Trakia Journal of Sciences, Vol. 17, Suppl. 1, pp 873-882, 2019
Copyright © 2019 Trakia University
Available online at:
http://www.uni-sz.bg

ISSN 1313-7069 (print)
ISSN 1313-3551 (online) **doi:10.15547/tjs.2019.s.01.144**

PERSONAL DATA SECURITY FOR SMART SYSTEMS AND DEVISES WITH REMOTE ACCESS

P. Veleva*

Department of Informatics and Mathematics, Faculty of Economics, Trakia University,
Stara Zagora, Bulgaria

ABSTRACT

Issues related to the personal data security of users of smart devices with remote access are discussed in the paper. An empirical study through a structured interview and a web-based survey via e-mail and social media conducted by a specific company is presented. The actions taken by the company to ensure the security and personal data protection of its users and business partners are presented. The company's main activity is designing and constructing automatic systems and electronic devices with remote access via the Internet. The survey is part of the company's activity to achieve good business results, loyal and accurate corporate policy benefitting all contracting partners and long-term business partnerships.

Key words: personal data protection, electronic systems with remote access, Internet of Things

INTRODUCTION

In recent years, the world and the Bulgarian economy have been changing at an extremely fast pace, looking for a better and easier way to utilize the services in the Global Network. As a result, there has been an accelerated development of activities in every public domain. In an advanced society, the development of new technologies is an indispensable part of the constantly changing needs and requirements of people and businesses. The development of the Internet of Things concept arises as a result of the natural evolution of the Internet. The new capabilities and new horizons that open up to technologies with remote access and control make them a part of the global governance system. This new evolutionary development of information technology is seen as an object of innovation with the potential for growth and development globally.

The idea of the Internet of Things (IoT) originated in 1999. In a short presentation to The Procter & Gamble leadership, the founder of the Auto-ID research group at the Massachusetts Institute of Technology in the United States, Kevin Ashton sets the foundation for the concept of IoT (1). In his presentation, Ashton portrays the importance and benefits of the massive development of the so-called Radio Frequency Markers (RFID) and their deployment to different devices. He argues that a global computer network could be set up in which all material, physical objects can be connected through the Internet, allowing them to interact with each other by constantly exchanging data and information about their environment and processes, without the need for constant interference from people (2).

The next few years have been marked by a significant increase in interest in the so-called Intelligent Devices by leading companies in the business as well as by the media. The United Nations International Telecommunication Union published in 2005 a first report detailing the innovative nature of the Internet of Things (3, 4).

In 2008, the first European conference on "Internet of Things" was held in Zurich,

***Correspondence to**: *Petya Veleva, Department of Informatics and Mathematics, Faculty of Economics, Trakia University, Stara Zagora, Bulgaria, Tel: 0896601537; 042 699 438, E-mail: pveleva@uni-sz.bg*

Switzerland (5). Immediately after it, the so-called IPSO Alliance, comprising fifty member companies, including world-renowned technology giants like Bosch, Cisco, Ericsson, Intel, SAP, Sun, Google and Fujitsu. Each of them has a strong interest in the idea of creating new products to fit into the IoT concept (6). The main purpose of this alliance is to encourage the use of Internet Protocol (IP) in the Global Network and to make it a tool to support the development of smart devices, their self-identification on the Internet and their linking to their own new network, along with other physical objects, as is the basic idea in the IoT concept (7).

In present, the Internet of Things concept becomes a way of life. This new technology integrates itself more and more in people's everyday life and encompasses all spheres of social, private and business life of the individuals. The emphasis is on the fact that the world is changing rapidly and new technologies are becoming more important to people worldwide. Innovations in various devices and household items such as watches, electrical appliances, fashion accessories, clothes, dentures, lenses, and many others have provided them different sensors e.g. for movement, heat, light, vibrations, etc.(8) These sensors allow things to "sense" everything that happens around them, record, analyze, or exchange the data with each other and with their users. It is important to mention that, besides creating the "sensitivity" of objects, it is also important to create their own identity. This property identity plays the role of a serial number of electronic devices on the Internet. Thanks to it, the assets can be identified on the Internet, collect data, process and transmit it to each other as well as to people (7, 9). The Global Network is a major factor in achieving and delivering communication between remote access electronic devices and people. Wireless Internet (WiFi), infrared, and Bluetooth are part of the capabilities of connecting devices to a single common network. This enables faster penetration of Internet technologies and business communications. Thanks to technology innovations, human intervention is minimized to the initial setting of the goals and tasks that smart devices must perform (7). This is why smart devices and services should be well protected. Unprotected devices can serve as a cyber portal for unauthorized actions, which in turn is a prerequisite for eventual theft of users' personal data or compromise. A need arises for developers of remote access devices and systems to ensure the security of users' personal data, their privacy, and that they do not expose them to potential harm, theft or abuse. It is necessary to build a common approach to security, to take appropriate decisions and to develop effective measures, both technological and legal, tailored to the scale and complexity of the Internet of Things (10).

