ASPECTS OF BODY METRICS DATA MANAGEMENT IN THE LONG TERM FOR THE EUROPEAN FITNESS INDUSTRY

Guérineau, Benjamin-Julia (1,2); Samir, Kousay (3); Richrath, Marvin (4); Paetzold, Pr. Kristin (5); Montero, Joaquin (5)

1: Laboratoire Roberval, FRE UTC-CNRS 2012, Sorbonne Universités, Université de technologie Compiègne; 2: Laboratoire Numérix, École de technologie supérieure de Montréal; 3: KTH Royal Institute of Technology, Department of Production Engineering; 4: Institut für integrierte Produktentwicklung (BIK), Universität Bremen; 5: Universität der Bundeswehr München, Fakultät für Luft- und Raumfahrt, Institut für Technische Produktentwicklung

ABSTRACT

The dawn of the fourth industrial revolution, mostly known through the German initiative "Industrie 4.0", builds on a set of technologies emerging from software and information and communication technologies (ICT); paired with the growth of the Internet-of-Things (IoT), the so-called “smart products” are expanding on the market. These smart products integrate data collection and processing capacities. Additionally, the collected data have their own lifecycle, and can be classified as sensitive data. In that sense, companies developing hardware products may need support to step in “smart products” development. Digital transformation strategy is a possible overall support for companies. However, regarding smart product development and IoT data management, no studies to date have addressed formalized guidelines to support companies. This article proposes a set of guidelines focusing on IoT data management to support hardware companies in their transformation towards smart products. The proposed guidelines are exemplified on a fitness industry case which is using wearable devices collecting body metrics, considered as sensitive data.

Keywords: Industry 4.0, Digital transformation, New product development, Experience design, IoT data management

Contact:
Guérineau, Benjamin-Julia
Sorbonne Universités, Université de technologie Compiègne
Ingénierie Mécanique
Canada
benjamin.guerineau@utc.fr

Cite this article: Guérineau, B.-J., Samir, K., Richrath, M., Paetzold, K., Montero, J. (2019) ‘Aspects of Body Metrics Data Management in the Long Term for the European Fitness Industry’, in *Proceedings of the 22nd International Conference on Engineering Design (ICED19),* Delft, The Netherlands, 5-8 August 2019. DOI:10.1017/dsi.2019.211

https://doi.org/10.1017/dsi.2019.211 Published online by Cambridge University Press

1 DIGITAL TRANSFORMATION AND THE DATA MANAGEMENT ISSUE

The current decade will probably be marked by the dawn of the fourth industrial revolution, conceptualized across different countries by different programs and initiatives which try to determine the way of conducting this revolution, defining the key technologies and a high-level roadmap. Among them, probably the most well-known is Industrie 4.0, which emerged in Germany in 2011 (Kagermann *et al.*, 2013). For the moment, this upcoming industrial revolution is only a forecast. However, the emergence of new technologies and trends is a common feature to all previous industrial revolutions (Lasi *et al.*, 2014). The fourth industrial revolution seems not to derogate, and will probably be driven by, a set of technologies - some of which may not have been identified yet. Among these new technologies, the integration and expansion of connectivity (Porter and Heppelmann, 2014), the enhancement of information and communication technologies (ICT) (Li, 2017), and the development of digital technologies are shaping new products. Tightly linked with the connectivity and ICT development, the Internet of Things (IoT) paradigm extended the Internet network to the consumers' products. The IoT "is a new technology paradigm envisioned as a global network of machines and devices capable of interacting with each other" (Lee and Lee, 2015). The IoT offers an "infrastructure of interconnected physical entities, systems and information resources together" (ISO, 2016). From the authors' perspective, IoT is supporting connectivity through an infrastructure, and allows the connection of devices, the nodes of this pervasive network. Therefore, the industrial landscape is about to change and will offer new opportunities to companies.

Consequently, this upcoming industrial revolution can lead companies to evolve the way of developing and manufacturing products, as well as rethinking and innovating their business models (Burmeister *et al.*, 2015) and the products themselves. In that sense, the fourth industrial revolution is not only about technology, it is also about a complete transformation of companies and industries. This transformation can be conducted using digital transformation strategies. These strategies rely on four transformational dimensions which are the use of technologies, structural changes, changes in value creation, and financial aspects (Matt *et al.*, 2015). Accordingly, industries are reaching a tipping point, and can decide to enter the fourth industrial revolution through a digital transformation strategy to conduct changes on these four dimensions. All of these dimensions must be coordinated as tight dependencies exist between them.

Hence, the use of technologies is related to product transformation from traditional to smart products, and is one aspect of digital transformation. Companies can develop smart products through the integration of new components and technologies (Porter and Heppelmann, 2014), which in turn allow the capability to collect, process and store data. To that extent, Vermersan *et al.* underscored that "the utilization of the smart product, equipment and infrastructure will lead to a huge amount of available data" (Vermersan and Friess, 2010). In that sense, the transformation from traditional products to smart products brings a new element into play. The step toward smart products raises the question of data management, including collection, processing and storage. Although the product data management is not new for some companies, the data collected, processed and stored along product usage can be unfamiliar for hardware companies and is coming with associated issues.

