facilitates version control of BIM for users and teams, or else they would share large files via email or file sharing services. The DT platform enables collaboration so that all project stakeholders have access to the latest version of the models and upload their own modifications.

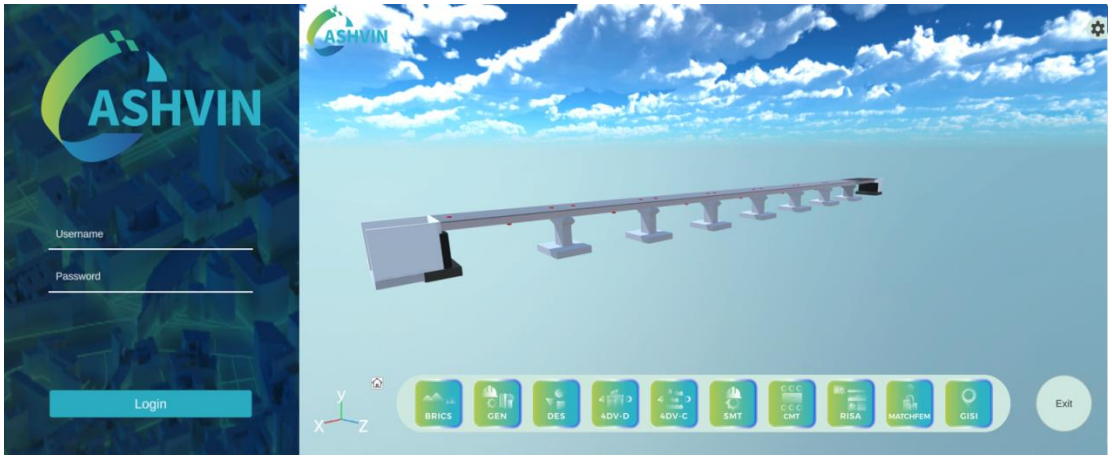

Figure 6: ASHIVN DT platform

Secure Password: The password is not stored in plain text but only as a salted hash. That is in a form that makes it practically impossible for anyone to steal the password even with access to our database.

Security: The DT platform can be deployed and maintained as an instance of the platform in several locations as required by the client. The DT platform aims to be deployed on AWS to provide the cloud platform and to configure instances of the application to operate inside the AWS region, aligning with the data residency requirements of the clients. This ensures the ASHVIN DT platform reaps from both encryption and high levels of physical security for protecting client data.

Encryption: To ensure a highly secured service, the platform implements encryption at all layers of our product design. Initially, before logging in, the initial connection to the services is secured via 2048 Bit Extended Validation Certificates. This essentially confirms the user is accessing the DT platform service before entering the credentials. After logging in, all communication on the platform occurs over HTTPS secured connections with the same levels of protection as internet banking. Once data is stored on the platform, it is encrypted again with the purpose that 'data at rest' is encrypted with keys that only the DTT personnel have access to.

Data storage retention: All data that is collected will be stored only as long as is necessary to accomplish the purpose for which it is collected, or as long as is permitted or required by applicable law. Periodically, DTT will review its data processing systems to determine whether the purposes for the collection and processing of your data remain valid.

Third-party: Not only does DTT avoid sharing user Private Information with third parties, it also inserted careful measures to limit our own access to it. However, the

DT platform still utilizes several third-party software products and data processors when analysing platform data. For the sake of transparency, these are outlined below.

Table 1: Third party software

Software	Use
Revit	3D modelling
Grasshopper	FEM simulation & point cloud
Dynamo	Parametric modelling
Unity3D	Platform development

4.4.1 Visualization

Visualization has a vital role in all aspects of privacy within the data ecosystem, both for the data owners and data consumers. Some of the privacy-preserving data visualizations techniques are as follows:

Hide Data: The technique includes both spatial and non-spatial data. An obfuscation technique for volumetric data transformation obfuscates volume data and delegates rendering volume data to a remote server, thus preserving privacy. For temporal data, visualization is often used to encode the outcomes of an anonymization method (e.g., k-anonymity, l-diversity-closeness, differential privacy), thus leveraging clustering in the data space for visualizing event sequences. With non-spatial data, visual uncertainty is added to a conventional technique like scatter plot or parallel coordinates as an additional defence mechanism (Bhattacharjee et al., 2020).

