Computer Science and Information Systems 18(1):323–350 https://doi.org/10.2298/CSIS200922057K

Incorporating privacy by design in Body Sensor Networks for Medical Applications: A Privacy and Data Protection Framework

Christos Kalloniatis[1], Costas Lambrinoudakis[1], Mathias Musahl[2], Athanasios Kanatas[1], and Stefanos Gritzalis[1]

[1]Dept. of Digital Systems, University of Piraeus,
GR 18532, Piraeus, Greece
{chkallon,clam,kanatas,sgritz}@unipi.gr
[2]German Research Center for Artificial Intelligence,
67663 Kaiserslautern, Germany
mathias.musahl@dfki.de

Abstract. Privacy and Data protection are highly complex issues within eHealth/M-Health systems. These systems should meet specific requirements deriving from the organizations and users, as well as from the variety of legal obligations deriving from GDPR that dictate protection rights of data subjects and responsibilities of data controllers. To address that, this paper proposes a Privacy and Data Protection Framework that provides the appropriate steps so as the proper technical, organizational and procedural measures to be undertaken. The framework, beyond previous literature, supports the combination of privacy by design principles with the newly introduced GDPR requirements in order to create a strong elicitation process for deriving the set of the technical security and privacy requirements that should be addressed. It also proposes a process for validating that the elicited requirements are indeed fulfilling the objectives addressed during the Data Protection Impact Assessment (DPIA), carried out according to the GDPR.

Keywords: privacy protection, data protection, GDPR, Framework.

1. Introduction

The medical developments and the rapid changes in the Europe demographics are increasing promptly the average age of European citizens. These changes pose several challenges for EU future and require urgent policy responses in order for EU to organize appropriate healthcare solutions addressing to a growing number of individuals [1]. This necessity is leading to a broader enhancement and application of Information and Communication Technology (ICT) within healthcare systems, emerging the establishment of the eHealth systems, where services and tools, based on ICT, can improve prevention, diagnosis, treatment and monitoring [2], as wells as the healthcare-related data management and exchange [3]. Plenty of research approaches in the domain of eHealth systems put special emphasis on the design of remote health-monitoring systems and equipment [1, 4-5], leading medical and public health practice to a large-scale adoption of mobile medicine/mHealth [6]. mHealth is supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants and other wireless devices that provide remote access to health services and users. Especially, body-worn monitoring devices and wireless medical sensor networks are on emerge [1,7]. Wireless medical sensor networks are considered of major impact on e-healthcare [8], providing plenty of benefits such as: ease of use, reduced risk of infection, reduced risk of failure, reduced patient discomfort, enhancing of mobility and low cost of care delivery, while allowing the data of a patient's vital body parameters to be collected by wearable or implantable biosensors, such as heart rate monitors, pulse oximeters, spirometers and blood pressure monitors [7]. Despite the fact that medical apps enable remote health monitoring, they are also raising security and privacy concerns due to the basic personal e-health systems' functionalities, such as: personal data storage and processing, personal data exchange with other third-party systems (personal or institutional), integration of (personalized) public data, exporting personal data for statistical use and exchange of private personal data messages [5]. These are considered to be some of the most important barriers for the fully implementation of e-healthcare solutions [9]. The "privacy paradox" significantly affects the effectiveness of existing solutions, since most of the users are concerned about the protection of their medical data and at the same time, they agree on using these devices, since they are vital for their health [10]. There are also cases of users who are not aware of the potential harm that can be caused from a deliberate or an accidental threat. In general, privacy and personal data protection constitutes a major concern for e-health consumers [11], affecting wearables adoption. Indicatively, 82% of the respondents to a PricewaterhouseCoopers (PwC) survey reported that they are worried that wearable technology will invade their privacy [12]. Therefore, users' acceptance is strongly dependent on trust. Additionally, the principles enforced by the new General Data Protection Regulation (GDPR) put special emphasis on the protection of citizens' privacy by elevating the obligations of the parties collecting, distributing and processing users' data [13]. To this respect, privacy engineering has gained much attention in Europe, and lately across the Atlantic, as a significant part of the system development process, where security and privacy software engineers along with developers should define the principles in the form of technical requirements that need to be satisfied in order for the system to ensure a minimum level of security and being trustworthy for the citizens [14]. Thus, as far as the e-health and m-health systems concern, which are critical due to the sensitivity of the collected and distributed data within them, security and privacy have been always of immense interest to research communities. However, most of previous researches [15-16-17-18] focusing on the security and privacy frameworks for m-health applications that provide users with more control regarding the use of their sensitive health data within then, does not combine the benefits of privacy engineering along with the new technical and legal aspects of GDPR legislation in medical wearables applications, while some interesting approaches, aiming to highlight the privacy requirements of the m-health applications within the context of GDPR, focus only on specific target group of patients, such as Mustafa, Pflugel & Philip's [9] study regarding patients suffering from Chronic Obstructive Pulmonary Disease, excluding larger or healthier target groups in which m-health applications are also addressed.

In this regard, BIONIC, a pioneering system, funded by the European Union's Horizon 2020 research and innovation program under Grant Agreement No 826304, going beyond previous research, introduces medical wearables to the workplace in order to form a strong paradigm of how wearable technology can respect the user's rights to privacy, maintaining the highest standards in terms of privacy and data protection and to familiarize many users with these rights and their ability to control the sharing of their data. Its mission has been manifold, aiming at the development of a) a holistic, unobtrusive, b) autonomous and c) privacy preserving platform for real-time risk alerting and continuous persuasive coaching, enabling the design of workplace interventions adapted to the needs and fitness levels of specific ageing workforce. To that aim, it provides a Privacy and Data Protection Framework, which suggests the appropriate steps so as the technical, organizational and procedural measures for the satisfaction of the security, privacy and legal requirements. BIONIC, through this Framework, covers the gaps in existing methodologies, focusing on the increase of the end users' trustworthiness to the developed software. More specifically, it provides the combination of privacy by design principles with the newly introduced GDPR requirements in order to create a strong elicitation process for deriving the set of technical requirements that should be addressed, while it proposes a process for validating that the elicited requirements are indeed fulfilling the objectives addressed during the Data Protection Impact Assessment (DPIA), carried out according to the GDPR.

The rest of the paper is organized as follows. Section 2 presents the issue of privacy within e-Health/m-Health Systems, while subsection 2.1 focuses especially on privacy preserving schemes under GDPR. In subsection 2.2 Privacy by Design approaches are presented and their relevance with GDPR. Section 3 briefly presents the BIONIC system and its main features while 4 presents the proposed privacy Framework. Finally, Section 5 concludes our work.

2. Privacy within e-Health/m-Health systems

The wide prevalence and utilization of mobile medical devices in the area of eHealth, collecting health data about individuals and performing monitoring and managing of health-related information, raises serious challenges for the eHealth systems in order to support effectively privacy protection of individuals' personal data and access control [1]. Considering that health information is a particularly sensitive subset of personal information, accompanied with ethical considerations, privacy is established as one of the main requirements of eHealth area [19]. Since within eHealth there are multiple collaborating parties coming from a diverse range of authorities under different managements, privacy concerns derive from the sensitivity of the data that the applications access, handle, store, use and from how/with who it is shared, indicating highly numbered security weaknesses and privacy threats [20]. In this regard, Omoogun et al. in [21] support that different sensors, used for monitoring within mHealth, are designed without taking into consideration security and privacy aspects and therefore are vulnerable to numerous types of attacks, or subjects to data leaks. Challenges and threats such as eavesdropping, impersonation, data integrity, data breach and collusion pose even more provocations for the privacy-aware management of the patients' personal data to control pervasive tracking and profiling [22]. Additionally, users' privacy concerns may be a great barrier to the acceptance of the eHealth technology [1,23] and in order to adopt socially acceptable health services, the security and privacy issues need to be analyzed and addressed [3]. Privacy is a highly complex issue within eHealth systems, which are designed to meet specific requirements deriving from the organizations and providers who use them, as well as from the variety of legal obligations deriving from GDPR and privacy enforcement rules that dictate protection rights of data subjects and responsibilities of data controllers [3]. Therefore, an adequate framework is needed in order to balance different levels of privacy regarding their data, considering, for providing the appropriate technical solutions, not only the individuals' requirements and needs and the health care service providers' and data controllers' purposes, but also the different sets of regulations for privacy. However, such a Framework in previous literature is lagging behind, as it will be presented in the following subsection.