Providing users with trust in the Internet as well as intelligent devices and related services can be achieved by delegating certain rights that ensure privacy and respect for the privacy of users (7). In order to preserve the anonymity of users and to restrict access and use of their personal data, remote access devices developers use different cryptographic techniques and approaches that allow protected data to be processed and stored without the information content available for third parties (10, 11).

Acceptance and trust from the consumer depend on the use of common, open and widely available standards. They are the building blocks for smart devices with remote control. This increases the added value for consumers, the development of innovation and reveals more economic opportunities (11).

Last but not least, a key area in the development of the Internet of Things concept and the introduction of smart devices in the household and business is related to legal and regulatory aspects. The need for an adequate legal framework is a priority of legislation in each country. The use and deployment of smart devices and related services require many regulatory and legal issues to be solved, but it also strengthens the existing legal issues related to the Internet. Issues related to IoT are wide-ranging, and in essence, the technology is developing at an extremely rapid pace, which goes beyond the ability of the relevant political, legal and regulatory structures to adapt. This continuous dynamic in the development of the Internet of Things is a potential obstacle to the adaptation of an adequate legal framework (12). Examples of legal issues related to the Internet of Things include the current conflict between law enforcement and civil rights; data storage and destruction policies; legal liability for the unintentional use of personal data; security breach; violation of privacy, and others. Another example may be the problem of cross-border data flows that occur when the Internet of Things devices collect data about people in one jurisdiction and pass them on to another jurisdiction with different data protection laws in processing (11, 13).

The Commission of the European Communities in its "Communication from the Commission to the European Parliament, the Council, the European Economic, and Social Committee and the Committee of the Regions" sets out its views on addressing these issues and potential threats. According to it, two of the European Union's (EU) fundamental rights, namely respect for privacy and the protection of personal data are closely tied to the adoption of the concept of the Internet of Things (14).

These two European Union’s rights are directly related to the need for trust, security, and continuity from society when implementing and managing the concept of the Internet of Things. The Communication of the Commission of the European Communities highlights two key aspects. The first one focuses our attention on the European Network and Information Security Agency (ENISA). As part of the work program implementation in 2009, in support of European Union policy, the Agency finds that the emerging risks that affect people's trust are directly related to the understanding of privacy and security risks (14, 15). Another important point in building consumer confidence is the ability to adapt the technology systems to the individual's preferences within the safety limits (16). Many studies in this area show that if consumers are given a sufficient level of control, it increases their confidence and at the same time plays an important role in the rapid spread of technology. In the sphere of business, things are similar - information security is expressed in the availability of business data reliability and confidentiality (16). All this is the basis in January 2012 for the European Commission to propose a package of data protection reforms. The reform package consists of a proposal for a general regulation on the protection of personal data (17), intended to replace the Data Protection Directive (18).

The General Data Protection Regulation (GDPR) with full name Regulation (EU) 2016/679 of the 27th April 2016 concerns the protection of individuals with regard to the processing of personal data and the free movement of such data. This Regulation was published in the Official Journal of the European Union on the 4th of May 2016, but its implementation started on the 25th of May 2018 (19).

By introducing the GDPR, the current regulatory and regulatory framework in the EU countries has changed considerably. Emphasis is placed on the increased requirements regarding the protection of personal data. This accent is additionally reinforced by the sanctions for failure to comply with its provisions (20).

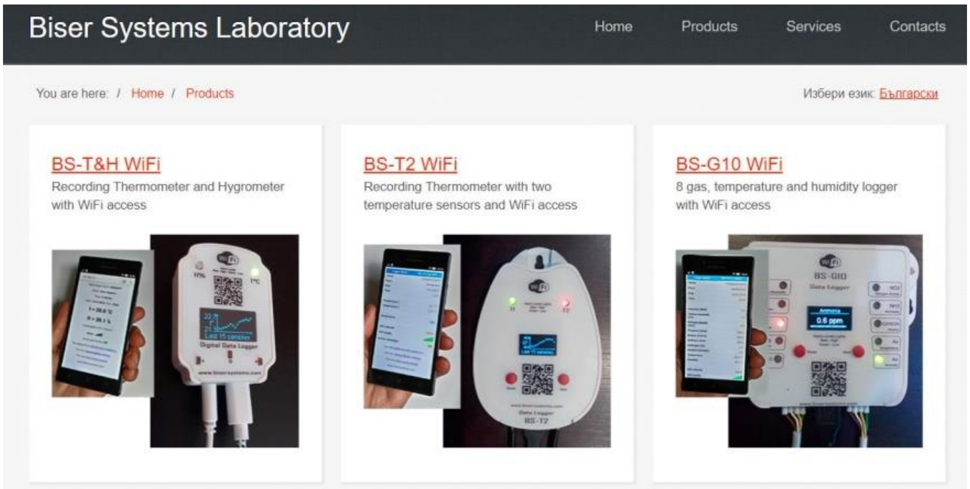
In her report on Privacy, the Classified Information Protection Adviser and Legal Advisor, Dr. Fetty points out that the GDPR has strengthened the powers of the supervisory authorities to investigate, authorize and deliver opinions, as well as corrective powers. Dr. Fetty pointed out in her report that these powers "must be seen in view of the increased penalties for breaching the requirements of the regulation, which must be effective, proportionate and dissuasive. In addition, it must be considered that the supervisory authority may impose a temporary or definitive restriction, prohibit the processing of data and order discontinuation of data flow to a recipient in a third country or international organization " (21).