Evaluate Risk: Privacy-preserving data sharing risks can be mitigated in a non-intrusive scenario by restricting the queries that can be used for exploring the data. Similarly, it can be applied for visualizations, wherein the different visualizations are assessed based on risk factors before making them publicly accessible. Data owners would therefore need to identify risks thoroughly before the release of data. Adaptive Graphical Visualization Interface (AGVI) as an interface is user-adaptive. Because it changes according to the user's needs, it provides an interface considering multiple roles from both a data subject and a data consumer's perspective (Muchagata et al., 2019).

Ensure Data Governance: These parameters and policies can then be combined with user-specific data governance policies to ensure the highest possible level of privacy and the lowest level of risk. To make sure these policies are implemented appropriately, a strong data management strategy needs to be put in place. This will dictate who is responsible for data at different parts of its lifecycle, like design and planning engineers, site managers, project managers, and facility managers.

5 USER AWARENESS

Efficient privacy preservation is heavily reliant on user awareness. Although the technical aspects of information security are often emphasized strongly, most cases concerning a vulnerability of a company's security involve human ignorance and a lack of awareness (Furnell and Clarke, 2012; Safa et al., 2015). It is estimated that 95% of cybersecurity breaches can be traced back to human flaws (The Global Risks Report, 2022). Therefore, the close link between individual **information security behaviour** (ISB) and technological control within a company cannot be ignored. ISB is the combination of security activities conducted by end-users to ensure the security of information as established by information security policies (Padayachee, 2012).

The construction industry has been subject to various high-profile cybersecurity breaches in recent years, as construction businesses represent tempting targets for malicious attacks because of the handling of sensitive information and high-value economic exchanges (National Cybersecurity Center, 2022). In the course of the requirement identification stage, ASHVIN partners also disclosed their own experiences with cyberattacks.

The involvement of stakeholders and the storing of valuable data concerning financial transactions and latest construction developments contribute to the perception of construction businesses as easy and attractive targets for cyber-attacks. For instance, the extensive use of suppliers and sub-contractors engaging in vast amounts of high value payments causes these to become tempting targets for phishing attacks, whereby individuals receive a targeted email with a link while attempting to trick the business into conducting a payment into a criminal's account. However, financial loss is not the only risk involved in these types of security threats targeting individual end-users, as data breaches and ransomware attacks can additionally result in the stealing of information or the temporary shutdown of a business, causing significant reputational loss with partners and customers.

While ASHVIN does not directly focus on financial transaction, digital twin data is still vulnerable to attacks such as ransomware. The risk of successful cyber-attacks is significant for the construction industry given that information security relies on the collaboration of numerous stakeholders within decentralized networks, offering many access points for attackers. If individuals are not trained on cyber-security risks, this allows for network vulnerability.

A series of interviews were conducted in the context of ASHVIN with the aim of inquiring managers and workers about their individual security habits. Results from this research suggested that although workers manifested a degree of awareness about personal security, this knowledge failed to translate into practice as they did not act on it. Following the inputs given through the interviewees' responses, this general failure to adhere to one's knowledge of cybersecurity is attributable to a lack of interest, as most respondents expressed a lack of concern.

Thus, it is critical to adopt a holistic approach to information security management, which emphasizes and communicates to stakeholders the importance of acquiring and enacting competent ISB. Due to the multi-layered characteristic of the maintenance of an efficient ISB within a company, such an approach considers

organizational, technological, and social components as relevant. A maximation of end-user's information security behaviour is a valuable way to address the threats posed by a lack of user awareness.

Attention to these matters is particularly relevant when considering the potentially prominent risks posed by a digital twin technology, given that access to the model can result in an acquisition of critical insights into the system and the assets that it replicates. Moreover, access by an external and prohibited party to the digital twin can additionally pose severe threats to the integrity and safety of the model, as control of physical assets can be gained. Therefore, access should be duly restricted to authorised end-users, while also ensuring that these stakeholders maximize their ISB.

In this section, end-users are the various stakeholders within construction companies, including construction workers, site owners, researchers, and contractors, who are involved with the development of a construction project. In other words, it refers to anyone directly involved with, or with access to, the technological affordances of the company.