2 SMART PRODUCTS: DATA, OPPORTUNITIES AND CONCERNS

Data is a new and core aspect of smart products, by the opportunities created, as well as the concerns raised. Among the opportunities, Kagermann *et al.*, presented the example of creating value opportunities through the integration of new services based on collected data processed by algorithms (Kagermann *et al.*, 2013). For the companies, collected data can also be looped to the development process (Kiritsis, 2011) and used to improve product design and better understand the user experience.

Regarding the concerns, Kagermann *et al.*, also warned about the cyber security threat, saying "the goals of security measures are to increase confidentiality, integrity and availability" (Kagermann *et al.*, 2013). Therefore, the development and the commercialization of "smart products" are raising new challenges for companies. Part of these challenges emerge from product and usage data collection and management. As discussed by Fan and Chen, "the existing data management technology cannot meet the need of data management in the Internet of Things independently" (Fan and Chen, 2010). IoT data management should follow the data lifecycle and consequently includes the capture of the data, transmission through connectivity, processing, storage and destruction. IoT data management is thus concerned by different aspects such as cyber security, ethics, physical and geographic storage,

https://doi.org/10.1017/dsi.2019.211 Published online by Cambridge University Press

processing algorithms, and data sensitivity. Indeed, smart products can also collect physiological metrics, bank data or GPS data logs. Furthermore, the recent General Data Protection Regulation (GDPR) covering the European Union and European Economic Area is adding strict rules to personal data management.

Therefore, releasing a new smart product can be an issue, especially for small and medium enterprises (SMEs) for whom resources can be limited and have inadequate capabilities (Li *et al.*, 2017). In addition, as underscored by Faller and Feldmúller, “SMEs have the difficulty to be highly skilled in applications and technologies of Industry 4.0” (Faller and Feldmúller, 2015). For these reasons, this paper aims at proposing guidelines to support SMEs along their digital transformation with a special focus on IoT data management.

The next section presents the methodology used to design the guidelines, envisioned as a possible answer to the problem statement. The fourth section is the state-of-the-art and gather different aspects of data features and IoT data management. The existing guidelines are reviewed as well. The fifth section is divided into two subsections. The first one focuses on the summer school use case, as well as the strategy adopted to conduct changes from traditional products to “smart products”. The strategy is explained through the choices made and the questions raised along the project course. The explanations represent the “designerly” ways of knowing, which combined with the state-of-the-art insights, enable to propose a set of guidelines to support companies aiming to develop “smart products”. The guidelines are presented and explained in the second subsection. The final section proposes a conclusion paired with an outlook and the perspectives.

3 METHODOLOGY: “LEARNING BY DOING”

The work presented throughout this paper was conducted in the context of the International Summer School on Integrated Product Development, edition 2018 (IPDiss18). The IPDiss18 relies on the “learning by doing” dictum paired with the achievement of a product development scenario. This scenario was defined based on the situation of a small hardware company designing and manufacturing fitness devices. The main project’s objective was formulated as follow: “Develop a new business model centered around the company’s fitness devices for increasing the user’s fitness, for a range of customers”. The company has identified three trends based on customers’ needs and expectations, as well as market opportunities. Among these trends, the “digitization opportunities” and integration of connectivity have oriented the work towards the development of a product including a wearable device and a cell phone application. This illustrates the case of traditional and hardware companies which attempt a digital transformation by conducting changes on the organization, business models, and products to enter the fourth industrial revolution.

To develop the concept and provide a commercial solution, the Integrated Product Design (IPD) process (Andreasen, MM and Hein, 1987) was used to structure the scenario, from the “recognition of need phase” to the “execution phase”. The IPD process integrates marketing, design and production aspects conducted concurrently with product development, consequently improving the experience of design and bringing it closer to an industrial case.

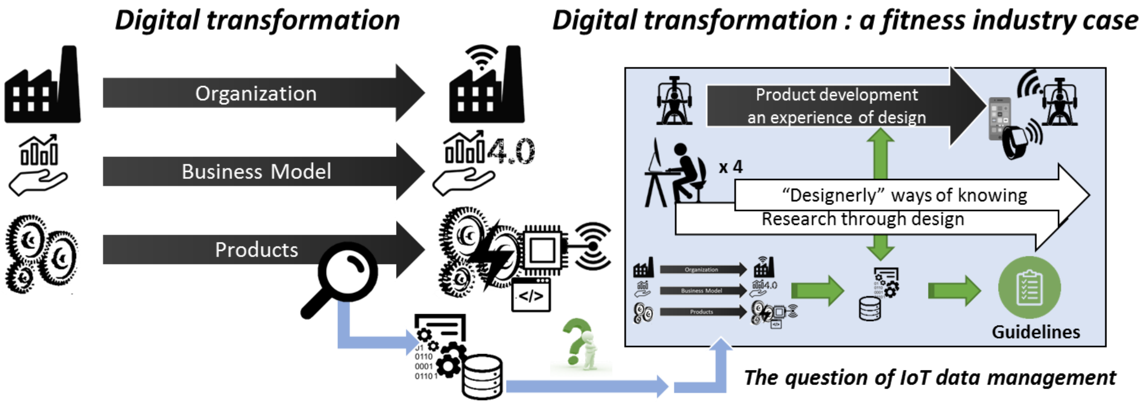


Figure 1. Overall methodology: generic digital transformation raising the IoT data management question.

https://doi.org/10.1017/dsi.2019.211 Published online by Cambridge University Press

The work was conducted by four PhD candidates who can be considered as practitioners of design. Design was experienced through the product development leading to a formalized research outcome. This experience of design with practitioners of design and the associated work are inspired by research through design. Indeed, the "learning by doing" dictum associated to the project can be considered a simplified echo to Frayling's "how can I tell what I think till I see what I make and do", used to define research through art and design (Frayling, 1993).