2.1. Privacy approaches within eHealth systems under GDPR

GDPR provides new definitions regarding individuals' data. Specifically, as far as health/medical data concerns, in GDPR (Article 4-15) is defined as the "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status". Additionally, it is considered to be of sensitive ones according to the Article 8 paragraph 1 of the Directive 95/46/EC and as a special category of personal data according to GDPR (Article 9). Therefore, special emphasis, as well as the explicit consent of data subjects, is required when processing them. As [24] argues, the applying of the principles of privacy by design, in order to build security and privacy into the systems, could be a solution to the privacy concerns regarding e-health data. Hence, despite the importance of privacy protection of health/medical data within e-Health area, which has been recognized in a number of works [20,23], to our best knowledge not many research works approach it from the outset of the design or take into consideration the necessity of compliance with new GDPR requirements. Privacy needs to be considered during systems design and implementations [25]; otherwise as [1] support, plenty of limitations are posed on the system's deployment, leading to a not adequate data protection solution for the users. Additionally, literature [26] highlights that previous research mainly focuses on the security issues and especially on cryptographic techniques (e.g. [7]) that perform client-side encryption of data to protect against untrusted service providers, solving fragmentary some aspects within mHealth, while privacy engineering in this area is lacking. Milutinovic & De Decker in [1] p.53 have presented a list with the privacy requirements that an eHealth system should fulfill in order to be compliant with the legal and ethical requisites and gain a wider acceptance as following: a) personal and recognizable information should be protected by strict access control policies, b) non-medical professionals should not access to patients' information, excluding authorized guardians, c) data access should be logged securely, so that later auditing is enabled and d) flexible control access policies should be revoked or expanded. From a technical aspect, Sawand & Khan in [27] p.534 propose that eHealth monitoring systems should fulfill the following security requirements: a) Trusted Authority, which generates public and secret key parameters, is responsible for the issuing keys, granting as well differential access rights to the patients' based on their attributes and roles, b) cloud service provider, in order to provide secure communication mechanisms, as well secure data storage, processing and retrieval according to the access rights of the requesters, c) registered user, referring to the patients' registration to the trusted authority in order to define their data access and the attributes based on specific access policy and d) data access requester, referring to a doctor, a pharmacist, a researcher and a health care service, whose access rights and are defined by the patient who use the eHealth monitoring system.

Pirbhulal et al. in [28] pp.385-386 suggest a more analytic context regarding remote healthcare systems, including not only security, but also privacy requirements as follows: a) data confidentiality, in order to prevent any disclosure during any data transmission, b) data integrity, in order to protect original data from external attacks, c) data availability, in order for the data to be available to legitimate and authenticated nodes/users, d) data freshness, ensuring that data is updated and no one authorized or not can replay old data, e) scalability, in order to reduce latency and control computational and storing overheads and g) secure key distribution, in order to allow encryption and decryption operations for accomplishing the estimated security and confidentiality. As the previous work, the study of [29], as far as the safety of Wireless Body Area Network systems concern, supports the data confidentiality, the data integrity, data freshness and the secure management requirements, but it also maintains a) the availability of the network, in order to provide at all the times access to patients' information both to healthcare professionals and patients, e.g. in case of an emergency health issue, b) data authentication, by which the applications should be capable to verify that the information is sent from a known trust center, c) dependability, referring to the systems' reliability, since data errors may lead to health-threating issues, d) secure localization, in order to prevent attackers to transmit improper details, such as fake signals about the patient's location, e) accountability, in order for the individuals' personal information to be secured, f) flexibility, referring to the individuals' flexibility of designating the control of their medical data and g) privacy rules and compliance requirement, referring to the need to secure private health information by setting privacy measures, such as rules/polices regarding the right to access to patients' sensitive data, since several regulations are enlisted for health care services. In this regard, ambitious current approaches, such as the study of [30], which developed a framework called Privacy-Protector to preserve the privacy of patients' personal data in IoT-based healthcare applications by presenting a secret sharing scheme, which devises the patients' data and stores it in several cloud servers for optimizing the secret share size and supporting exact-share repairs, while still keeping the advantages of the previous scheme, or previous studies [15-16], focusing on the security and privacy frameworks for m-health applications that provide users with more control regarding the use of their sensitive health data within them, are not taking into consideration legal aspects of privacy that are mandatory for eHealth environments.

Especially, as far as compliance with GDPR concerns, until now few research works consider the new requirements. Authors in [25] focused their study on openEHR, a standard that embodies many principles of secure software for electronic health record and provided a list of requirements for a Hospital Information Systems compliant with GDPR, in order to examine to what extent, the openEHR may be a solution for the compliance to GDPR. Although, matches were found, the results showed that the related to the organizational processes GDPR requirements, hardly could be met by any EHR specification standard. Iwaya's et al. study in [26] p.46 on mobile health data collection systems that have been used by community health workers, provides a list with specific privacy recommendations associated with the privacy principles and challenges emerged from the systems under the GDPR. This includes: a) Transparency-enhancing tools, guidelines for purpose specification, fine-grained access control, anonymization and pseudonymization, data validation and integrity and automated data deletion measures for the principle of Data Quality within mHealth, which refers to the process of transparent data, the purpose specification, the data minimization, the data accuracy and integrity and the data retention, b) Obtaining informed consent and check validity of consent measures for the principle of Legitimate Process, which refers to a legitimate data processing of sensitive data that takes into consideration other relevant legal basis for using personal data, c) Accurate, up-to-date, easily found and understandable information about data controller, purpose, recipients measures for the principle of Information Right of Data Subject, d) TETs for individualized information (e.g., privacy dashboards) and timely response to data subject's information requests and rectifications for the principle of Access Right of Data Subject, e) Provision of interfaces for objections and timely responses measures for the principle of Data Subject's Right to Object, f) Authentication and authorization, secure communication and storage and logging measures for the principle of Security of Data, which refers to personal information confidentiality, integrity and availability and the detection and communication of personal data breaches and g) Compliance with notification requirements and logging measures for the principal of Accountability, which refers to the implementation of safeguard data protection and compliance with data protection provisions to subjects, general public and supervisory authorities. Finally, [9], under the EU project WELCOME, studied the privacy of the mHealth applications for patients suffering from Chronic Obstructive Pulmonary Disease, and proposed the following privacy requirements within the context of GDPR: a) data patients' right to access and modification or erase by the applications in any case of inaccurate measurement, b) patients' right to information for the collected data by the applications and the time period of processing, c) limitation of collected data in accordance to the functionality of the applications in combination with the respective permissions, d) patients' fully awareness of the security measures regarding data storage or transmit to other third parties, e) patients' right to information regarding the risk and benefits of an m-health application, g) the prohibition of using collected data for marketing or profiling purposes, stated on an informed medical consent, h) appropriate security mechanisms for mobile devices, providing access only to authorized users with the proper authentication, i) access controls in order for authorized users and mobile devices to be authenticate, k) integrity of the medical data provided by the applications, l) proper security mechanisms for data storage. However, this interesting approach focuses only on a specific target group of patients, excluding larger or healthier target groups in which m-health applications are also addressed.