Moreover, improvement of ISB is an approach which contemplates knowledge on the user-end as crucial towards the maintenance of information security standards. As such, this section addresses the predominant risks involved on the user-end, and consequently how information security awareness and behaviour can be maximized.

5.1 Social Engineering

Social engineering entails manipulation tactics with the aim of acquiring confidential information from individuals. According to recent data, social engineering methods constitute 93% of successful data breaches (Webroot, n.d.). There are various forms of information which can be acquired through these strategies, ranging from passwords to further details to gain access to one's computer. Adequate information security behaviour of end users is aimed at counteracting this, amongst other threats.

Exposure to direct social engineering threats is often materialized in two ways, namely through a link or a download request. Moreover, in the context of ASHVIN these pervasive threats have been noticeable, as all interviewees which were part of the research project reported the reception of a spam email on their personal laptops. These types of instruments can lead to the effective installation of malware or malicious software, potentially allowing access to one's personal accounts. Although ASHVIN deploys 2-factor authentication, which constitutes an efficient anti-phishing tool, the effectiveness of these methods is compromised if not accompanied by adequate user awareness and behaviour.

Social engineering strategies often adopt the form of an impersonation of a trusted source, by creating a logical scenario through which a trusted individual is requesting this information. This subset of social engineering is known as a Phishing Attack and is conducted through various communication mediums, such as emails or social media. Alternative strategies additionally encompass false requests to "verify" one's information, or the providing of personal data because you are the "winner" of a prize, amongst other crafted scenarios.

The best ways of ensuring avoidance of becoming a victim to social engineering tactics is through the securing of one's devices, as well as the cultivation of ISB

amongst end-users. The former can be addressed by installing reliable anti-phishing and anti-virus software, firewalls, and communication filters. Measures to promote ISB in users will be discussed in the following sections.

5.2 Enhancement of User Awareness

5.2.1 Present Knowledge Assessment and Self-Efficacy

Prior to the implementation of tools to increase user awareness of information security in the workplace, it can be beneficial to first assess the present knowledge amongst end-users. This can be achieved through the distribution of a survey aimed at estimating employees' awareness on various focus areas of cybersecurity in the workplace. This survey can be distributed to present workers, as well as newly joining employees.

A similar knowledge assessment process has been executed in the context of stakeholders in ASHVIN through the previously mentioned interviews. Particularly, knowledge areas concerning password safety and digital communication management were explored, with the findings suggesting that further training would be beneficial. To this effect, ASHVIN produced an easy to interpret infographic (Appendix 1) highlighting key aspects of cybersecurity and privacy practices.

Given that the distribution of a survey can be more logistically and economically efficient, this method is proposed as a valuable alternative to assess ISB knowledge at a larger scale. The development of such a survey has been previously conducted by Parsons et al. (2017), resulting in an instrument which aims to examine user behaviours on numerous dimensions of cybersecurity, namely: information handling, reporting of incidents, use of mobile devices, use of e-mail, internet and social media, and management of passwords. This form of assessment can provide an overview of the security behaviours amongst employees, in turn aiding in the identification of knowledge areas which require further strengthening. The collection of this data can additionally be valuable to determine which end-users require training in specific areas.

Evaluating the present stance on information security matters is particularly relevant given the influence of **self-efficacy** on security preserving behaviours. Self-efficacy is a person's belief in their abilities to conduct a task, and their motivations and actions towards such tasks. Previous research findings effectively demonstrate a positive relationship between individuals' self-efficacy in information security and their information security behaviours (Kör & Metin, 2021). The level of self-efficacy among employees can be evaluated using a survey.

5.2.2 Information Security Policy

Awareness of – and adherence to – cybersecurity guidelines is determined by its information security policy, which describes the responsibilities and roles of employees to secure the technology resources and information of an organization (Bulgurcu et al., 2010).

This policy is also aimed at providing clearly delineated instructions to individuals on what should be done in specific circumstances while providing fundamental knowledge on how they should interact with the various technology and information resources of the company.

Clarity and simplicity are key factors when developing such a policy, to ensure its understandability. Moreover, an exhaustive and intelligible information security policy within a company should be complemented with rigorous cybersecurity literacy efforts aimed at increasing workers' knowledge and self-efficacy.