In addition, as underscored by Cross, "some of it [Design knowledge] is knowledge inherent in the activity of designing, gained through engaging in and reflecting on that activity" (Cross, 2001). Throughout the activity of designing conducted along the scenario, design problems have emerged by which knowledge was generated by the practitioners. This knowledge was created to propose a viable solution to the IoT data management issue in accordance to the material a SME can have. Indeed, the IoT data management question can be new for the traditional SMEs. To that extent, the research was influenced by the "designerly" ways of knowing (Cross, 2001) to generate and gather knowledge used to compose a set of guidelines to support companies in their digital transformation.

Figure 1 illustrates and synthesizes the overall methodology adopted to create the guidelines.

4 STATE-OF-THE-ART

The creation of many small computational units instead of one big one is a trend which comes with the fourth industrial revolution. One or several of these units can create a system or a smart product. These smart products are decoupled units which together create a big network of information and control, therefore the importance of grouping the smart products increases. The big network is described as the IoT. Each smart product connected to the network contains its own central processing unit (CPU), self-contained and able to compute its own results. The distributed software architecture approach combines these smart products with software in which tasks and computations can be shared. Another approach of the software combines the collective intelligence of the smart products to create more knowledge about the surroundings. The combination of these two software objectives creates distributed intelligent smart products that can both work on their own but also combine information with other smart products towards a common goal. Having each entity encapsulated also makes expandability as a built-in feature (Jammes and Smit, 2005; Jokinen and Lastra, 2016; MacKenzie *et al.*, 2006).

The communication that occurs has a time perspective, in terms of parameters to control, which is a difficult matter in distributed intelligent architectures. This is due to the inability to send and receive messages without delay. IoT relies on the quick transfer of information. The delay is not associated with the smart products as they can be controlled real-time, however when communicating over an Enterprise Service Bus (ESB) time can pass before the messages are received. To tackle this minor problem, event-driven Service Oriented Architectures (SOA) are created. Event-Driven SOA rely on the occurrence of an event to trigger services. These services can in turn perform simple tasks or entire enterprise processes. This comes from the incorporation of Event-Driven Architecture (EDA) where an occurrence of an event triggers other events. An event can be any notable thing outside or inside the business. When an event occurs, all interested systems react to that event. As this is very loosely coupled the sender of the event may only know that they sent the message but not to what other systems or services transpired because of the event (Michelson and Links, 2011; Michelson, 2006).

The issue of security and privacy grew with the introduction of the IoT network idea. The nature of Industrie 4.0 technologies is linked to information and communication technologies which is closely related to information sharing, it is also here where the issue of cybersecurity comes into play. Dispersed assets create opportunities where security is compromised (Ashibani and Mahmoud, 2017; Ten *et al.*, 2010). However, for autonomous decision making more information from the physical world needs to be digitalized. It is not viable for the increased amount of smart products to be connected physically, therefore wireless technologies are the key to adopting IoT. Wireless Sensor Networks (WSN) is a term used to define a system of smart devices which measure different physical phenomena and send gathered data to a centralized hub. The data streams can be processed from there or sent real-time to the control systems for direct use (Akyildiz *et al.*, 2007).

With the application of WSN, IoT is seen as the stepping stone for enabling autonomous machine-to-machine operations. Recent developments enable specific architecture structures which incorporate IoT enabling technologies. The importance of the middleware layer, which transcribes the raw data, is increased due to the information processing occurring in that specific layer (Khan *et al.*, 2012).

https://doi.org/10.1017/dsi.2019.211 Published online by Cambridge University Press

Scalability requires a robust backbone for the system, otherwise scalability issues may arise when expansion is due. Two main parts of these are data transfer and data processing and management. Big Data expands the middleware layer to a degree where it may be necessary to define these parts before implementation (Xu *et al*., 2014).

As (Fan and Chen, 2010) describe the structure of such systems, data management is located in the centre of the "Interlayer". The data management has defined functions to increase value of the perceived data created from the hardware. These functions include cleaning, filtering, aggregation and conversion. The end product after these functions is comprehensible data (Miorandi *et al*., 2012).

Binary data is transmitted between the smart products in the network. When the data, during a later stage, is made comprehensible through processes and functions, the importance of sensitive data management is introduced. Auto identification (Auto-ID) technology is used to automatically identify entities with the help of tokens with individual code. This information is collected in a computer system to support controlling functions like localisation of entities or recording of status information. The most known technology for this purpose is Radio Frequency Identification but also other technologies such as Near Field Communication or use shape recognition are used in several use cases. Which technology is best to use is highly dependent on the circumstance of the use case and therefore requires intensive evaluation before implementing. One of the key function in future Auto-ID technology is the integration into a wireless communication network. This enables the management of different tokens according to the physical unit they are attached to. Auto-ID technology is purely related to a digital identification of physical entities. Other systems such as Real-Time location systems are built on top of Auto-ID technology. Auto-ID technology gives opportunities to make assets visible and enable early decision making. The functionality of localisation makes the Real-Time Localisation Systems (RTLS) the next step after Auto-ID solutions (Liu *et al*., 2012; Shamsuzzoha *et al*., 2013; Ustundag and Cevikcan, 2018). This in turn leads to the understanding that the usage of RTLS systems also includes identification of the entity being tracked.