2.2. Privacy by Design Schemes under GDPR

Privacy by Design, as it was supported by [31], has been incorporated into the GDPR and it is considered to be the most appropriate approach for meeting the privacy and data protection expectations to a large scale, since it offers realistic solutions in order for legal requirements to be combined with the technical ones [24]. In this regard, the data controllers and processors are obligated to enforce the appropriate technical and organizational measures and procedures to ensure the protection of the data subjects' rights and to be compliant with data protection principles [32]. As [33] support, data protection by design should be managed after the specification of the processing purposes and during the processing itself. The controller is obligated to ensure the security of the system, as well as to enhance Protection Impact Assessment into the architecture of the system in order to safeguard adequately by default individuals' rights regarding their data. Hence, the proposed privacy principles by [31] have been under criticism regarding its difficulties to be implemented into the system requirements [34-35]. Therefore, the stated necessity to embed the technological aspects of privacy within the regulatory field [14] and to bridge GDPR privacy regulations with technical solutions is even more emerged, in order for privacy engineering practice to confront more easily the privacy concerns and the compliance to the Regulation [36-]. To address that need, [37], aiming at translating existing GDPR requirements into technical solution templates for compliant services, defined a catalogue of three types of privacy control patterns, namely: a) general privacy control patterns, b) patterns that affect the data subjects' rights and c) patterns regarding data controllers and processors' obligations. Although authors support that the proposed patterns provide generally applicable privacy guidelines, it is important to note that their work focused only on the following specific GDPR principles, Transparency and Traceability, Purpose Limitation, Data Minimization, Accuracy and Storage Limitation, since the principles of Lawfulness, Fairness, Integrity and Confidentiality and Accountability are considered not to be fulfilled by technical measures in a manageable time limit. Authors in [36] presented an approach based on model transformations, aiming to enable a more constructive approach to privacy by design under the principles of GDPR. Although, their work consists an interesting approach to bridge privacy legal and technical field, it focuses only on limited requirements, such as purpose limitation, or accountability of the data controller and consequently it presents specific technical privacy properties. In this sense, [34] supports that the need of holistic privacy patterns is emerged in order for the systems to achieve compliance with the new GDPR regulation, while even the notable privacy approaches, such as LINDDUN, a risk-based method for modelling privacy threats in order to support software developers in identifying and addressing privacy threats early during software development, should be combined with other goal-oriented approaches so as to be effective. [38] introduced an interesting privacy ontology that models the GDPR main conceptual cores as following: data types and documents, agents and roles, processing purposes, legal bases, processing operations, and deontic operations for modelling rights and duties, focusing on the analysis of deontic operators in order to manage the checking of compliance with the GDPR obligations. However, the study has not yet achieved to integrate the different levels of semantic representation for multiple goals and the analysis was restricted only to the Right to Data Portability. Finally, the current EU project PDP4E [14] aims to integrate data protection approaches such as LINDDUN, PRIPARE and PROPAN into systems engineering methodologies and process models, specializing them to operationalize GDPR compliance. Although, authors recognize the impact of goal-driven approaches, they focus mainly on risk-based approaches as LINDDUN and PROPAN, a threat identification method, as well as on

PRIPARE methodology, derived from a previous EU project [39], which has combined articulations of risk-based methods and privacy by design principles for implementing privacy in practice. Therefore, no one pure goal- oriented methodology is considered, despite the fact that GDPR is considered as a purpose-oriented approach [34]. Thus, it is arguable to maintain that a Privacy by Design, goal-oriented privacy methodology could effectively support the implementation of the privacy technical prerequisites that the GDPR poses itself. With respect to this and taking into account that Privacy Safeguard-PriS [40], a goal-driven Privacy by Design engineering methodology, was considered as an effective one for GDPR-compliant socio-technical systems [41], lacking thus in incorporating legal aspects, we provide the ground for PriS to be implemented in our Framework, by making provision for the legal concepts that GDPR has imposed. To address that, we emphasize on the interrelation between GDPR approach and PriS methodology in a high level. PriS considers privacy requirements as organisational goals (privacy goals), which constraint the causal transformation of organisational goals into processes, and by privacy-process patterns describe the impact of privacy goals to the affected organisational processes. In particular, eight types of privacy goals are recognised, namely: Authentication, Authorisation, Identification, Anonymity, Pseudonymity, Unlinkability, Data Protection and Unobservability. At first, PriS was designed to support traditional privacy-aware information systems. Thus, cloud computing environments introduced a number of new privacy related concepts, leading to an extended version of PriS [42-43] that provides a new set of privacy requirements along with the ones already stated, namely, undetectability, isolation, provenanceability, traceability, interveanability and accountability. The next step is the modelling of the privacy-related organisational processes. These processes aim to support the selection of the system architecture that best satisfies them. Therefore, PriS provides an integrated way-of-working from high-level organisational needs to the IT systems that realize those [40]. On the other hand, GDPR aims a) to promote data collecting and processing organisations' and companies' work, by introducing specific rules and requirements as a primary goal of the organizations, as well as by providing direct instructions for the implementation of data protection, dealing thus with several complex aspects, such as company-level awareness raising, nature – scope - context and purposes of processing, adoption of both organizational and technological data protection processes and measures at the start of a project, cost of implementing the protection measures and documentation of processing operations [32-33] and b) to provide EU citizens with further control on their personal data, while minimizing the threats against their data rights and freedoms [32]. Consequently, the conceptual association with PriS methodology is more than clear, since PriS promotes a set of expressions based on which the whole processes of an organization are considered, starting from the goal level and leading to the selection of the appropriate implementation techniques.

3. The BIONIC Project

BIONIC is a pioneering system, funded by the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 826304, which provides industry with a unified methodology focused on the perspective of ageing in the workplace, by supporting its application in research.

Its mission was manifold, aiming at the development of a holistic, unobtrusive, autonomous and privacy preserving platform for real-time risk alerting and continuous persuasive coaching, enabling the design of workplace interventions adapted to the needs and fitness levels of specific ageing workforce. Since many typologies of industry jobs are physically demanding, it is necessary to support the aging workforce with appropriate tools that can help them to stay at their jobs, assessing the potential impacts of their work activities on their health, and recommending exercises to mitigate those impacts and promote healthy and active lifestyles. In this regard, the BIONIC solution constitutes a valuable tool for achieving these objectives, bringing medical wearable technology into a new paradigm accordingly to the World Health Organisation principles for e-Health and m-Health, by integrating sensor modules in multi-purpose, configurable Body Sensor Networks (BSNs) introducing key enablers of user acceptance based on value, comfort, confidence and trust.

Configurable BIONIC Body Sensor network has been originally conceived as a platform combining a wide variety of connected sensors enabling the build-up of a real-time holistic data model of the human body, by capturing static and dynamic whole-body information, such as e.g., body posture, gait, running style, etc., possibly combined with key bio-signals, such as body temperature, heart rate, and environmental signals. Dynamic monitoring of overall body posture integrated into everyday or work clothing will significantly promote the wide adoption of motion tracking wearables, by eliminating the need to attach sensing devices firmly to the body, thus affecting comfort and possibly impeding movement during work or everyday / physical activity. Existing commercial wearables with open APIs (e.g., smartwatches, sole pressure sensors) will also be integrated to enable a holistic integrated continuum of data to derive self-quantification information. Depending on the specific chronic MSD condition, body-part specific BSN modules in the form of e.g., belts or bandages (for monitoring lower back and knee chronic MSD) will be developed. Detailed monitoring of these body parts will be based on innovative localized biomechanical models, focusing on age-induced constraints and chronic impairments (age adapted body - part specific models). Additionally, BSN allows freedom in the selection and positioning of the sensors on the body, depending on the requirements of the specific application (fitness, performance, medical, ergonomics etc.), while it enables the development of customizable or even multi-functional wearables, i.e. networks with inherent redundancy of sensors, with their functionality configured by application software.

Another major key innovation relates to the concept of AI on a chip, i.e. embedding predictive Artificial Intelligence algorithms in the Body Sensor Network (BSN). Raw data pre-processing at the source prevents immense flows of data being transmitted to remote gateways. Feature extraction at the source will result in informative and non-redundant features, ready to be fed into artificial neural networks. The combination of such machine learning algorithms with biomechanical model-based estimation will allow for deducing relevant and interpretable parameters for efficient real-time, in-field and long-term personalized risk/physical strain and recovery assessment from individual sensor data.

Therefore, continuous personalized on-site assessment of the real capacity of ageing workers, using BIONIC wearables, will allow to derive valuable information both at a personal, as well as at a statistically relevant age dependent level, associating the imbalances and risks with design criteria and recommendations that facilitate the selection and adaptation of appropriate positions, while ageing workers will keep their personal data private. Feedback to the user will be provided in real-time through the BSN to actuators such as haptic, acoustic, visual systems. Communication to external Network is optional and under control of the user, who can decide case by case who will get access to the results or the raw data. To fulfil that, an integrated prototype of monitoring and data presentation software will be used, including three different applications targeting: a) workers, where self-monitoring application providing access to their movement data such as daily and archived statistics, risks identified and exercise recommendations, incorporating advanced UX and intuitive ways of human computer interaction to accommodate ageing users' requirements, ensuring optimum comprehension of the relevant warnings and advice and maximizing the preventive effect of the system, b) managers: where ergonomic risk assessment applications provide real-time feed of selected worker movement information to construction site managers to allow for injury prevention as well as periodical reports, including assessment results and recommendations for workplace interventions and c) doctors, where specially designed application provide doctors with access to workers movement and health information, efficiently structured and prioritized based on ergonomic risk, allowing doctors to support the workers in a timely manner.