5.2.3 Knowledge Sharing

Knowledge sharing processes rely on an individual's imparting of their expertise, understanding or insights to another individual. This is aimed at an efficient acquisition of knowledge by the recipient, so that this new knowledge is employed to perform their task in a better way. Knowledge sharing can be manifested in two different ways, namely formal and informal.

Formal knowledge sharing involves education, such as policy communication or training, while the informal counterpart refers to advisory services and informal consulting. Addressing both forms of knowledge sharing within a company is beneficial because they are mutually reinforcing.

These efforts can be materialized through the arrangement of a board of cybersecurity experts within an organization, which will provide information security awareness training programs. These training programs consist in the transmission of fundamental cybersecurity knowledge to employees, in addition to policy communication. The board of cybersecurity experts would also be available for consultations regarding information security concerns. Every time a cybersecurity update is done, or new machinery and technology are being used, updated information security awareness training programs should be imparted.

Additional efforts to cultivate knowledge sharing within a company can consist of encouraging the use of privacy preserving social media systems to communicate between workers. This ensures not only that professional communication is done through secure means, but additionally encourages workers to share questions and knowledge regarding information security matters within the company. Within ASHVIN, knowledge sharing occurs through Erasmus University's participation in meetings and interviews with demo site representatives.

5.2.4 Access and Transparency

Training on ISB should additionally be extended to individuals' management of personal data within the company. To communicate the importance of ISB to workers, it can be valuable to additionally train them on their privacy rights and the extent of data collection practices within the company. By doing so, workers will acquire knowledge on the operating monitoring technologies within the company, which will in turn allow a transmission of the relevance of maintaining competent privacy preserving behaviour. This area of education is particularly relevant given the frequent close link between personal information and work-related data.

Furthermore, datapoints from workers can be collected as a by-product while ensuring safety and efficiency in the workplace. Even though in the present context of ASHVIN data collection practices of natural individuals strictly adhere to the norms stipulated in the GDPR, entailing that principles of minimization and proportionality are integrated into the operating mechanisms, these principles might fail to be acknowledged by workers. This is because of the noticeable presence of monitoring

technologies in the workplace, and worker's lack of knowledge regarding their scope and limitations.

Moreover, specifically in the context of manual jobs, monitoring practices in the workplace tend to translate into reduced trust in management (Holland et al., 2015), in turn potentially causing a deterioration in workplace relations. As such, transparency is proposed as a beneficial approach to increase trust and enhance perceptions of informational justice (Ball, 2021). Additional benefits of incorporating transparency of monitoring practices within workplaces include an improvement of workers' performance and increased perceptions of task satisfaction (Hovorka-Mead et al., 2002).

The principle of transparency can be materialized through the above-mentioned knowledge sharing practices, as this would serve as a productive discussion space for personal privacy concerns and the monitoring practices taking place within the workspace. The development of the ASHVIN platforms also considers workers as users, providing them with access to their own data. Importantly, the project aims to make this access straightforward and clear.

6 RECOMMENDATIONS ON PRIVACY AND SECURITY

One of the key objectives of this deliverable is to delineate recommendations to ensure privacy and safety preserving practices in ASHVIN, while simultaneously optimizing the implementation of IoT based digital twin platform. This concluding section serves as a compilation of proposed measures which are directly aimed at adhering to the objectives of efficiently and robustly safeguarding worker's privacy and safety in ASHVIN. These measures derive from sections above and have been selected because of their defining characteristics to capture the key objectives. Given this deliverable's consideration of an integrated approach, the recommendations adopt a sociotechnical nature which acknowledges both the human and technical factors required to comply with these aims.

The recommendations are structured into three main sections: transparency, proportionality, and holistic cybersecurity. These measures together aim to establish privacy preservation for workers by promoting a trustworthy and fair work environment, underpinned by the core principles of the GDPR. Because of the multi-layered characteristic of cybersecurity maintenance on an organizational level, the interdependence between technological affordances and end-users in an IoT-based digital twin platform is examined below.

6.1 Transparency

The integration of transparency within the workplace is amply valuable in terms of trust relations and performance. As such, this principle entails workers are informed about the monitoring practices within the company. The following subsections are specific recommendations to ensure the proposed transparency standards.