The field of IoT data management is in rapid change due to Big Data collection and the increased amount of companies choosing to digitalize most of the data available. A common theme that emerges points out that to be sustainable in the market today, requirements for maintenance and continuous developments are necessary. These requirements are for all components of the system including techniques, methods and frameworks (Fan *et al*., 2015; Takata *et al*., 2004).

The European Nation has recently introduced the GDPR which focuses on personal data security and integrity; it was implemented during the second quarter of 2017. The new regulation focuses on modern data management of sensitive data, or data that can be identified to a specific person. These regulations require transparency between customer and company. Another requirement is an official publication when a data breach is found. Those who do not follow these regulations stand to be prosecuted with serious consequences (Stigestadh and Moberg, 2018; Tankard, 2016).

The process of securing the company assets becomes increasingly important with digital products and services. To approach this task, companies are adapting and introducing new methodologies of maintaining data integrity and security, where some require a reform in regulations (King and Raja, 2012). The use of guidelines increases company awareness and competitiveness in the long term, as proposed by (Porter and Heppelmann, 2014). The guidelines help with defining the company's core value-adding capability, introducing considerations that could be more useful in the long term. The aspects to be considered can be divided into sub-category questions. The answers will indicate the categories which are in need of further investigation. Firstly one has to closely define the nature of the business approach and the business model, restricting to B2B or enable capabilities for expansion to further customers in the future. The same should be clearly defined for the specific feature or capability that creates the market leadership. When the business grows, the importance of outsourcing, distribution channels and ownership will increase. Therefore, it is advisable to have strategies in mind from the beginning to not become overwhelmed by the amount of work required during a later stage. Especially for modern firms where the market competition is fierce and the focus can be on cloud services. Data security of the product data for those scenarios is vital as the digital products are susceptible for far more vulnerabilities than traditional physical products. It is seemingly easy for ownership to change due to such circumstances and it may be wise to rethink if the product should be part of a closed loop system or encompass the open approach.

Companies need to define their approaches and business models clearly as digitization creates fiercer competition.

https://doi.org/10.1017/dsi.2019.211 Published online by Cambridge University Press

5 PROPOSITION: GUIDELINE FOR SMALL AND MEDIUM ENTERPRISES

The sensitivity of the data that can be handled by the SMEs can be relatively high, so it must be kept in mind that it can stolen, and third parties can use it for unwanted commercial purposes. It is therefore necessary to clarify the direction that entrepreneurs should take when handling all this data flow, so as not to inadvertently harm the user. It is also clear that with the approval of the data administrator, this information can provide advantages to anyone interested, in pursuing different purposes. In order to foresee the mishandling of the data, the entrepreneur is recommended not only to understand how his/her own system works (in the case that is not self-developed) but also to understand its future evolution. It is always advisable to develop a simple data storage system taking into account the current regulations with the respective strategies of data quality, integration and analytics.

Having the body metrics of a certain group of people in the near future can be something usual for companies even in real time flow. A clear example of this, is the first step that Apple has taken with its AppleWatch® (Phelan, 2017), creating a scenario where the device monitors the pulse with the pretext of integrating this information on applications related to the user's health.

In the following section a use case proposed to the authors is presented, in which they had to take the role of a SME to cope with the situation of a fitness equipment manufacturer going through digital transformation.

5.1 Use case: fitness centres

From 2016 to 2017, revenues in the European health and fitness market rose by 1.9% to 26.6 million euros, while the average monthly membership fees decreased by 0.1%. This increase is primarily from the newly opened fitness centres and their associated customer growth. This development is mostly driven by the low-cost providers, which generated the strongest growth (absolute memberships). As the number of fitness centres increase, so does the demand for the fitness equipment (Deloitte, 2018). In view of this trend, the development and introduction of new business models represents an opportunity to meet the growing competitive pressure that would set themselves apart from the competition. This contribution is based on a business model developed for a fitness equipment manufacturer (SME) who wants to improve user´s fitness through a digital transformation of its fitness devices. The concept pursues the strategy of entering the market by establishing business relationships with fitness centres (B2B) in order to acquire fitness centre users as customers in the long term (B2C).

The development of this business model involves the implementation of smart technologies, and the use of such technologies leads to changes in the product development (Guérineau *et al*., 2018) and the product life cycle of the fitness devices. Not only, for instance, the existing manufacturing lines have to be adapted but other aspects come into play. The step towards digital transformation has pushed the collection of large amounts of personal data into focus.

The acquisition of data begins right after the product enters the market, and thus is necessary to constantly audit and maintain the IT system, and to bear in mind responsible data processing which is carried out during the entire product life cycle, must be also continued even after the end-of-life of the product.