In this sense, BIONIC introduces Body Sensors Networks in the everyday life to a market segment, which is not so easy for wearable electronics solutions to reach, i.e. older individuals. BIONIC's strong focus on usability and privacy aspects (e.g. HCI, gamified coaching, GDPR principles) will bring these users the confidence and trust to try more similar solutions which can improve their quality of life. It will also convince them in practice that such technology is not only for the gadget savvy youths but can provide real value related to their health and wellbeing. This integrated methodology within a broader procedure is able to facilitate aspects such as, the management of experience in companies, the transfer of knowledge or the transition to retirement, that are relevant aspects for improving companies' productivity and competitiveness. Figure 1 presents the concept diagram of BIONIC.

The BIONIC project supports two main types of services. The first is conducted during the working hours where every worker receives live feedback form the Body Sensor Network that he/she wears while the second is performed during leisure time with the support of a "lighter" Body Sensor Network consisting of less sensors than the full BSN.

More specifically, the full BSN network consists of a set of sensors attached on the workers workwear. This workwear includes a t-shirt, a helmet/cap and a trouser that the worker wears during his/her work. These sensors provide raw data to an AI chip (located in the trousers) which generates processed data related to the workers current health status. The AI chip interacts with the worker's smart watch mostly for getting additional information for the worker's statues (e.g., heart rate) and for sending notifications to the worker (e.g., alarm messages). Also, the worker possesses a mobile device for handling his/her data and interacting with BIONIC apps as well as for conducting the coaching exercises at home.

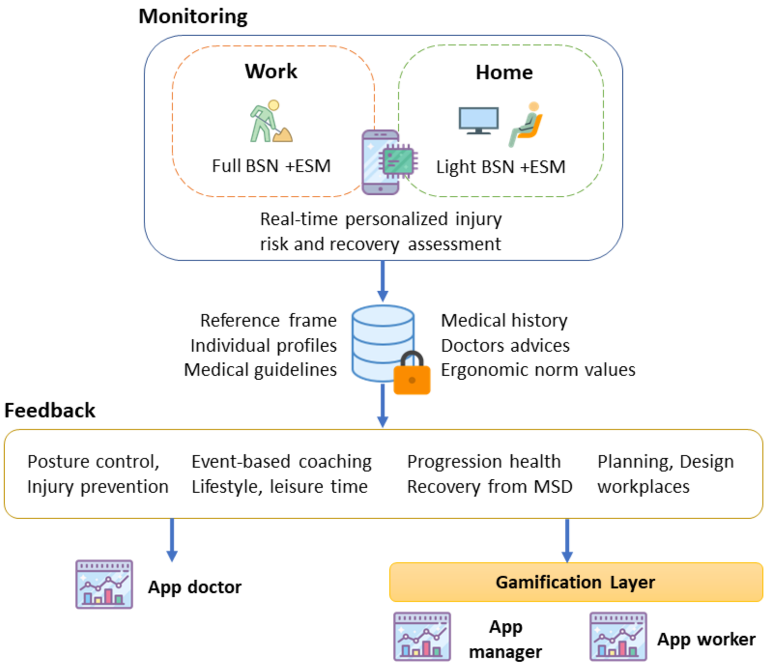

Fig. 1. BIONIC Data Flow

The "light BSN" is the body sensor network consisting of the worker's smartwatch, some Inertial Measurement Units (IMU) sensors and a mobile device and is used from the worker during his leisure time (not working hours) to exercise himself/herself based on the coaching app of the BIONIC project. Beside the use of the specific app the light BSN monitors worker's ergonomic and health data for capturing his/her habits and moves outside the working environment in order to prevent unwanted situation and/or to better advise the worker during the day.

The proposed BIONIC data flow is presented in the following figure. The full BSN and the light BSN parts are also visible in figure 2.

Based on the aforementioned figure BIONIC collects all processed data (as exported from BSN) in a secure storage in order for the developed apps to have access on and mainly provide the necessary feedback to the worker. The data produced by the light BSN are stored in the secure storage repository if the worker wishes to do so. For R&D purposes and only for the duration of the project the raw data produced by the BSN network are stored in an anonymised form in a separate database called "Research Data" in the respective figure.

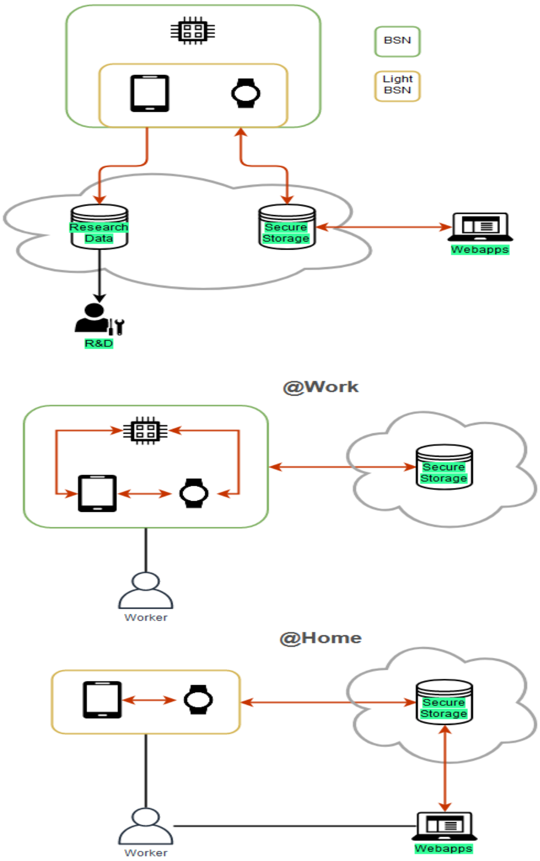

Fig. 2. BIONIC Data Flow

Regarding the types of data collected from the BSN and light BSN networks are mainly the following:

- Kinematic data, probably at IMU sample rate (e.g., joint angles)
- Kinetic data, probably at lower sample rate (e.g., vertical ground reaction force, ground contact information, external load indicators)
- Depending on chosen ergonomic tools:
  - timestamped detected events (e.g., picking something up, body positions) and repetitions
  - possibly ergonomic scores
- Physiological data (Heart rate, blood pressure, body temperature)

Following the context of BIONIC the aim of this paper is to present an efficient Data Protection Framework considering both the technical as well as the legal and organizational requirements for ensuring the safety and security of the workers. The next section presents the proposed Privacy and Data Protection Framework.

4. The Privacy and Data Protection Framework

BIONIC, considering both GDPR principles and PriS concepts, proposes a flexible and efficient GDPR Compliant Personal Data and Privacy Management methodology in order to ensure the security, safety and privacy aspects of using holistic and unobtrusive Body Sensor Networks on ageing workforce, which is going to employ the system in their daily tasks. The Framework ensures that GDPR principles, such as purpose limitation, data minimization, accuracy, accountability, the lawfulness of processing, the user consent, are fully satisfied. In this regard, the medical wearable applications will respect all the data owners' rights (ageing workers), such as their rights to object to the storage/processing of their information, their right to be forgotten, their right to restriction of processing, while the obligations of the intermediate users, such as occupational health professionals, production managers, and in general all the professional profiles that manage the system and potentially exploit all the data generated within BIONIC are specified. Finally, all necessary technical, organizational and procedural measures for the satisfaction of the eliciting security and privacy requirements are considered and thus enhancing confidence and trust among all stakeholders. It comprises of the following four stages:

Stage 1: Personal Data handling processes elicitation

The purpose of this step is to define the perimeter of the Personal Data handling processes, by capturing, reviewing and formalizing the following issues: a) The categories of the personal data processed, b) The categories of the data subjects, c) The purposes of each processing activity, d) The identification of high risk data processing activities, e) The legal basis of each processing activity (e.g. contract and/or consent and/or legitimate interest and/or statutory obligation), f) The categories of recipients to whom the personal data are disclosed, g) The envisaged time limits for erasure of the different categories of data – if they exist, h) The existing technical and organizational measures for the protection of personal data.