The new standards for data protection provided by the GDPR are already part of the Bulgarian legislation under the EU and the direct application of the law in all Member States. All this is determined by the purpose of this study, namely to investigate the privacy policy of the measures taken by a particular company (Biser Systems Ltd.) to ensure the security and protection of the personal data of its users and business partners in managing the remote access electronic devices produced by the company.

MATERIAL AND METHODS

1. Company Biser Systems Ltd. as a subject of research

The subject of research in this publication is a small company, which according to data from the Commercial Register of the Republic of Bulgaria is engaged in the design, construction, programming, production, and testing of electronic devices Biser Systems Ltd. The company provides consultancy and mediation activities, both domestically and abroad, for more than 10 years (22). The products that are produced are non-standard electronic systems designed to solve specific problems of customers from different areas of the household and industry. Some of these devices offering remote access are shown in **Figure 1**:



BS-T&H WiFi
Recording Thermometer and Hygrometer with WiFi access

BS-T2 WiFi
Recording Thermometer with two temperature sensors and WiFi access

BS-G10 WiFi
8 gas, temperature and humidity logger with WiFi access

Figure 1. Devices developed by Biser Systems Ltd., offering remote access via WiFi, (22)

2. Data acquisition and data processing

Two methods of collecting information are used for the purposes of empirical research. One is a structured interview and the other is a web-based survey.

The main purpose of the structured interview is directly related to the purpose of the survey - gathering sufficient information about the methods and measures taken by the company to protect the personal data of counterparties in intelligent device management and related services. The main source of information and the respondent is the manager and owner of the company Biser Systems Ltd.

In turn, the e-survey is located on the company's website and distributed to its clients via e-mail. The aim is to focus on the information gathered on consumer information, on the protection of their personal data and on the existing legal framework for managing the Internet of Things and to study consumer opinion on risks and attitudes related to unauthorized access to personal data when working with remote control devices.

The data is processed with the modules of marketing research based on the frequency analysis built into the electronic platform Google Forms.

RESULTS AND DISCUSSION

1. Structured interview conducted with the manager of Biser Systems Ltd.

In preparing the interview, the accuracy of the information needed for the study was achieved through a dedicated questionnaire with targeted questions, which were divided into three main groups containing several sub-questions. Here are only the main target groups of questions, namely:

1.1 Target groups with questions

Target group questions No. 1: What privacy policy was taken in Bisser Systems Ltd.?

Target group questions No. 2: What kind of policy has been taken by Bisser Systems Ltd. for the use and management of the cookies on the Internet?

Target group questions No. 3: What policy has been taken by Bisser Systems Ltd. for protection, confidentiality, and integrity of personal data of job applicants in accordance with the General Data Protection Regulation?

1.2 Analysis of received data

As a result of the structured interview with the kind assistance of the company's manager, the following summaries can be made:

Target group questions No. 1: The entry into force of the General Data Protection Regulation of 25th of May 2018 (GDPR) covers the rights and obligations of administrators, processors and data subjects themselves. In the course of business relationships, all users of the company's website http://bisersystems.com, as well as all customers and contractors, provide personal data. The policy pursued by Bisser Systems Ltd. aims to clarify the principles and measures that the company undertakes to protect the security of the personal data of its clients so that they can not be used without the knowledge and explicit consent of them. On the other hand, this policy also describes the responsibilities that Bisser Systems Ltd. assumes as the administrator of personal data. According to the company's manager, the policy of the company will change over time as the digitization process is extremely fast and the order and the relations related to the processing of the personal data will change continuously. That's why Biser Systems Ltd. strives to improve and adapt its practices with the changes that are reflected in the company's policy. The company’s manager says that Biser Systems Ltd. adheres strictly to the provisions in the field of data protection in every activity related to the processing of personal data via http://bisersystems.com. The manager specified that he is not in a position to guarantee the protection of the personal data of his users and clients in cases when the data are reached through the referral from http://bisersystems.com to other websites and separate pages because there is no possibility of control on the processing of data by third parties. In order to guarantee the security and protection of the personal data of its users, Biser Systems Ltd. has taken the necessary organizational and technical measures, consisting of two stages: stage of designing modules on the company's website and the offered services, complying with the new protection requirements the personal data and the registration stage of the user on the website and consent to create a public profile for marketing purposes. The measures that Biser Systems Ltd. undertakes to protect the personal data of its users include: limiting the access to the personal data of the consumers; strict compliance with internal company policy and compliance with the guidelines and guidelines for the protection of personal data required by the competent supervisory authorities. The security measures implemented by Biser Systems Ltd. are subject to regular supervision by the supervisory authorities and periodically updated. The company’s personal data processing activities follow a certain sequence and comply with applicable privacy laws. Through its web site, Biser Systems Ltd. collects personal data in several ways, which are: Business Partner Forms; feedback forms; subscribing to a newsletter and more. Data categories are a name, phone, e-mail, cookies, and other data related to user behaviour on the website itself. In turn, when users correspond to Biser Systems Ltd. through their website, they are required to provide data that is correct, accurate and up to date. Furthermore, in the structured interview, the manager explains, that the storage and destruction period of the users' personal data at http://bisersystems.com depends entirely on the company's need for time to achieve the purposes for which the data were collected. Bisser Systems Ltd. takes appropriate activities to destroy data that is no longer necessary after the company's goals have been achieved. There are exceptions in cases where there is a legal basis for storing the relevant data for a longer period of time.

The methods for collecting and processing personal data through http://bisersystems.com are legal as specified in Art. 6 grounds, of the GDPR (19). When filling out the Contact Form, the user's personal data is processed on the basis of their consent and in order for the company to respond to their specific request (inquiry). In the case where the web site’s users fill in the form of Business Partners, their data is processed in order to provide the service requested by the company. When users enter their email for subscription to a newsletter, this is considered as a confirmatory act whereby the user gives his/her free, informed and unambiguous consent to the processing of personal data relating to him/her in order to obtain product information and the services offered by Biser Systems Ltd. Company users can withdraw their consent at any time to stop receiving company-related information.

Target group questions No. 2: According to the manager of Biser Systems Ltd., cookies in their essence are an information package in the form of a small file size that is used by websites, storing the user's local network information. Using cookies, websites including http://bisersystems.com are able to distinguish and remember their visitors as well as their individual preferences, settings, and actions. The primary purpose and sole use of the cookies are improving the performance of the digital asset to the website. The cookies collect information about the user's activity on the website and do not provide information about a particular user or visitor on the company's website. Cookies can also be used for marketing and advertising purposes, track user behavior or measure ad campaign performance, etc. Cookies are used by the website, do not link to a specific name, address, or IP address of the users that visited the website. Users and visitors to http://bisersystems.com may use their products and services without agreeing to cookies. Also at any time, they can delete them from their local hard disk, but it can cause difficulties for them to see some elements and work with the company's website.

Target group questions No. 3: Collection and processing of personal data related to the recruitment procedure. Biser Systems Ltd. also collects and processes personal data connected to job applicants when the need for new staff arises. The Company commits itself to correctness and transparency in collecting, using and protecting said data. Biser Systems Ltd. collects the following information, which applies for the job offer: name, address, contact details (telephone, e-mail, etc.); qualification information, skills, professional experience, length of service of the applicant; information concerning the applicant and his/her rights to work in Bulgaria. Data can be collected by the company from applications for employment; CVs; personal documents such as a passport and identity card, during an interview or other forms of assessment from former employers and etc.

Biser Systems Ltd. processes the personal data as this allows the company to manage the recruitment process, evaluate the experience and the skills of applicants and determine who is the most suitable candidate for the job. The company has an internal data protection policy that provides security and guarantees that it won't be lost, destroyed, misused or provided to third parties. Received data for the selection of the personnel of Biser Systems Ltd. are stored for a period of 6 to 12 months, depending on the end result of the recruitment process. If the candidate is approved, his or her personal data is stored in his/her employment record for the duration of the employment. If the application is not approved, it shall be processed for a period of 6 months, to be used in possible future recruitment options with the candidates approval.

For compliance with the General Regulation on the Protection of Personal Data and the correct and accurate collection of information concerning the users of http://bisersystems.com, an authorized employee of Bisser Systems Ltd. is responsible. This employee is responsible for ensuring the timely detection of security breaches and the need for notification to the supervisory authority or data subjects concerned.