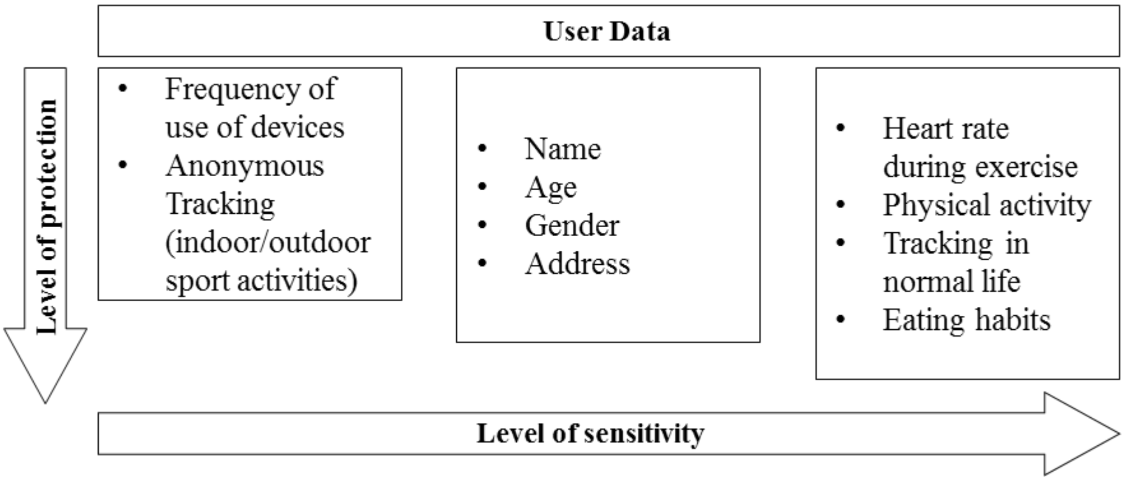

User Data
Level of protection
• Frequency of use of devices
• Anonymous Tracking (indoor/outdoor sport activities)
• Name
• Age
• Gender
• Address
• Heart rate during exercise
• Physical activity
• Tracking in normal life
• Eating habits
Level of sensitivity

Figure 2. Classification of the data with different levels of security according to its sensitivity

https://doi.org/10.1017/dsi.2019.211 Published online by Cambridge University Press

At the beginning the SME had very basic fitness devices and envisioned to step towards smart products. In that sense, the SME aims to make them smarter through the integration of sensors in the existing machines and the use of smart wearables linked to a network for increasing activity monitoring. The type of data to be handled includes body metrics records (BMR), personal information for the wearables (hearth rate, position tracking, and temperature), machine settings for the fitness devices (frequency, load, repetitions), and everything associated to an identification profile of the user (gender, age, ID number). The to-be-acquired data is classified in categories, and concepts for storage and further processing are developed. In this particular case the field "sensitivity" and the classification is analysed accordingly the diagram in Figure 2.

Regarding storage infrastructure, when deciding on an in-house storage, it must be taken into account that the security policy implemented must be kept up-to-date and carried out by the SME. However, when using cloud-based storage, the security policy is usually outsourced to the company offering the storage service. While the customer may have a feeling of safety that their data is only stored in in-house facilities, sometimes it is not the best solution, so it is important to understand this commitment ratio. After all, the SME must decide this depending on the projection of costs throughout the project, although the reduction of workload in terms of cybersecurity is a significant factor when making this decision. In this case, it was decided for an in-house storage purely for economic and marketing reasons, but it was decided to outsource the security policy for the data. This is done because as sensitive information is stored, the focus is on mitigating the risk of the client data being used for commercial purposes by third parties. It is true that the cloud-based solution is easier to scale, but the SME decided to implement escalation of the infrastructure right at the middle of the product lifecycle. In addition, telling the costumer that the sensitive data will be encrypted and stored in some in-house private facility is believed to have a greater marketing impact when offering the service.

The detailed data will be deleted off the server after 1 year, with the explicit consent of the user. The company will keep only general data with a high level of K-anonymity after the year and along the lifecycle of the product, for evaluation purposes. The contracts will be for a minimum of 1 year, so in that way the client is not generating poor quality entries in the indexes generated by the SME. This procedure is actually implemented by the current fitness centres BM in Germany, an example is Fitstar®. When the client leaves the membership all the personal data will be deleted, unless they want to keep it on the server for future registrations.

5.2 Findings

Since 1998, according to the UK's Data Protection Act, body metrics data can be considered as sensitive data because it falls in the sub-category of data containing information about physical condition. Moreover, the GDPR considers the biometric and health data as strictly personal sensitive data that must be subjected to a higher level of protection. In order to responsibly protect the user's privacy, the authors encourage entrepreneurs who did not go through digital transformation to comply the proposed guideline recommendations appearing in Figure 3 when handling a large amount of sensitive data.