6.1.1. Inform Workers Thoroughly

This includes the scope of devices which collect data and what purposes this data collection has. Moreover, in the case that the data might expose individual workers when cross-referenced, these should be made aware of the potential impact of this on their lives. It is important that employees understand how workplace monitoring affects them, and if so, how their performance will be valued. This knowledge sharing process should additionally be extended to informing them on what the monitoring might reveal to co-workers and third parties.

6.1.2. Inform Workers Effectively

When initiating the knowledge sharing process, a series of factors should be considered to ensure the efficient information of workers. These considerations shall begin with the acknowledgement of potential cultural differences which may influence how privacy is perceived and how personal data is valued. For instance, in certain countries worker unions may prevent privacy abuses, while in other abuses might be complied with due to fear of losing one's job. These differences should be considered and serve as a basis for the customization of knowledge sharing practices.

This is particularly relevant given that there is no one-fits-all solution in these contexts, so due care should be taken to find which techniques are the most suitable to inform workers. As such, this might require custom-made privacy notices and trainings. For instance, besides traditional knowledge sharing techniques to inform

employees like posters or flyers, alternatives should also be considered such as instructional videos or training sessions depending on the context.

These knowledge acquisition efforts should additionally be complemented with the presence of an organizational measure in which employees are able to voice their concerns about invasive monitoring, privacy breaches, disproportionate data collection, etc. This measure additionally entails the designation of who or what will act upon employees' input (i.e., privacy officer, ethical committee, etc.). Finally, in order to establish an equality of treatment and promote a transparent workplace, it is recommended that supervisors and managers are additionally exposed to the same monitoring practices as their employees.

6.2 Proportionality

Proportionality is at the core of efficient personal data preservation within ASHVIN. This principle draws firm and decisive boundaries on data collection practices by limiting them to strictly necessary monitoring techniques and is consistent with the parameters of contextual integrity (Nissenbaum, 2003). The interests that are served should be effectively met (i.e., workplace safety, efficiency) but in a manner that is minimally intrusive and privacy preserving.

6.2.1 Always collect data with a purpose

Adherence to proportionality demands that the benefits associated with restricting the right do not outweigh the costs associated with exercising this right. Thus, only personal information that is appropriate for processing can be gained during data collection processes. To this end, the principles of purpose limitation and data minimization are relevant. The former designates that personal data must always be acquired for "specified, explicit and legitimate" purposes (Data Protection Working Party, 2015). The latter establishes that data personal data collection should be minimized (Data Protection Working Party, 2015). Altogether, this underlines that purpose limitation and adherence in combination with data minimization are key components of a holistic approach to privacy and cybersecurity.

6.3 Holistic Cybersecurity

Insurance of privacy preservation in the present context additionally opts for the adoption of a holistic cybersecurity approach, which is extended to the integration of efficient technical measures, while additionally considering relevant human factors.

6.3.1 Implement encryption and MFA

These issues are firstly tackled through the implementation of SSO with Keycloack, OAuth 2.0, and OpenID Connect authentication protocols. The incorporation of Keycloak OpenID connect is valuable because it safeguards the addition of an extra authentication layer on top of OAuth2.0.

Furthermore, because the GDPR's consideration of information relating to identified or identifiable persons as personal data, algorithmic encryption through edge computing addresses the posed privacy risks. In other words, if personal data is encrypted throughout its lifecycle, it is placed out of scope for GDPR compliance. However, it should be noted that the risk of decryption may rise due to future technological developments (Source: IT Governance Privacy Team, 2019). Therefore, it is recommended to continuously review the risk of decryption and consider the

implementation of alternative encryption tools accordingly. These risks are directly addressed through the encryption of the database and the communication between devices by using the Kubernetes API.

The implementation of AI and visual data processing techniques further addresses security and privacy concerns, as masking methods allow for the removal of human-identifiable information from visual datasets. Moreover, the output of timelapse devices is limited to the duration of activities and no information about individual employees is recorded. Raw data is processed on JETSON devices and no information is stored in local databases.

6.3.2 Assess and invest in information security behaviour

Given that human link is often the weakest in the cybersecurity maintenance chain, social engineering risks are approached as critical towards the preservation of privacy within the company. To this end, an increase in the ISB self-efficacy of workers is considered as central, because this then translates into improved ISB among a workforce. In practical terms this might result in a significant decrease of phishing incidents, for instance.