From the structured interview, conducted with the kind assistance of the manager of Bisser Systems Ltd., it is clear that the actions taken to protect personal data and preserve the privacy of consumers cover almost all aspects of the business. Since the legal framework based on the GRPD protection is a relatively new phenomenon in the Europen's Union Member States and Bulgaria in particular, there are still no concrete results on the efficiency of the actions undertaken by the company.

2. Web-based survey

The online survey is becoming an increasingly preferred form of conducting research and analysis. This is due to the advantages and innovations that the Information Technology offers. The tools of Internet Communication and the fact that electronic data is used helps to carry out the research in the shortest period of time.

For the purpose of empirical research, a total of 106 people were questioned within 10 days electronic survey. The results are summarized using the Frequency Analysis method. The survey conducted is random, since the respondents have access to it via the Internet and there are no restrictions or controls on the target audience groups.

The full set of questions about the conducted web-based survey can be found at: https://docs.google.com/forms/d/1yx_Xupl6YZkIIapKfUMhHDRkqGQRiAb_r2plBJft40I/edit#responses

The study included 79 women (74.5%) and 27 men (25.5%) aged 20 to over 50 years. The predominant age group is 21 to 30 years old or 31.1% of the respondents. This result is understandable because it is the age group that is the fastest and easiest to use in Innovative Technologies.

From the survey results it is clear that the percentage of people with higher education (63.2%) is considerably higher than the other degrees indicated by respondents: 27.4% have secondary education, the proportion of respondents with a college education of 8.5% and the number of people with elementary education is negligible (0.9%).

Figure 2 presents a graph on the frequency and purpose of using the global Internet network by respondents. The figure shows that 104 out of 106 respondents use the Internet daily, which is 98.1% of all surveyed people. The number of people using the Internet several times a week and several times a month is negligible (0.9%).

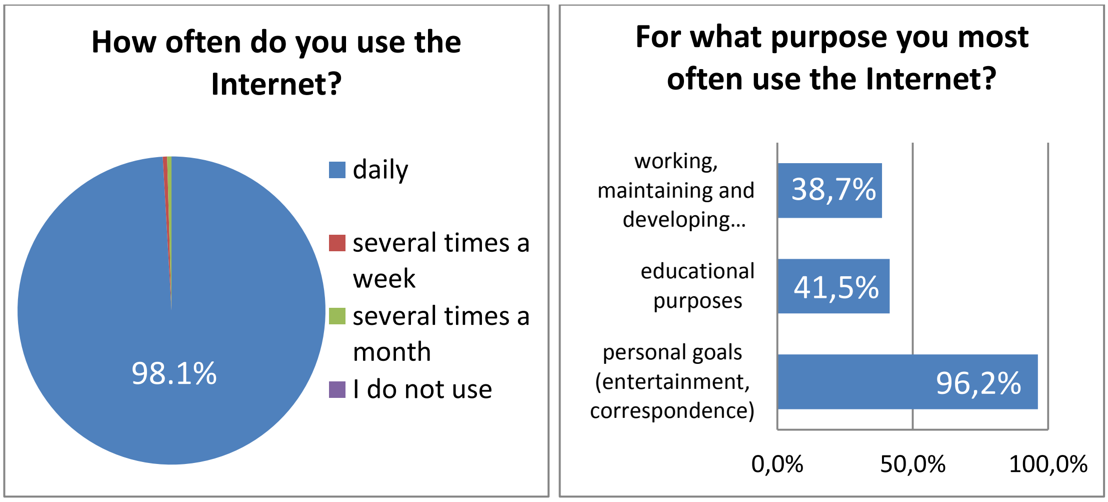


Figure 2. Percentage of the frequency and purpose of using the Internet by the respondents

Most often, the Global Network is used for personal purposes such as entertainment, correspondence, online shopping (96.2%). At around 42% of respondents use the Internet for educational purposes, while the remaining 38.7% use the Internet for business purposes such as work, maintain and develop their business.

From the survey, it is clear that more than half of the respondents (58.5%) are not familiar with the term "Internet of Things". The percentage of respondents thinking that smart devices working with remote access are useful (88.7%), significantly exceeds the percentage of negative respondents (11.3%). This percentage is depicted in **Figure 3.**