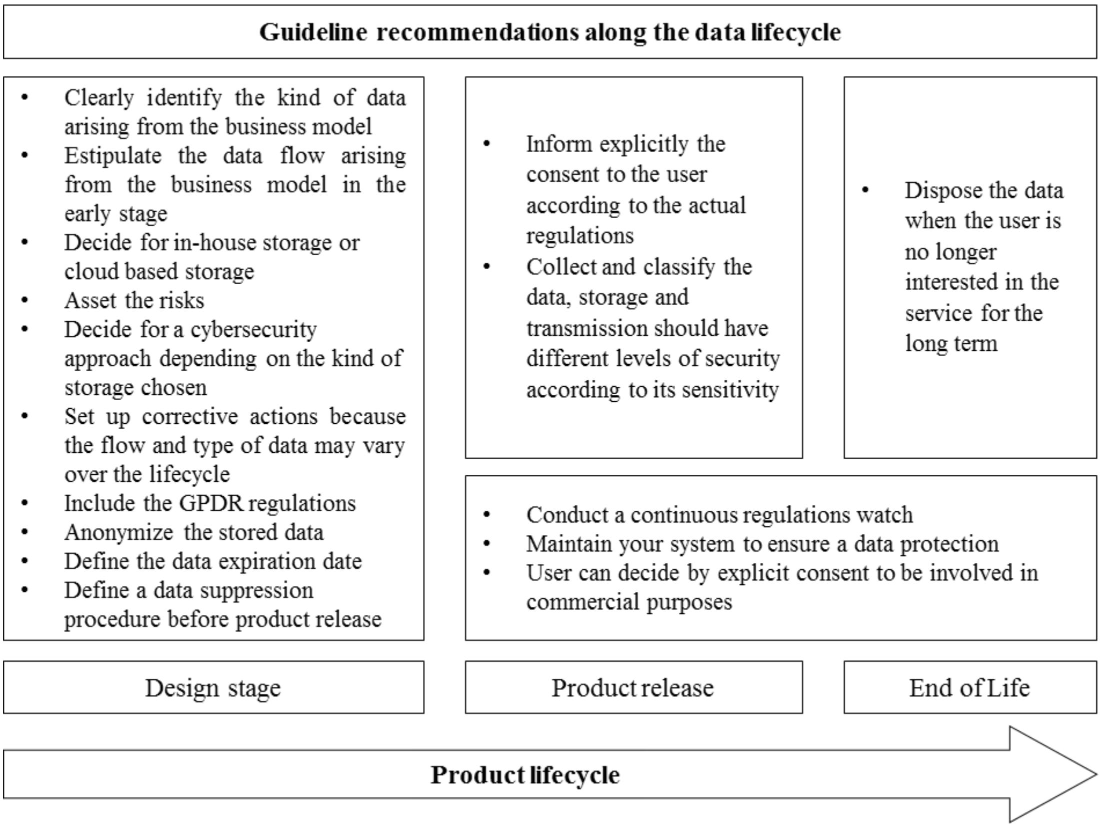
Many sections of the guideline recommendations can be considered in the early stages of the product development process, however, the number of the suggestions indicate that the process of digital transformation is not trivial.

In this case, right after the product release a large amount of data will be gathered. The data collected and then stored by fitness wearables have their own particularities, and is defined in this article as BMR. These types of records are far from what is known as Electronic Health Records (EHR) (Szolovits *et al*., 1994), but the reality is that they deserve to be treated in a similar way, given the ease with which such sensitive data can be used for commercial purposes. The main difference is that the data collected by wearables are continuous sampling and, although in this case they are not transmitted in continuous streaming, in the near future this could easily happen. In this way the data belonging to each user is constantly growing within a database in the form of body metrics histograms.

In the first instance the plan for responsible management should be defined, and the purpose of the data understood, keeping in mind that the user should never be harmed in any way. The protection of the data should be proportional to the sensitivity they represent and it must be established in advance how to anonymize data. Separate storage, if it is an option, must be done from the beginning. Regarding the risks involved, it is always important to raise the worst case scenarios and plan to act accordingly; even though a leak may seem not likely due to security or corruption failures, a data

https://doi.org/10.1017/dsi.2019.211 Published online by Cambridge University Press

breach can occur. Before starting to manage a database that grows constantly at a speed proportional to the number of users, the owner of the database must understand that it is advisable to divide the data into a sensitive and non-sensitive parts with separated storage, from the first moment. The sensitive part operates under a different encryption than its counterpart. The encryption must be done prior to its transmission to the storage server, thus complicating the possibility of manipulation and improper use of data by the data administrator, which could be a third party or cloud-based. In the same way that the user´s privacy is ensured in the EHR according to (Benaloh *et al*., 2009), it is advisable to do the same with sensitive BMRs by means of encryption and access control.



Guideline recommendations along the data lifecycle

- Clearly identify the kind of data arising from the business model
- Estipulate the data flow arising from the business model in the early stage
- Decide for in-house storage or cloud based storage
- Asset the risks
- Decide for a cybersecurity approach depending on the kind of storage chosen
- Set up corrective actions because the flow and type of data may vary over the lifecycle
- Include the GPDR regulations
- Anonymize the stored data
- Define the data expiration date
- Define a data suppression procedure before product release

- Inform explicitly the consent to the user according to the actual regulations
- Collect and classify the data, storage and transmission should have different levels of security according to its sensitivity

- Dispose the data when the user is no longer interested in the service for the long term

- Conduct a continuous regulations watch
- Maintain your system to ensure a data protection
- User can decide by explicit consent to be involved in commercial purposes

Figure 3. Guideline recommendations for hardware SMEs moving towards "smart products"

Along the product life the SME should keep a relationship with the users and clarify important issues. The users, at the time of contracting the service must be explicitly informed about the risks involved with their personal data and how their data will be used in the short and long term, according to the current European regulations, i.e. under the GDPR. The longevity of the data must be predetermined according to the long-term plans, and the data must be destroyed if the users wish to leave the system. In this type of data collection system, it is important to highlight that the human factor is not present during the collection itself - which is performed automatically and constantly by a device - ensuring the accuracy, uniformity and quality of the collected data.