A valuable way to begin addressing these risks is by conducting a present knowledge assessment through a survey or interviews. Moreover, cybersecurity efforts within the company should be specifically addressed in the information security policy, which communicates the pre-established security standards effectively and succinctly to employees. Given the relevance of human factors, it is imperative to address these in conjunction with technical measures for an effective security strategy.

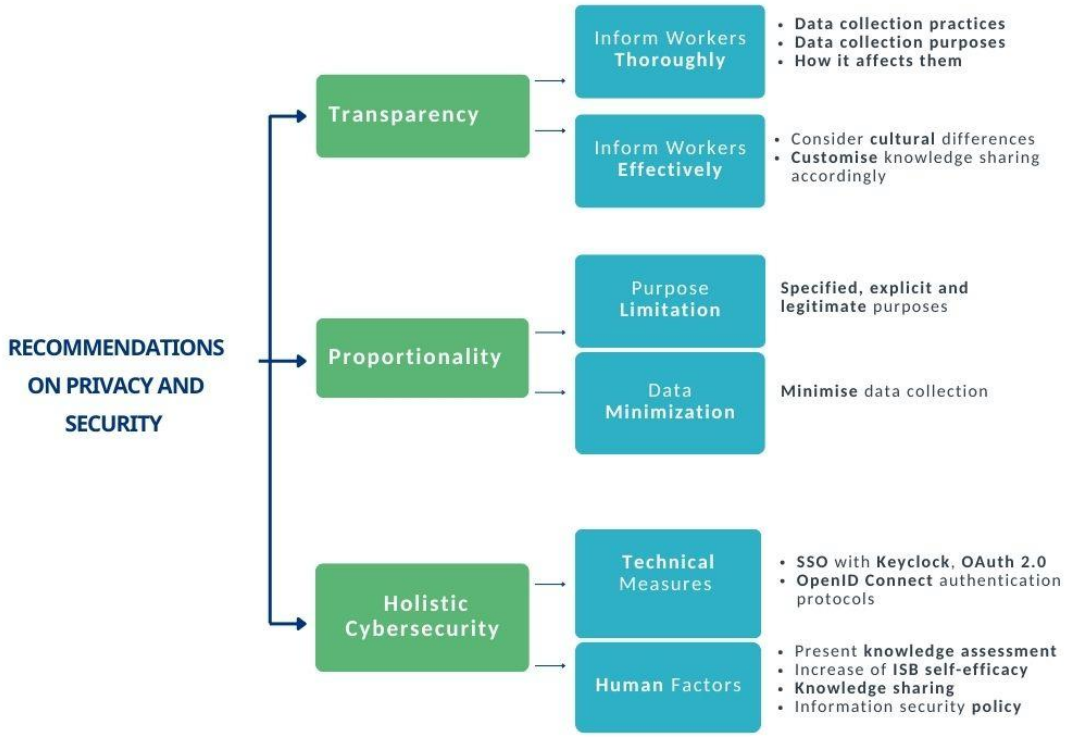

Figure 7: Recommendations on privacy and security

7 REFERENCES

Ball, K. (2021). Electronic monitoring and surveillance in the workplace: Literature review and policy recommendations. *JRC Publications Repository.*https://doi.org/10.2760/5137

Bhattacharjee, K., Chen, M., & Dasgupta, A. (2020, June). Privacy-preserving data visualization: Reflections on the state of the art and research opportunities. In *Computer Graphics Forum39*(3), 675-692.

Bulgurcu, B., Cavusoglu, H.,&Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness.*MIS Quarterly, 34*(3), 523–548.

Data Protection Working Party. (2015). *Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones*. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf

European Union (2016). Regulation 2016/679. *Official Journal of the European Communities*. Retrieved fromhttp://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf

European Union Aviation Safety Agency (EASA). (2021). *Easy Access Rules for Unmanned Aircraft Systems (Regulation (EU) 2019/947 and Regulation (EU) 2019/945).* Retrieved from https://www.easa.europa.eu/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulation-eu

European Union Aviation Safety Agency (EASA) (2022). *Drones—National Aviation Authorities.* Retrieved from https://www.easa.europa.eu/domains/civil-drones/naa

Furnell, S. &Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*,*31*(8), 983–988.