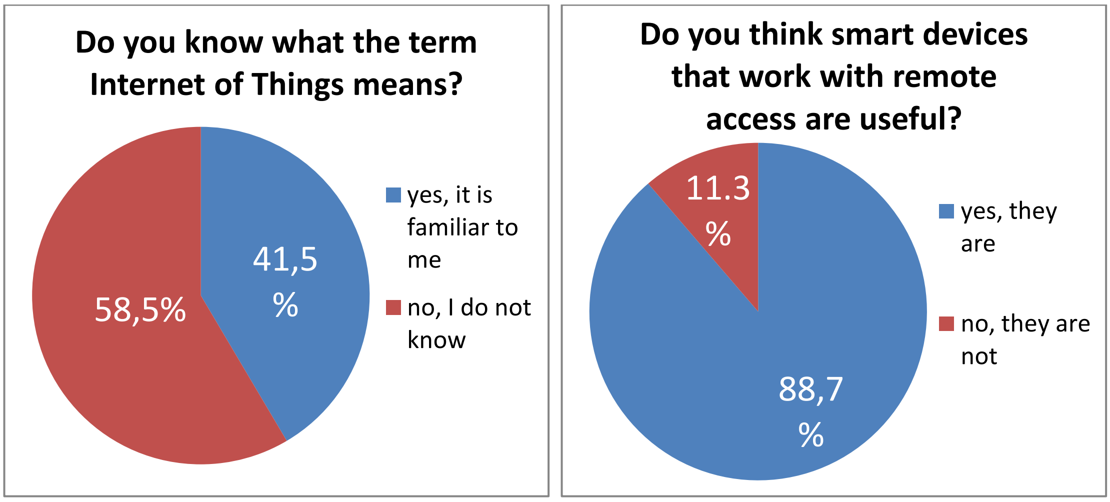


Figure 3. Percentage ratio of people familiar with the term Internet of Things and the utility of Smart Devices

To the question, "Would you buy smart devices for your home or business? " 82.1% of the respondents answered positively and only 17.9% gave a negative answer.

To the question, "If you have your own business, would you use smart devices and related services?" the positive response rate (83%) significantly exceeds negative responses (17%).

This is an evidence that technology is significantly leveraging consumer lifestyles and facilitating successful business operations. **Figure 4** shows the percentage of the above issues.

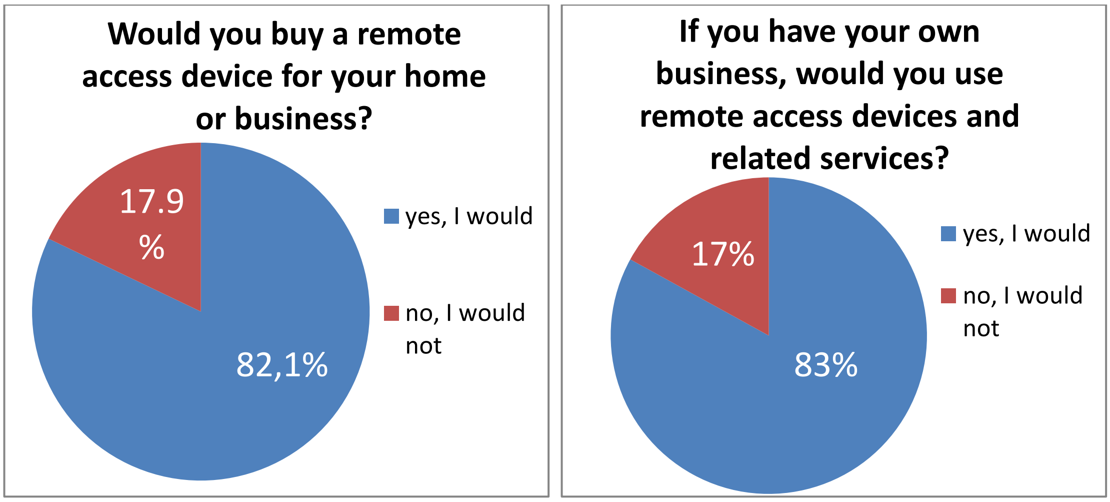


Figure 4. Percentage of responses to whether they would buy and use remote access devices for their home or business

Figure 5 presents graphs on consumer interest in Internet privacy on a scale of 1 (I'm not concerned) to 6 (Highly concerned) and the degree of risk involved in the use of smart devices with remote access. **Figure 5** shows that 50.9% of respondents are highly concerned about the security of their personal data on the Internet, but the percentage of non-concerned users is not negligible. About 93% of respondents believe that the use of intelligent devices and related services poses a high risk, and 7% of them believe that such risk does not exist.