The provided guideline integrates simple actions that SMEs can use, to deal with carrying out a digital transformation. In many senses, it enhances the transparency so that SMEs can assess the risks and opportunities for their desired digital transformation. Our contribution aspires to be pragmatic and oriented toward industry. The research is meant to be applicable and is not necessarily addressed toward the scientific community.

6 CONCLUSION & OUTLOOK

Traditional SMEs can be advised of the importance of following guidelines to help them to process and manage the data they deal with. The relevant problems that can arise regarding IoT data management of SMEs is more impactful in the long term, which is why it is important to raise awareness among entrepreneurs from an early stage. With the guideline presented is possible to support SMEs through the digital transformation. As it can be seen, a small digitization of an existing product can create a massive

https://doi.org/10.1017/dsi.2019.211 Published online by Cambridge University Press

amount of data, and the SMEs must unexpectedly deal with something that - if not handled in the right way - can bring inconvenience or can be used for unwanted purposes.

Following the trend that people want to be increasingly connected, it is expected that the traffic of personal data will increase, in addition to the rise and the commercial success of smart products. Consequently, the uncertainty of how to handle information responsibly also grows. Particularly for the kind of data analyzed in this contribution, the actual approaches for healthcare data management are applicable but in a less exigent way. It is necessary to differentiate between levels of sensitivity, e.g., the difference between having all the disease history personal data from a person and having a continuous position and heart rate available. As a partial solution the encryption and the optional separate storage of location and body metrics are recommended in the short term. Additionally, it is important to maintain these actions in the long term as well, till the longevity of the data is old enough to be disposed of.

In the future and with the growing digitization, it will be necessary to have a solid practice of how to handle huge amounts of personal and health data in the long term. Based on this, if it is correctly anonymized, population statistics or even reliable indexes about trends can be constructed that, used in the right way, can help improve quality of life.

REFERENCES

Akyildiz, I., Melodia, T. and Chowdury, K. (2007), “Wireless multimedia sensor networks: A survey”, *IEEE Wireless Communications*, Vol. 14 No. 6, pp. 32–39.

Andreasen, MM and Hein, L. (1987), *Integrated Product Development*, IFS-Springer Verlag.

Ashibani, Y. and Mahmoud, Q.H. (2017), “Cyber physical systems security: Analysis, challenges and solutions”, *Computers and Security*, Elsevier Ltd, Vol. 68, pp. 81–97.

Benaloh, J., Chase, M., Horvitz, E. and Lauter, K. (2009), “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records”, *The ACM Cloud Computing Security Workshop*, pp. 343–362.

Burmeister, C., Luettgens, D. and Piller, F.T. (2015), “Business Model Innovation for Industrie 4.0: Why the ‘Industrial Internet’ Mandates a New Perspective”, *SSRN Electronic Journal*, No. January, available at:https://doi.org/10.2139/ssrn.2571033.

Cross, N. (2001), “Designerly Ways of Knowing: Design Discipline Versus Design Science”, *Design Issues*, Vol. 17 No. 3, pp. 49–55.

Deloitte. (2018), *European Health and Fitness Market Introduction*, available at: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/consumer-business/European Health and Fitness Report_2018_extract.pdf.

Faller, C. and Feldmúller, D. (2015), “Industry 4.0 learning factory for regional SMEs”, *Procedia CIRP*, Elsevier B.V., Vol. 32 No. Clf, pp. 88–91.

Fan, S., Lau, R.Y.K. and Zhao, J.L. (2015), “Demystifying Big Data Analytics for Business Intelligence Through the Lens of Marketing Mix”, *Big Data Research*, Elsevier, March.

Fan, T. and Chen, Y. (2010), “A scheme of data management in the Internet of Things”, *2010 2nd IEEE International Conference on Network Infrastructure and Digital Content*, pp. 110–114.

Frayling, C. (1993), “Research in Art and Design”, *Royal College of Art Research Papers*, Vol. 1, p. 9.

Guérineau, B., Rivest, L., Bricogne, M., Durupt, A. and Eynard, B. (2018), “Towards a Design-Method Selection Framework for Multidisciplinary Product Development”, *Design Conference 2018*, pp. 2879–2890.

ISO. (2016), “ISO / IEC CD 30141 : Text of CD 30141”, *Information Technology - Internet of Things Reference Architecture (IoT RA)*.

Jammes, F. and Smit, H. (2005), “Service-oriented paradigms in industrial automation”, *IEEE Transactions on Industrial Informatics*, Vol. 1 No. 1, pp. 62–70.

Jokinen, J. and Lastra, J.L.M. (2016), “Industrial monitoring and control approach for dynamic and distributed intelligent systems”, *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, IEEE, pp. 1–7.