Holland, P. J., Cooper, B., & Hecker, R. (2015). Electronic monitoring and surveillance in the workplace: The effects on trust in management, and the moderating role of occupational type*. Personnel Review*, 44, 161- 175.

Hovorka-Mead, A. D., Ross, W. H., Jr., Whipple, T., &Renchin, M. B. (2002). Watching the detectives: Seasonal student employee reactions to electronic monitoring with and without advance notification. *Personnel Psychology*, 55, 329-362.

Kör, B., &Metin, B. (2021). Understanding human aspects for an effective information security management implementation. *International Journal of Applied Decision Sciences,14*(2), 105-122.

Mivule, K. (2013). *Utilizing noise addition for data privacy, an overview.*https://doi.org/10.13140/2.1.4629.2482

Muchagata, J., Vieira-Marques, P., & Ferreira, A. (2019). mHealth Applications: Can user-adaptive visualization and context affect the perception of security and privacy? *ICEIS* (2), 444-451.

National Cybersecurity Center (2022). *Cyber security for construction businesses.* Retrieved from https://www.ncsc.gov.uk/guidance/cyber-security-for-construction-businesses

Padayachee, K. (2012). Taxonomy of compliant information security behavior.*Computers & Security*,*31*(5),673–680.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. &Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies.*Computers & Security*, *66*, 40–51.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work, 24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Pridmore, J., & Oomen, T. A. (2019). A practice-based approach to security management: Materials, meaning and competence for trainers of healthcare cybersecurity. *International Security Management*, pp. 357-369.

Seo, J., Han, S., Lee, S., & Kim, H. (2015). Computer Vision techniques for construction safety and health monitoring.*Advanced Engineering Informatics*, *29*(2), 239–251. doi: 10.1016/j.aei.2015.02.001

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. &Herawan, T. (2015). Information security conscious care behaviour formation in organizations.*Computers & Security*, 53, 65–78.

Webroot (n.d.). *What is Social Engineering? Examples and Prevention Tips*. Retrieved from https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering

World Economic Forum, Marsh & McLennan, SK Group, & Zurich Insurance Group (2022). *The global risks report 2022.* World Economic Forum. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

APPENDIX 1: SECURITY AND PRIVACY GUIDELINES (EN / ES)

ASHVIN

Digitising and transforming the European construction industry

contact@ashvin.eu

@AshvinH2020

www.ashvin.eu

Security and Privacy Guidelines for Construction Professionals

Central to the security of construction companies are **employees**.

Together, we contribute to **cyber security** and protect the **privacy** of your fellow co-workers.

1

What?

Sensitive data is information about workers or the organisation.
E.g: health data, blueprints, CCTV, or sensor data.

2

Where?

You may work with several technological tools on your site. All send data to the IOT-platform.

3

Why?

Wrongful use of sensitive information can harm the organization, your co-workers, and yourself.

4

Who?

Employees are the first line of defence: an integral part of the cyber security of construction companies.

5

How?

With the right knowledge and skills, everyone can protect sensitive data against attackers.

How can you contribute and keep everyone secure?

Passwords

- **Never share your passwords** with others.
- Try not to write log-in details down on paper. Store your passwords where only you can access them.
- Use the **password manager tool** recommended by your supervisor.

- **Do not reuse passwords** – each platform, device and website should have different and strong passwords.
- Use the **multi-factor authentication** tool on the Ashvin platform.

Follow the guidelines

- Read and understand your organisation's **Information Security Policy**.
- Always ask if you have **questions** or **suggestions** for improvement. Your input is valuable!

Confidentiality

- **Never share** data collected in the workplace with colleagues or people outside work.
- To keep the construction site safe for all, always **report behaviour that causes security risks** to your supervisor. Your report will be handled with integrity.

Software

- Always **update** your operating systems to the most recent version.
- Use the **anti-virus** and **anti-phishing** software recommended by your supervisor.

Phishing and malware

- Suspicious email? **Never click on links you do not trust**.
- Attackers may **impersonate friends or colleagues** to communicate with you through emails or social media.

- Construction projects involve multiple companies, so cyber-criminals may mimic one of these. Be extra alert and **always double-check the sender's email adress**.