To this end, a Questionnaire for Accessing GDPR Compliance is designed and implemented. The objective of this questionnaire, addressed to BIONIC respective stakeholders, is to identify, through a systematic procedure, the aforementioned information for each purpose of data processing separately. The questionnaire includes seven items, requiring open responses, regarding the following issues: a) Short Description for the purpose of processing, b) Legal Basis for the purpose of processing, including the subcategories i) Law, ii)User / patient consent, iii) Contract, c) The data involved in serving the specific purpose of processing, including the subcategories i) General Data, ii) Personal Data, iii) Special categories of Personal Data, d) The necessity of the involved data for serving the specific purpose of processing, e) The sources of collected data, f) The transmission of personal data to third parties, g) The processing of automated decision-making, including profiling. Therefore, its main output concerns the listing of the Purposes of Processing and the Personal Data Categories**.**

Stage 2: Compliance Level on GDPR requirements

During the second stage, it is essential to map the organizational context following the results of stage 1. Therefore, when the above list of information has been compiled, the processing of each personal data category is being reviewed against the GDPR requirements to deduce the existing compliance level, through a GDPR gap analysis.

Topics that are examined are presented indicatively as following: a) lawfulness, fairness and transparency of the personal data processing, b) the processing purpose limitation, the data minimization, c) the consent of the data subjects, d) the personal data storage limitation, e) the measures for personal data protection, f) integrity and confidentiality, g) The readiness of the involved stakeholders to respond to the data subjects' rights' is examined, such as the 'right of access', the 'right to rectification', the 'right to be forgotten', the right to restriction of processing', the 'right to data portability', the 'right to object', h) Information to be provided where personal data have not been obtained from the data subject, i) Automated individual decision-making, including profiling, j) Data protection by design and by default, k) Joint controllers, l) Security of processing, m) Processing under the authority of the controller or processor, n) Tasks of the data protection officer, o) Transfers on the basis of an adequacy decision. Moreover, the readiness of the organization to respond to the data subjects' rights' will be examined. Indicatively the 'right of access' , the 'right to rectification', the 'right to be forgotten', the 'right to restriction of processing', the 'right to data portability', 'right to object'.

Indicative activities that will be performed during the gap analysis include: a) Review of legal basis on which the organization processes Personal Information, b) Review the necessary retention periods per category of Personal Information for various reasons such as, for compliance with a legal obligation, for inquiries of auditing authorities, for legal claims, for public interest etc, c) Review of Privacy Notices, d) Review of the legal basis for marketing services, e) Legal review of all defined internal Personal Information Protection Policies and Procedures, f) Legal Review of sample employment contracts and updating with necessary legal language to allow the processing of employees Personal Information for legitimate business purposes, g) Review of standard consent forms used to collect and record data subject consent for the processing of Personal Information, h) Legal review of standard Intra- and Third-Party contracts, Procurement contracts and Supply Contracts to identify any contractual gaps in relation to Data Protection relevant clauses. If no standard contracts are used, the review will cover key activities, which should at least include all contracts related to identified high risk processing activities, i) Understand the operational policies and procedures for the IT systems, j) Access the efficiency of the organization to protect the data (data protection measures), k) IT and Security Governance review, l) Network architecture review. The main output of this stage concerns a Set of GDPR Compliance Requirements for each identified purpose of Processing.

Stage 3: Security and Privacy requirements elicitation

Security is protection against intended incidents, i.e. incidents that happen due to a result of deliberate or planned act. Security concerns the protection of assets from threats, where these are categorised as "the potential for abuse of protected assets". Whereas, privacy concerns the protection of the assets' owner identity from users that do not have the owner's consent to view/process their data. Risk analysis or equivalently Risk Assessment is the methodology where an IT infrastructure and/or interconnection between computational devices is methodically analysed and the corresponding Security/Privacy threats are identified as long with the specific vulnerabilities and/or potential failures may cause them. Moreover, the goal of a security assessment, is to ensure that necessary security and privacy objectives are integrated into the design and implementation of an architecture. A Vulnerability is defined as a weakness, in terms of security and privacy that exists in from a resource, an actor and/or a goal [17].

Vulnerabilities are exploited by threats, as an attack or incident within a specific context. A Threat represents circumstances that have the potential to cause loss; or a problem that can put in danger the security features of the system [44]. In Stage 3, a Risk analysis, identifying threats, vulnerabilities, data, is conducted in order to deduce attack modelling and threat propagation. The need for such analysis results directly from the GDPR principle of accountability. The analysis assists in the identification and assessment of security and privacy risks and thus in the selection of the appropriate measures to reduce these risks and as such reduce the potential impact of the risks on the data subjects, the risk of non-compliance, legal actions and operational risk. At the end, the privacy by design approach Privacy Safeguard (PriS) is applied to collect all identified security and privacy requirements (Legal, Organizational, Technical), validating that they are indeed expressed in a technically sound manner and ensuring that they can be implemented in the context of the specific system. The requirements elicitation methodology supports threat, vulnerability and attack analysis, reasoning on security and privacy requirements and modelling of the system. PriS was selected for the security and privacy modelling of BIONIC since: i) It consists a privacy by design method, an approach that GDPR sets on its main principles, ii) It is one of the oldest and mostly evaluated privacy by design methodologies, iii) On a conceptual level, GDPR principles' concepts are associated with PriS privacy requirements concepts, iv) It combines stakeholders' needs and goal-driven modelling which is very important due to the purpose-oriented philosophy of the Regulation and v) It can be easily aligned with a risk-based analysis, which is also prerequisite for GDPR. The proposed steps for implementing stage 3 can be described as follows:

Substep1: Identify System Assets and Stakeholders

The purpose of this step is to define the perimeter (boundaries) of the study. A global vision of the components and communications between components will be clarified. At this step, the following data will be collected and formalized: a) Essentials assets of the BIONIC system, b) Functional description of components and relations between components, c) Security issues that need to be addressed by the study, d) Assumptions made if appropriate, e) Existing security rules (law and regulation, existing rules in other studies), f) Constraints (internal or external) from BIONIC system itself. At the end of this step, a clear vision of the components and the links between them will be formalized that are going to be used as input for the risk analysis method.

Substep2: Identify Potential Security and Privacy Threats and related System Vulnerabilities

The security/privacy threats and vulnerabilities affecting the BIONIC system will be studied as outcome from a dedicated risk analysis. The threats and vulnerabilities are going to be specific for the BIONIC's infrastructure components. The following activities will be performed: a) List the relevant attack methods (In collaboration with project partners - experts) against security and privacy, b) Characterize the threat agents for each attack method retained according to their type, c) Identify the security and privacy vulnerabilities of the entities according to attack methods, d) Estimate the vulnerability level, e) Formulate the security and privacy threats, f) Assign priority in the security and privacy threats according to the probability of their occurrence. The list of the pertinent security and privacy threats and the type of attacks will be the main outputs of this step.

Substep3: Security and Privacy Requirements Analysis

From the previous step, the identification of the respective threats and the attack methods that can be deployed to the proposed system leads to the identification of the system’s vulnerabilities. At this stage, Security and Privacy vulnerabilities detection will lead to the identification of the security and privacy objectives, which are the way that vulnerabilities are reduced thus reducing the potential risk on the identified entities. PriS methodology will be used as a privacy by design approach in order to analyse from the elicited threats and vulnerabilities the security and privacy goals that will have to be fulfilled. The next step of the specific stage is the definition of the security and privacy requirements that basically describe in a specific way the realization of the identified security and privacy objectives. The following actions will be considered when identifying security and privacy requirements: a) List the security and privacy functional requirements, b) Justify the adequacy of coverage of the security and privacy objectives, c) Highlight any coverage flaws (residual risks) with justifications, d) Classify the Security and privacy requirements for each use case, e) Where appropriate, justify the coverage of dependencies of security and privacy requirements. The main output of this stage concerns a) a List of Threats and Attacks, b) the provision of Legal and Organizational Measures and c) the elicitation of the appropriate security and privacy requirements.

Stage 4: Data Protection Impact Assessment

According to the Regulation (EC) 2016/679 of the European Parliament and of the Council of 27th April 2016 for the protection of natural persons with regard to processing of personal data and on the free movement of such data, where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. Taking into account the systems’ and threats’ continuous evolution, risk management “necessitates” the identification of appropriate controls. The processing of personal data, the hierarchy and management of risks has to be examined in a way that optimises the cost and contributes to the most suitable decision-making, aiming at protecting personal data. Impact assessment contributes to the application of privacy principles, in a way that the data subjects are able to preserve control of their personal data. A data protection impact assessment, and hence, the criticality of data shall (in accordance with Regulation (EC) 2016/679 of the European Parliament and of the Council) particularly be required in the case of: a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person (e.g., user profiling by web search activity monitoring for targeted advertising and promotion of products and services (hotels, restaurants, etc.), b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10 (e.g., processing of patients’ medical records (special category of personal data) from healthcare organisations, including medical history, illnesses, and patient care, etc.) or c) a systematic monitoring of a publicly accessible area on a large scale (e.g., traffic monitoring for informing drivers of the fastest route, residence entries' monitoring, public transport entrance, etc.).