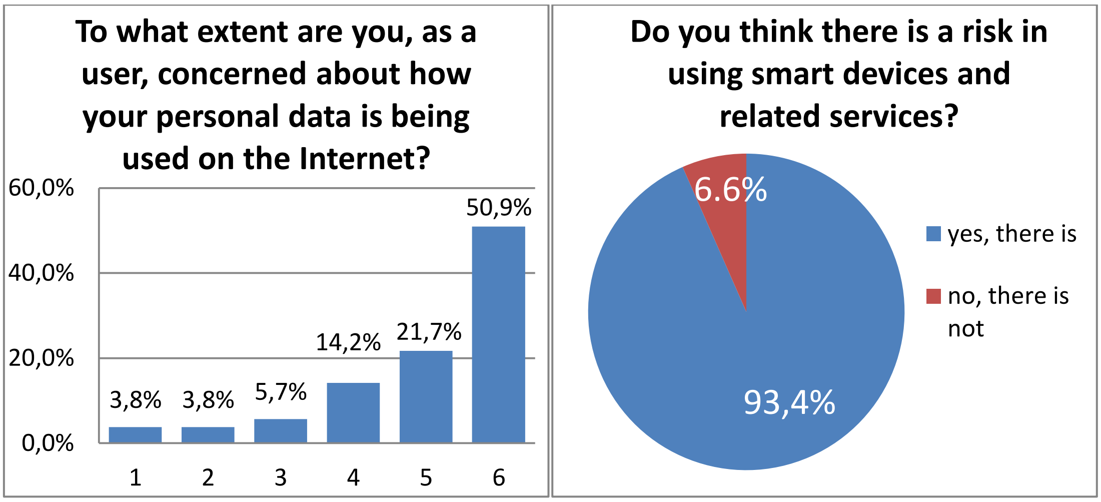


Figure 5 Percentage ratio of users' concerns about their personal data and the risk of using smart devices

To the question, "Do you know what the General Data Protection Regulation (GDPR) is?", 84% of respondents say they are aware, and only 16% of them have never heard of this regulation.

Figure 6 shows the percentage of respondents' answers on whether they themselves are aware of how to protect their personal data on the Internet and what activities are needed to protect users' privacy when using devices with remote access. **Figure 6** shows that 51.9% are well informed on how to protect their personal data on the Internet, 23.6% equally respond they are slightly informed or they do not know what to do to protect their personal data, and 0.9% of the respondents have never heard of it. As another graph, 46.2% do not know what kind of prevention to make to protect their personal data when using remote access devices; 26.4% of the respondents are well informed, 25.5% are slightly informed, and 1.9% of the respondents have never heard of it.

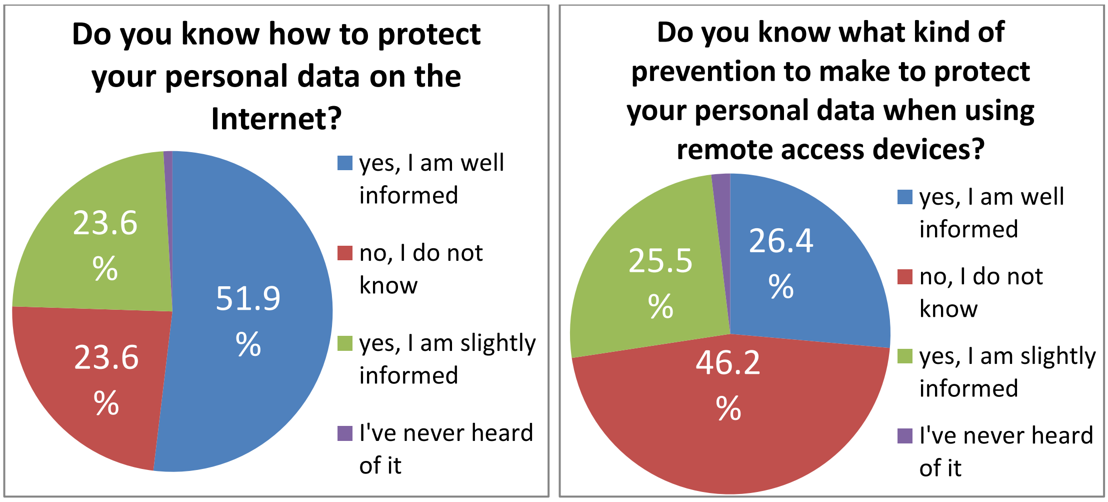


Figure 6 Percentage of responses to data protection measures for Internet and remote access devices

Based on the empirical study, several conclusions can be made. Every company that develops an online business needs to have a correct and secure policy to protect the personal data of its clients and business partners, in compliance with the requirements of the Bulgarian legislation and the regulations and laws in force in it.

The results of the web-based survey show that most of the users are aware of the General Data Protection Regulation, and the majority of consumers know how to protect their personal data on the Internet themselves. On the one hand, it is clear from the survey that IoT and related services are still new to the society and there is a high degree of mistrust on the part of users on remote access devices. On the other hand, respondents' answers show that information and communication technologies are entering with the increasingly rapid pace the daily life of business and consumers and the Internet is becoming a tool for the development and improvement of smart technologies and related devices with remote access.