Kagermann, H., Wahlster, W. and Helbig, J. (2013), “Recommendations for implementing the strategic initiative INDUSTRIE 4.0”, *Final Report of the Industrie 4.0 WG*, No. April, p. 82.

Khan, R., Khan, S.U., Zaheer, R. and Khan, S. (2012), “Future internet: The internet of things architecture, possible applications and key challenges”, *Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012*, pp. 257–260.

King, N.J. and Raja, V.T. (2012), “Protecting the privacy and security of sensitive customer data in the cloud”, *Computer Law and Security Review*, Elsevier Advanced Technology, Vol. 28 No. 3, pp. 308–319.

Kiritsis, D. (2011), “Closed-loop PLM for intelligent products in the era of the Internet of things”, *CAD Computer Aided Design*, Elsevier Ltd, Vol. 43 No. 5, pp. 479–501.

https://doi.org/10.1017/dsi.2019.211 Published online by Cambridge University Press

Lasi, H., Fettke, P., Kemper, H.G., Feld, T. and Hoffmann, M. (2014), “Industry 4.0”, *Business and Information Systems Engineering*, Vol. 6 No. 4, pp. 239–242.

Lee, I. and Lee, K. (2015), “The Internet of Things (IoT): Applications, investments, and challenges for enterprises”, *Business Horizons*, “Kelley School of Business, Indiana University”, Vol. 58 No. 4, pp. 431–440.

Li, L. (2017), “China’s manufacturing locus in 2025: With a comparison of ‘Made-in-China 2025’ and ‘Industry 4.0’”, *Technological Forecasting and Social Change*, Elsevier, Vol. 135 No. February 2017, pp. 66–74.

Li, L., Su, F., Zhang, W. and Mao, J.Y. (2017), “Digital transformation by SME entrepreneurs: A capability perspective”, *Information Systems Journal*, No. February 2016, pp. 1129–1157.

Liu, J., Wang, Q., Wan, J. and Xiong, J. (2012), “Towards real-time indoor localization in wireless sensor networks”, *Proceedings - 2012 IEEE 12th International Conference on Computer and Information Technology, CIT 2012*, pp. 877–884.

MacKenzie, C.M., Laskey, K., McCabe, F., Brown, P.F. and Metz, R. (2006), “Reference model for service oriented architecture”, *Public Review Draft 2*, Vol. 1 No. October, pp. 1–31.

Matt, C., Hess, T. and Benlian, A. (2015), “Digital Transformation Strategies”, *Business and Information Systems Engineering*, Springer Fachmedien Wiesbaden, Vol. 57 No. 5, pp. 339–343.

Michelson, B.B.M. and Links, E. (2011), “Event-Driven Architecture Overview 2011”, *Architecture*.

Michelson, B.M. (2006), “Event-driven architecture overview”, *Patricia Seybold Group*, Vol. 2.

Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I. (2012), “Internet of things: Vision, applications and research challenges”, Ad Hoc Networks, Elsevier B.V., Vol. 10 No. 7, pp. 1497–1516.

Phelan, D. (2017), “The One Thing Nobody Has Told You About Apple Watch Series 3”, Forbes Online, September.

Porter, M.E. and Heppelmann, J.E. (2014), “How smart, Connected Products Are Transforming Competition”, *Harvard Business Review*, No. November, pp. 97–114.

Shamsuzzoha, A.H.M., Ehrs, M., Tenkorang, R.A., Nguyen, D. and Helo, P.T. (2013), “Performance evaluation of tracking and tracing for logistics operations”, *International Journal of Shipping and Transport Logistics*, Vol. 5 No. 1, p. 31.

Stigestadh, G. and Moberg, F. (2018), “Big Data, På Gott Och Ont: GDPR Som Stöd För Den Enskilde Individen”, Lunds universitet.

Szolovits, P., Doyle, J. and Long, W.J. (1994), “Guardian Angel: Patient-Centered Health Information Systems”, *Technical Report MIT/LCS/TR-604*, Cambridge, Massachusetts.

Takata, S., Kimura, F., Van Houten, F.J.A.M., Westkämper, E., Shpitalni, M., Ceglarek, D. and Lee, J (2004), “Maintenance: Changing role in life cycle management”, *CIRP Annals - Manufacturing Technology*, Elsevier, January.

Tankard, C. (2016), “What the GDPR means for businesses”, *Network Security, Elsevier Advanced Technology*, Vol. 2016 No. 6, pp. 5–8.

Ten, C.W., Manimaran, G. and Liu, C.C. (2010), “Cybersecurity for critical infrastructures: Attack and defense modeling”, *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans*, Vol. 40 No. 4, pp. 853–865.

Ustundag, A. and Cevikcan, E. (2018), “Industry 4.0: Managing The Digital Transformation (Springer Series in Advanced Manufacturing)”.

Vermersan, O. and Friess, P. (2010), *The Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*, Vermersan, O. and Friess, P. (Eds) River Publishers, New York, NY, available at:https://doi.org/10.1007/978-1-4419-1674-7.

Xu, L. Da, He, W. and Li, S. (2014), “Internet of things in industries: A survey”, *IEEE Transactions on Industrial Informatics*, Vol. 10 No. 4, pp. 2233–2243.

https://doi.org/10.1017/dsi.2019.211 Published online by Cambridge University Press