Moreover, the assessment shall contain, in accordance with Regulation (EC) 2016/679 of the European Parliament and of the Council, at least: a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; c) an assessment of the risks to the rights and freedoms of data subjects; d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned. This privacy impact assessment is based on a robust conceptual framework related to personal data and data subject protection, to the processing of this data by Information Systems or non-automated means, as well as to an impact analysis of possible incidents of personal data for the data subjects they belong to. Impact assessment aims at the protection of personal data, according to the definition provided by the GDPR, during its processing, as well as the protection of elements that support their processing and are recognised as **Assets**. The value of such assets is equal to the **Impact** brought upon by a possible **violation** of individuals' privacy. A Feared Event is the illegitimate access to personal data, unwanted modification of personal data, as well as the data disappearance. The violation of Information Systems needs the existence of **Vulnerability** and the appearance of a relevant **Threat** coming from a **Risk source**. Summarising, we note that a Threat exploits a vulnerability of an Information System and can have as a result an incident of data protection breach, inflicting some **Impact** on data subjects.

A Risk is a hypothetical scenario that describes how Risk Sources (e.g., an employee bribed by a competitor; could exploit the vulnerabilities in personal data supporting assets (e.g., the file management system that allows the manipulation of data); in a context of threats (e.g., misuse by sending emails); and allow feared events to occur (e.g., illegitimate access to personal data); on personal data (e.g., customer file); thus, generating potential impacts on the privacy of data subjects (e.g., unwanted solicitations, feelings of invasion of privacy, etc.). The risk level is estimated in terms of **severity**, which represents the magnitude of a risk. It essentially depends on the prejudicial effect of the potential impacts, and **likelihood**, which represents the possibility for a risk to occur. It essentially depends on the level of vulnerabilities of the supporting assets facing threats and the level of capabilities of the risk sources to exploit them as shown below.

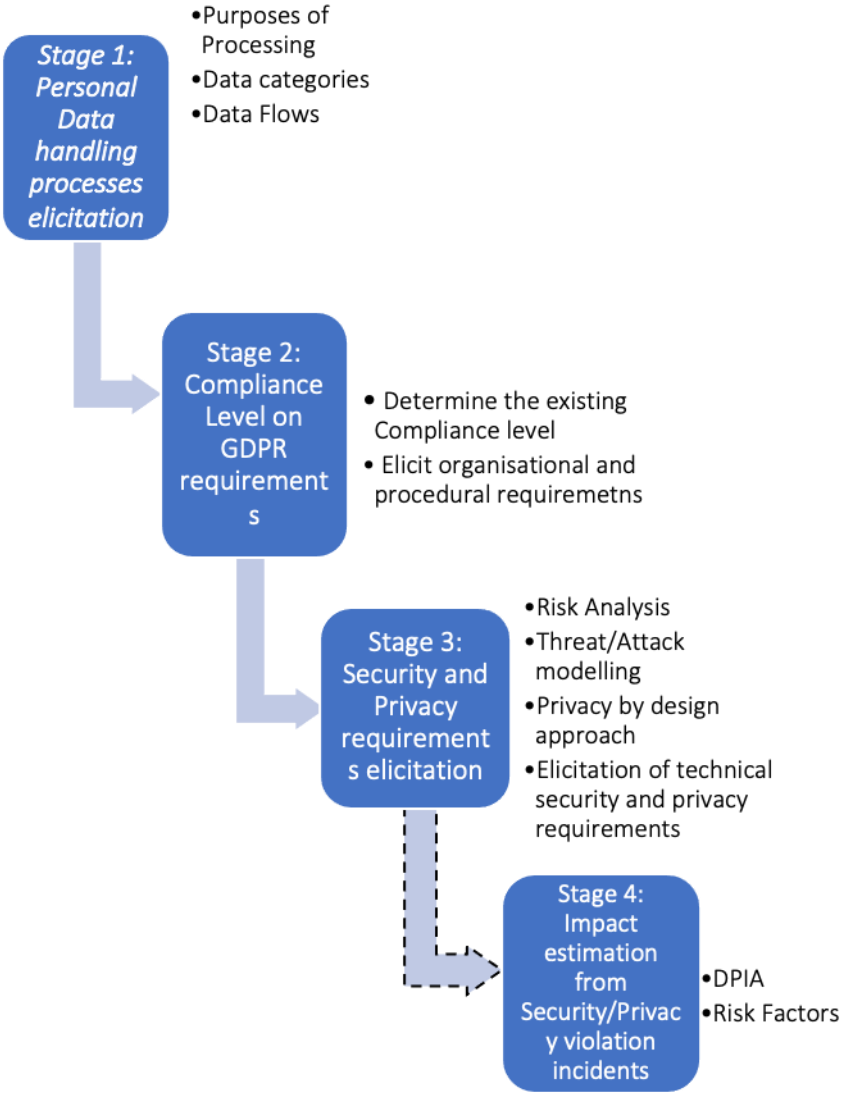
Stage 1: Personal Data handling processes elicitation
•Purposes of Processing
•Data categories
•Data Flows
Stage 2: Compliance Level on GDPR requirements
• Determine the existing Compliance level
• Elicit organisational and procedural requiremetns
Stage 3: Security and Privacy requirements elicitation
•Risk Analysis
•Threat/Attack modelling
•Privacy by design approach
•Elicitation of technical security and privacy requirements
Stage 4: Impact estimation from Security/Privacy violation incidents
•DPIA
•Risk Factors

Fig. 3. BIONIC Privacy and Data Protection Framework

In this stage a data protection impact assessment (DPIA) method will be applied in order to identify the severity and likelihood of any possible privacy violation incidents. During this stage all security and privacy requirements elicited in stage 3 will be evaluated in order to eliminate any possible conflicts prior to the selection of the security and privacy countermeasures. In parallel the DPIA will assist in the identification and assessment of privacy risks and thus in the selection of the appropriate measures to reduce these risks and as such reduce the potential impact of the risks on the data subjects, the risk of non-compliance, legal actions and operational risk. Then the appropriate technical countermeasures for the satisfaction of each requirement will be identified. This information will facilitate the developers to select and proceed with the most suitable implementation techniques for ensuring the security (confidentiality, integrity and availability) of the data processed, as well as the protection of the users' privacy (user consent on data processing and data transmission, satisfaction of user rights etc.). For conducting the DPIA it is necessary to consider both the output of stage 2 regarding the organizational and legal requirements as they are derived from the Gap analysis as well as the output of stage 3 regarding the technical security and privacy requirements derived from the risk/threat analysis and the privacy by design approach. The main output of this stage concerns a) the severity of the privacy violations incidents and b) the likelihood of the privacy violations incidents. The output of stage 4 will enable the developers to select and proceed with the most suitable implementation techniques for ensuring the security (e.g., confidentiality, integrity and availability) of the data processed, as well as the protection of the users' privacy (e.g. user consent on data processing and data transmission, satisfaction of user rights) under GDPR principles. The proposed framework is presented in figure 3.