Know your rights

- This company operates under the General Data Protection Regulation. The information collected about you and your co-workers must be limited to **legitimate interests** and **made clear to you**.

- **Know the limits and speak up** if you feel that personal data collection processes are excessive.

Responding to a data breach

1. Know that this may happen to everyone – even when being cautious.
   Do not panic.
2. To limit the damage, **immediately contact your supervisor.**
3. **Follow their further instructions** carefully.

ASHVIN.EU

ASHVIN has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 958161.

ASHVIN

Digitalizando y transformando la industria de la construcción Europea

contact@ashvin.eu

@AshvinH2020

www.ashvin.eu

Recomendaciones de Ciberseguridad para Profesionales de la Industria de la Construcción

Los **empleados** son un componente **central** de la **seguridad** de una empresa de construcción.

Juntos, compartimos la responsabilidad de **mantener la información a salvo** de posibles ciber-ataques.

1 ¿Qué?

Los **datos confidenciales** son información sobre los **empleados** o la **organización.** E.g.: Datos de salud, de operación de máquinas o planos.

2 ¿Dónde?

Usamos **tecnologias** que **envían información** a la **plataforma-IOT** para mejorar la **seguridad** y la **eficiencia** de nuestro trabajo de contrucción.

3 ¿Porqué?

El **uso inapropiado** de **información confidencial** podría ser **perjudicial** para la **organización**, un **compañero** de trabajo o incluso para **usted**.

4 ¿Quien?

Los **trabajadores** son la **primera línea de defensa:** Una parte íntegra de la **ciberseguridad** una empresa de contrucción.

5 ¿Cómo?

Con las **herramientas** y **conocimientos** apropiados, **cualquiera** puede **proteger** los **datos confidenciale**s de su organización.

¿Cómo puede contribuir a mantenernos todos seguros?

Contraseñas

- **No comparta** sus contraseñas con nadie.
- **No escriba** sus datos de inicio de sesión en un papel.
- Utilice la **herramienta de administración de contraseñas** que le recomiende su supervisor.
- **No reutilice** las contraseñas: cada plataforma, dispositivo y sitio web debe tener su propia contraseña.
- Use la **autenticación multi-factorial** de Ashvin.

Siga la instrucciones generales

- **Lea** y **comprenda** la **Política de Seguridad** de su organización.
- **Comuníquese** con su supervisor siempre que tenga **dudas** o **sugerencias** para mejorarla. ¡Su contribución es valiosa!

Confidencialidad

- **Nunca** comparta datos recopilados en el lugar de trabajo con nadie.
- Para mantener el lugar de construcción seguro para todos, cualquier **comportamiento sospechoso** que pueda causar riesgos de seguridad debe **informarse** a su supervisor. Su informe será manejado con integridad.

Software

- **Actualice** los **sistemas operativos** de sus dispositivos a la versión más reciente.
- Utilice **softwares antivirus** y **anti-phishing** recomendados por supervisor.

Phishing y malware

- ¿Email sospechoso? **Nunca pinche en enlaces** en los que no confíe.
- Los ciberdelincuentes pueden hacerse pasar por **amigos** o **compañeros de trabajo** para comunicarse con usted a través de **correos electrónicos o redes sociales**.
- Los proyectos de construcción **involucran a varias empresas**, por lo que los ciberdelincuentes pueden imitar a una de ellas. Esté alerta y **siempre verifique la dirección de correo electrónico del remitente**.

Conozca sus derechos

- Esta empresa opera bajo las indicaciones legislativas establecidas por el **Reglamento General de Protección de Datos (RGPD)**. La información recopilada sobre usted y sus compañeros de trabajo debe limitarse a **intereses legítimos**, y su recopilación y usos deben **ser claros** para usted.
- **Exprese su opinión** si considera que los procesos de recopilación de datos personales son excesivos.

¿Cómo responder a un ciber-ataque?

1. Esto le puede pasar a cualquiera, incluso teniendo cuidado – **No se asuste.**
2. Para limitar los daños, **contacte immediatamente a su supervisor.**
3. **Siga sus instrucciones** detenidamente.

ASHVIN.EU

ASHVIN ha recibido financiación del programa de investigación e innovación Horizon 2020 de la Unión Europea en virtud del Acuerdo de subvención n.º 958161.