CONCLUSIONS

From this survey, it can be concluded that the Internet of Things provides great opportunities for the development of both business and society as a whole. Smart devices with remote access have significantly changed the way we live in many aspects - from the way we manage our homes to transforming a large number of business activities. Because of their potential to be at the heart of the next technological revolution, Smart Devices with remote access today are one of the main topics for both businesses and consumers.

Like any new technology, the Internet of Things poses a number of issues and challenges for developers of remote access devices and society. In the context of information technology, data security requirements are not new. At this stage of its development, the Internet of Things is still an unexplored territory that poses new and unique challenges for data security experts. Consumers' belief that smart devices and related services are well protected from abuses and violations related to the security of personal data and privacy of their lives is essential to the success of companies producing such kind of devices.

Another challenge for the IoT against the backdrop of growing business demands for smart devices with remote access on the market is to provide well-trained, qualified specialists who can be able to address the problems and offer an adequate solution.

In this connection, it is extremely important and necessary to have software platforms that allow the creation of a single application that can work equally well on all types of devices and operating systems. Thus, remote access device users will benefit from their full potential, and developers of such devices will be able to withstand the ever-changing technology environment.

In summary, it can be said that the Internet of Things and related remote control devices are of great benefit to people, their homes and businesses. They provide great opportunities for development, saving time and facilitating people's living and business. Through clear and accurate strategies, an adequate policy framework, proper data security activities, IoT from a utopian idea, is becoming a modern technological revolution for the benefit of the whole world.

REFERENCES

1. Postscapes, Tracking the Internet of Things, a brief history of the Internet of Things, http://postscapes.com/internet-of-things-history, 2018.
2. Ashton, K., That “Internet of Things” Thing. RFID Journal, 2009.
3. ITU Internet Reports 2005: The Internet of Things - Executive Summary, International Telecommunication Union, Geneva, 2, 2005.
4. ITU Measuring the Information Society Report 2015, The Internet of Things: data for development, International Telecommunication Union, Geneva, ISBN 978-92-61-15791-3, 147, 2015.
5. Nagel, L., Roidl, M. and Follert, G. The Internet of Things: On Standardisation in the Domain of Intralogistics, Adjunct Proceedings of First International Conference on the Internet of Things 2008, Ed. Florian Michahelles, 16-21, 2008.
6. IPSO Alliance, http://www.ipso-alliance.org
7. Alexiev, P., Internet of Property – Occurring, Essence And Differentiation, NBU, Sofia, 2016
8. European Statistics Manual, Statistics on the Digital Economy and the Digital Society - Households and Individuals, http://ec.europa.eu/eurostat/statistics-explained/index.php ?title=Digital_economy_and_society_statistics_-_households_and_individuals/bg, 2018.
9. Ilunin, I., IoT Privacy and Security Challenges for Smart Home Environments, https://hackernoon.com/iot-privacy-and-security-challenges-for-smart-home-environments-c91eb581af13, 2018.
10. Good Practices for Security of Internet of Things in the context of Smart Manufacturing, ENISA, ISBN: 978-92-9204-261-5, DOI: 10.2824/851384, 2018.
11. Vermesan, O., Friess, P., Internet of things – Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers, Aalborg, Denmark, 2013.
12. Commission's Personal Data Protection Strategy for Personal Data Protection (Horizon 2022), Commission for Personal Data Protection, Sofia, 2017.
13. Bertino, E. Security and Privacy in the Internet of Things, Purdue University, 2018.
14. The Internet of Things - An Action Plan for Europe,Communication from the Commission to the European Parliament, the Council, the European Economic, and Social Committee and the Committee of the Regions, Commission of the European Communities, Brussels, 278 final, 2009.
15. Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymisation, ENICA, https://gdpr.blog.hu/2018/02/26/ pseudonymisation_ and_ anonymisation_in_the_gdpr, 2018.
16. Handbook on European Data Protection Law, European Union Agency for Fundamental Rights, ISBN 978-92-871-9934-8 (CoE), ISBN 978-92-9239-461-5 (FRA), doi:10.2811/69915, 2014.
17. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), European Commission, 2012/0011 (COD) C7-0025/12, 2012.
18. Directive 95/46/EC of the european parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Union, L 281 /31, 1995.
19. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Regulation on data protection), Official Journal of the European Union, L 119/2, 2016.
20. A new EU regulation will affect all Bulgarian employers, https://www.economic.bg/ bg/news/9/nov-reglament-na-es-shte-zasegne-vsichki-balgarski-rabotodateli.html, 2017.
21. Fety, N., Protection of Personal Data, Legal Barometer, http://www.legalworld.bg/ 70116.zashtitata-na-lichnite-danni-%E2%80%93-osnovna-tema-v-noviia-broj-na-iuridicheski-barometyr.html ,16,June 2018.
22. Biser Systems Laboratory, official site, http://www.bisersystems.com