5. Conclusions

BIONIC acknowledges that the ageing population in Europe impacts multifaceted on the EU productivity growth [45-46] and rises healthcare costs that are leading to the necessity of developing new digital forms of health self-management systems outside the health-care services [47]. Therefore, it provides the development of medical wearables applications for personalized information and treatment to ageing workers, as a form of an m-health system [5], aiming to assist them in managing their health issues and maintaining behaviours that promote health, so as to improve the quality of their work and life. In this regard, it proposes a Privacy and Data Protection Framework that complies with GDPR legislation. The use of the PriS Privacy by Design method is very critical for capturing the required information following the whole software development lifecycle. Particular attention has been given on the different categories of personal data that are processed by the BIONIC platform, such as sensitive data, including recent developments in the field of biometric and health-related data. The Framework also ensures that the applications will respect all the rights of the data owners (workers), such as their right to object to the storage/processing of their information, their right to be forgotten, their right to restriction of processing. Following the proposed privacy-by-design approach, it ensures the satisfaction of all functional requirements, but also of all non-functional (security and privacy) related requirements imposed by the users. Furthermore, during the design phase, all legal and technical requirements of the General Data Protection Regulation (GDPR) are considered, while all necessary technical, organizational and procedural measures to address the GDPR requirements related to data protection, accountability and handling of potential data breaches are taken into account. Respectively, it is ensured that principles like the data protection (purpose limitation, data minimization, accuracy, accountability), the lawfulness of processing, the user consent, are fully satisfied. Following this Framework, the applications respect all the rights of the data owners (workers) like their right to object to the storage/processing of their information, their right to be forgotten, their right to restriction of processing etc. Finally, the implementation of new concepts, such as privacy and data protection by design and by default, accountability, data minimization, lawfulness of processing and users' consent in e-health and m-health systems are enabled, since different stakeholders from several workplaces and domains with different backgrounds may understand the same terms in different ways. In parallel while the elaboration and mapping of the allocation of liability between different actors in interconnected platforms can be conducted, as well as procedures for handling potential data breaches.

Concluding, the proposed Framework, covers the gaps in existing methodologies, focusing on the increase of the end users' trustworthiness to the developed software, by providing a strong elicitation process for deriving the set of technical requirements that should be addressed, while it proposes a process for validating that the elicited requirements, fulfilling the objectives to the GDPR.

Acknowledgment. This research has received funding from the European Union's Horizon 2020 Framework Programme for Research and Innovation under grant agreement #826304– BIONIC.

References

1. Milutinovic, M., De Decker, B.: Ethical aspects in eHealth–design of a privacy friendly system. Journal of Information, Communication and Ethics in Society, 14(1), 49-69. (2016)
2. WHO: "E-Health", (2015) [Online]. Available: http://www.who.int/trade/glossary/story021/en/.
3. Esposito, C., Castiglione, A., Tudorica, C. A., & Pop, F:. Security and privacy for cloud based data management in the health network service chain: a microservice approach. IEEE Communications Magazine, 55(9), 102-108. (2017)
4. Chib, A., & Lin, S. H.: Theoretical Advancements in mHealth: A Systematic Review of Mobile Apps. Journal of health communication, 23(10-11), 909-955. (2018)
5. Drosatos, G., Efraimidis, P. S., Williams, G., & Kaldoudi, E.: Towards Privacy by Design in Personal e-Health Systems. In HEALTHINF (pp. 472-477). (2016, February)
6. Marcolino, M. S., Oliveira, J. A. Q., D'Agostino, M., Ribeiro, A. L., Alkmim, M. B. M., & Novillo Ortiz, D: The impact of mHealth interventions: systematic review of systematic reviews. JMIR mHealth and uHealth, 6(1), e23. (2018)
7. Solomon, M., & Elias, E. P.: Privacy Protection for Wireless Medical Sensor Data. *International Journal of Scientific Research in Science and Technology*, 4(2), 1439-1440. (2018)
8. Almarashdeh, I., Alsmadi, M., Hanafy, T., Albahussain, A., Altuwaijri, N., Almaimoni, H.,& Al Fraihet, A.: Real-time elderly healthcare monitoring expert system using wireless sensor network. International Journal of Applied Engineering Research ISSN, 0973-4562. (2018)
9. Mustafa, U., Pflugel, E., & Philip, N.: A Novel Privacy Framework for Secure M-Health Applications: The Case of the GDPR. In 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3) (pp. 1-9). IEEE. (2019, January)

10. Lee, N., & Kwon, O.: A privacy-aware feature selection method for solving the personalization–privacy paradox in mobile wellness healthcare services. Expert systems with applications, 42(5), 2764-2771. (2015)
11. Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., & Zhu, Q.: Health information privacy concerns, antecedents, and information disclosure intention in online health communities. Information & Management, 55(4), 482-493. (2018)
12. PwC: The Wearable Future, Consumer Intelligence Series (2014). Available at: http://www.pwc.com/es_MX/mx/industrias/archivo/2014-11-pwc-the-wearable-future.pdf
13. Kurtz, C., Semmann, M. and Böhmann, T.: Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors presented at the Americas Conference on Information Systems (AMCIS), New Orleans. (2018)
14. Martin, Y. S., & Kung, A.: Methods and tools for GDPR compliance through privacy and data protection engineering. In 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 108-111). IEEE. (2018, April)
15. Alagar, V., Periyasamy K., and Wan, K.: Privacy and security for patient-centric elderly health care, 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian, 2017, pp. 1-6. (2017)
16. Alibasa, M. J., Santos, M. R., Glozier, N., Harvey, S. B. and Calvo, R. A.: Designing a secure architecture for m-health applications, 2017 IEEE Life Sciences Conference (LSC), Sydney, NSW, 2017, pp. 91-94. (2017)
17. Zhou, J., Lin, X., Dong, X. and Cao, Z.: PSMPA: Patient Selfcontrollable and MultiLevel Privacy-Preserving Cooperative Authentication in Distributed-Healthcare Cloud Computing System, in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 6, pp. 1693 1703. (2015)
18. Volk, M., Sterle, J. and Sedlar, U.: Safety and Privacy Considerations for Mobile Application Design in Digital Healthcare. International Journal of Distributed Sensor Networks, 2015, pp.1-12. (2015)
19. Li, X.: Understanding eHealth literacy from a privacy perspective: eHealth literacy and digital privacy skills in American disadvantaged communities. American Behavioral Scientist, 62(10), 1431-1449. (2018)
20. Edemacu, K., Park, H. K., Jang, B., & Kim, J. W.: Privacy Provision in Collaborative Ehealth With Attribute-Based Encryption: Survey, Challenges and Future Directions. IEEE Access, 7, 89614-89636. (2019)
21. Omoogun, M., Seeam, P., Ramsurrun, V., Bellekens, X., & Seeam, A. (2017, June). When eHealth meets the internet of things: Pervasive security and privacy challenges. In 2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security) (pp. 1-7). IEEE.
22. Bhuiyan, M. Z. A., Zaman, M., Wang, G., Wang, T., & Wu, J.: Privacy-protected data collection in wireless medical sensor networks. In 2017 International Conference on Networking, Architecture, and Storage (NAS) (pp. 1-2). IEEE. (2017, August)
23. Liu, L.S., Shih, P.C. and Hayes, G.R.: Barriers to the adoption and use of personal health record systems, Proceedings of the 2011 iConference, Seattle, WA, 8-11 February, ACM, pp. 363-370. (2011)
24. Romanou, A.: The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. Computer law & security review, 34(1), 99-110. (2018)
25. Sousa, M., Ferreira, D. N. G., Pereira, C. S., Bacelar, G., Frade, S., Pestana, O., & Correia, R. C.: OpenEHR Based Systems and the General Data Protection Regulation (GDPR). Building Continents of Knowledge in Oceans of Data: The Future of Co-Created EHealth. (2018)

26. Iwaya, L. H., Fischer-Hübner, S., Åhlfeldt, R. M., & Martucci, L. A.: mhealth: A privacy threat analysis for public health surveillance systems. In 2018 IEEE 31st International Symposium on Computer-Based Medical Systems (CBMS) (pp. 42-47). IEEE. (2018, June)
27. Sawand, M. A., & Khan, N. A.: Privacy and Security Mechanisms for eHealth Monitoring Systems. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 8(4), 533-537. (2017)
28. Pirbhulal, S., Samuel, O. W., Wu, W., Sangaiah, A. K., & Li, G.: A joint resource-aware and medical data security framework for wearable healthcare systems. Future Generation Computer Systems, 95, 382-391. (2019)
29. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S.: Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Informatics Journal, 18(2), 113-122. (2017)
30. Luo, E., Bhuiyan, M. Z. A., Wang, G., Rahman, M. A., Wu, J., & Atiquzzaman, M.: Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems. IEEE Communications Magazine, 56(2), 163-168. (2018)
31. Cavoukian, A.: Privacy by design [leading edge]. IEEE Technology and Society Magazine, 31(4), 18-19. (2012)
32. Lambrinoudakis, C.: The General Data Protection Regulation (GDPR) Era: Ten Steps for Compliance of Data Processors and Data Controllers. In International Conference on Trust and Privacy in Digital Business (pp. 3-8). Springer, Cham. (2018, September)
33. Tikkinen-Piri, C., Rohunen, A., & Markkula, J.: EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153. (2018)
34. Huth, D.: A Pattern Catalog for GDPR Compliant Data Protection. In PoEM Doctoral Consortium (pp. 34-40). (2018)
35. Rubinstein, I.S. & Good, N.: Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. Berkeley Technology Law Journal 28(2), 1333-1413. (2013)
36. Antignac, T., Scandariato, R., & Schneider, G.: Privacy compliance via model transformations. In 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 120-126). IEEE. (2018, April)
37. Rösch, D., Schuster, T., Waidelich, L., & Alpers, S.: Privacy Control Patterns for Compliant Application of GDPR. AMCIS 2019 Proceedings > Information Security and Privacy (SIGSEC) > 27. (2019)
38. Palmirani, M., Martoni, M., Rossi, A., Bartolini, C., & Robaldo, L.: Legal Ontology for Modelling GDPR Concepts and Norms. In JURIX (pp. 91-100). (2018, December)
39. Notario, N., Crespo, A., Martin, Y.S., Del Alamo, J.M., Metayer, D.L., Antignac, T., Kung, A., Kroener, I.,Wright, D.: PRIPARE: Integrating privacy best practices into a privacy engineering methodology. Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015 pp. 151-158. (2015)
40. Kalloniatis, C., Kavakli, E., Gritzalis, S.: Addressing privacy requirements in system design : the PriS method. Requirements Engineering 13.3, 241-255. (2008)
41. Robol, M., Salnitri, M., & Giorgini, P.: Toward GDPR-compliant socio-technical systems: modeling language and reasoning framework. In IFIP Working Conference on The Practice of Enterprise Modeling (pp. 236-250). Springer, Cham. (2017, November)
42. Kalloniatis, C.: Incorporating Privacy in the Design of Cloud-Based Systems: A Conceptual Metamodel, Information and Computer Security Journal, Emerald. (2017) https://doi.org/10.1108/ICS-06-2016-0044
43. Kalloniatis, C.: Designing Privacy-Aware Systems in the Cloud, Proceedings of the TRUSTBUS 2015 12th International Conference on Trust Privacy and Security in

Digital Business, S. Hubner, C. Lambrinoudakis (eds), September 2015, Valencia, Spain, Springer LNCS Lecture Notes in Computer Science. (2015)

44. Mouratidis, H., Islam S., Kalloniatis C., Gritzalis S. A framework to support selection of cloud providers based on security and privacy requirements in Journal of Systems and Software Vol. 86, no 9, pp.2276-2293. (2013)
45. Carbonaro, G., Leanza, E., McCann, P., & Medda, F.: Demographic decline, population aging, and modern financial approaches to urban policy. International Regional Science Review, 41(2), 210-232. (2018)
46. Sharma, R.: The Demographics of Stagnation: Why People Matter for Economic Growth. Foreign Affairs 95 (2): 18–24. (2016)
47. Petrakaki, D., Hilberg, E., & Waring, J.: Between empowerment and self-discipline: Governing patients' conduct through technological self-care. Social Science & Medicine, 213, 146-153. (2018)

Christos Kalloniatis holds a PhD from the Department of Cultural Technology and Communication of the University of the Aegean and a master degree on Computer Science from the University of Essex, UK. Currently he is an Associate professor and head of the Department of Cultural Technology and Communication of the University of the Aegean and director of the Privacy Engineering and Social Informatics (PrivaSI) research laboratory. He is a former member of the board of the Hellenic Authority for Communication Security and Privacy. His main research interests are the elicitation, analysis and modelling of security and privacy requirements in traditional and cloud-based systems, the analysis and modelling of forensic-enabled systems and services, Privacy Enhancing Technologies and the design of Information System Security and Privacy in Cultural Informatics. He is an author of several refereed papers in international scientific journals and conferences and has served as a visiting professor in many European Institutions. Prior to his academic career he has served at various places on the Greek public sector including the North Aegean Region and Ministry of Interior, Decentraliastion and e-Governance. He has a close collaboration with the Laboratory of Information & Communication Systems Security of the University of the Aegean and the Systems Security Laboratory of the University of Piraeus. He has served as a member of various development and research projects.

Costas Lambrinoudakis holds a B.Sc. (Electrical and Electronic Engineering) from the University of Salford (1985), an M.Sc. (Control Systems) from the University of London (Imperial College -1986), and a Ph.D. (Computer Science) from the University of London (Queen Mary and Westfield College – 1991). Currently, he is a Professor at the Department of Digital Systems, University of Piraeus, Greece. From 1998 until 2009 he has held teaching position with the University of the Aegean, Department of Information and Communication Systems Engineering, Greece. For the period 2012-2015, he was a member of the board of the Hellenic Authority for Communication Security and Privacy, while from 2016 he serves on the board of the Hellenic Data Protection Authority. Finally, from 2015, he is Head of the Department of Digital Systems and Director of the Systems Security Lab. His current research interests are in the areas of Information and Communication Systems Security and of Privacy Enhancing Technologies. For many years he is working on issues related to the protection of personal data and the compliance of information systems to the National and European Legislation. He is the author of more than 100 scientific publications in refereed international journals, books and conferences, most of them on ICT security and privacy protection issues. He has served as program committee chair of 15 international scientific conferences and as a member on the program and organizing committees in more than 150 others. Also, he participates in the editorial board of two international scientific journals and he acts as a reviewer for more than 35 journals. He has been involved in many national and EU funded R&D projects in the area of Information and Communication Systems Security. He is a member of the ACM and the IEEE.

Mathias Musahl is working as Researcher in Body Sensor Network group of „Augmented Vision" department, DFKI GmbH. He has finished his diploma in electrical engineering from TU Kaiserslautern in 2011. After that he worked for 6 years as a software engineer in the industry. There he worked on designing and implementing hardware and software for embedded devices related to distributed audio network infrastructure for the broadcasting industry.

Athanasios G. Kanatas is a Professor at the Department of Digital Systems, University of Piraeus, Greece, Director of the Telecommunication Systems Laboratory, and Director of the Postgraduate Programme in Digital Communications and Networks. He received the Diploma in Electrical Engineering from the National Technical University of Athens (1991), the M.Sc. degree in Satellite Communication Engineering from the University of Surrey, UK (1992), and the Ph.D. degree in Mobile Satellite Communications from NTUA (1997). He has published more than 200 papers in international journals and conference proceedings. He is the author of 6 books in the field of wireless and satellite communications. He has been the technical manager of several European and National R&D projects. His current research interests include the development of new waveforms and digital techniques for next generation wireless systems; wireless channel characterization and modeling; antenna design and security issues for V2V communications. He has been a Senior Member of IEEE since 2002. In 1999, he was elected Chairman of the Communications Society of the Greek Section of IEEE. From 2013 to 2017, he has served as Dean of ICT School of the University of Piraeus, Greece.

Stefanos Gritzalis is a Professor of Information and Communication Systems Security, at the Lab. of Systems Security, Dept. of Digital Systems, University of Piraeus, Greece (06.2019+). Previously, he was a Professor at the University of the Aegean, Greece, School of Engineering, Dept. of Information and Communication Systems Engineering, and member of the Info-Sec-Lab Laboratory of Information and Communication Systems Security (2002-2019). He was the Rector of the University of the Aegean, Greece (2014-2018), Head of the Dept. of Information and Communication Systems Engineering (2005-2009), Deputy Head of the Dept. of Information and Communication Systems Engineering (2012-2014), and Director of the Lab. of Information and Communication Systems Security (2005-2009). He has acted as Special Secretary for the Hellenic Ministry for Administrative Reform and Electronic Government (2009-2012). He holds a BSc in Physics, an MSc in Electronic Automation, and a PhD in Information and Communications Security from the Department of Informatics and

Telecommunications, University of Athens, Greece. His published scientific work includes more than 10 books, 33 book chapters (including the book “Digital Privacy: Theory, Technologies and Practices”, co-edited by A. Acquisti, S. Gritzalis, C. Lambrinoudakis and S. De Capitani di Vimercati, Auerbach Publications, Taylor and Francis Group). Moreover, his work has been published in 314 papers (133 in refereed journals and 181 in the proceedings of international refereed conferences and workshops). He has co-authored papers with more than 130 researchers from 25 countries during the last 28 years. The focus of his publications is on Information and Communications Security and Privacy.

Received: September 22, 2020; Accepted: December 20, 2020