GDPR – General Data Protection Regulation on Sites Requiring Accessibility

Mirena Todorova – Ekmekci

mhtodorova@gmail.com

Institute of Ethnology and Folklore Studies with Ethnographic Museum at the Bulgarian Academy of Science, Sofia, Bulgaria

***Abstract* — This paper describes what GDPR - General Data Protection Regulation is and why it matters for business, institutions and other legal entities, who need to collect personal data in order to provide and deliver services or products. They have to apply and describe to the consumers the principles and general rules to protect their data. Rules include reasons why personal data collection is necessary, transparency how and by whom it will be used and stored and for how long, as well as safety measures to not be used by other third parties or for other purposes unless the consumer clearly agreed.**

The paper explores the necessity and awareness to provide personal data to sites, how people provide it, what rights and options there are to protect it and why. Online users and clients are now more aware and receiving information on how their personal data is used by sites and service providers online. Research results on the extent people want and fear to share their personal data are also presented.

The paper presents in detail GDPR rules, requirements, rights and practices, as well as what is personal data and sensitive personal data and the different ways to process and protect it. The research also focuses on special personal data provided by people with disabilities in order to have accessibility on sites and use certain services. In the end, recommendations for sites with accessibility are presented, following GDPR protection requirements.

***Keywords* — accessibility, breaches, collecting data, disability, data bases, GDPR, Internet, personal data, processing, protection, regulation, sensitive data, security, services, rights, sites.**

I. Introduction

In 1998, a law was introduced in the EU about how your personal information needs to be protected. This law is called the Data Protection Act. Since General Data Protection Regulation 2016/679 (GDPR) EU law on data protection and privacy in the European Union and the European Economic Area came into force in 2018 companies, authorities and all legal entities have been struggling to comply. If they fail to achieve GDPR compliance, they are subject to potential lawsuits, data leaks, penalties and fines. GDPR requirements apply to each member state of the European Union, aiming to create more consistent protection of people's personal data across the EU.

In practice, most of the sites collect personal data to function or provide a service, including news sites and the social networks, which most of the people use. Online users should agree their data to be collected and saved in order to be able to use the service.

In order to correspond better to consumer needs and preferences, more sites are made with a programming code that detects what a user likes and wants. For example, if you buy baby goods via your Apple phone, then the site owners would most likely know that you are a parent of a newborn child, aged between 20 to 45 years old, using smartphone internet and applications and likely to buy expensive and complex technological household products. Having this data, a site or related site, social network page and service provider can offer you automatically (often without your understanding) other suitable products and services for a parent of this age in the specific location. Providers of movies and video like Netflix and You Tube also have programming code that detects what you like to watch most often and offers you other similar content. Generally, that makes the consumer happy, because he or she receives offers that are more suitable to him/ her, but what happens when the consumer does not want his actions and preferences online to be known and used by sites, their owners or third parties? What happens if their detected preferences and personal data are misused? Moreover, sensitive data containing race, religion, ethnicity,

disability, mental health condition or certain group memberships, can be used for disqualification and discrimination of people, when they apply for a credit, insurance, job, rent or something else.

A Visually or hearing impaired person often needS to notify the programming code of a visited site, that he or she has disabilities, by clicking a button or link, in order to see a specific content, which makes the site or service online accessible for him or her. The impaired user is not always explicitly asked to provide this personal data, as the site code detects and follows site clicks and actions and this way it makes analytical conclusions about the people using the site. This raises moral, ethical and legal questions and concerns many entities – companies, institutions, clients, marketing and software development experts.

Sites with accessibility should be especially careful and have protective mechanisms to not violate GDPR, to not misuse the collected sensitive personal data or have a software weakness and breach, enabling others to misuse it.

To explore this matter further, the paper will present in detail GDPR rules, requirements, rights and practices, as well as what is personal data and sensitive personal data and the different ways to process and protect it. In the end, the paper will present recommendations and good practices for sites with accessibility, following GDPR protection requirements.

II. Exposition

Digital world made it possible for large amounts of data to be easily collected, stored, transferred and used or misused. A misusage of stolen data from not well protected sites and servers can lead to great damage for the individuals concerned and even change political, social and economic environment in a country. As the hacker attacks increase [1] and the threat grows, this also increases the concern of people, public and governments and the need to be more aware and protect better personal data. Data leaks and breaches in security can harm significantly not only individuals, but also the image and financial state of the sites and data controllers concerned, due to media scandals and lawsuits.

1. Personal Data Leaks

The most common reasons for data breaches and leaks include: malware, weak, guessed or restored passwords with weak authentication methods on one level, fishing emails with false misleading data, software vulnerabilities - poorly designed or flawed software applications or not enough secure cloud connection sharing data system, unauthorized access or unauthorized and consented transfer of data to third parties, not related to the reason this personal data is collected and processed.

A 5.1 million BGN penalty was imposed in 2019 to the Bulgarian National Revenue Agency for the breach of personal data of 4,1 million Bulgarian citizens. Many citizens believe this penalty and protection measures were not enough, as in 2020 there were new attempts for online fishing breaches of people and companies with a fake email sent with BNR's domain name - nra.bg.

If access control is not adequate, it can also easily lead to a data breach. In July 2019, the Dutch Data Protection Authority (DPA) issued the country's first ever GDPR healthcare related fine [2]. The Hague's largest hospital, Haga Ziekenhuis, was fined €460,000 for failing to secure the personal data of one of their patients. The Dutch DPA stated that at least two of the hospital's security measures were insufficient. Not only did the hospital fail to alert administrators that an unauthorized employee was looking into personal files, but the hospital also failed to use a two factor authentication for accessing the database itself. 620 million accounts were stolen in 2019 from 16 hacked websites and they were subsequently sold on the dark web.

Facebook announced a massive security issue affecting at least 50 million users on 09.25.2018. Afterwards, on 19.12.2018, Facebook gave some companies more extensive access to user's personal data than it has previously revealed, letting them read private messages or see the names of friends without consent, according to a

New York Times report [1]. Facebook is facing also international investigations into the illicit harvesting of about 87 million users' personal data and then developing a software program that profiled those citizens to predict voting patterns and, through micro-targeted ads, influence US citizens' voting decisions. Facebook's Personal Data Tracking and usage for advertising purposes has also been a concern since long and governments are now trying to do more about limiting this tracking data collection and protecting the user more.

YouTube is also struggling in the last 2-3 years to refine and improve their advertising policies and methods, as they also record and use behavior and preference related data, collected from user accounts.

In 2018 Google engineers discovered a software leakage within the Google+ API used in the social media network. As over five million user's data was compromised, this led to the immense news coverage on consumer privacy levels within Google+ and the shutting down of the Google+ consumer social network on 2 April 2019.

On 20.11.2018 an Instagram software bug, connected to their GDPR and data protection tools, exposed many user passwords.

On 01.08.2018, Reddit said an attacker breached several employee accounts in mid-June.

In May 2018 Twitter asked 336 million users to change their passwords after the company recently discovered a bug that stored user passwords in plain text in an internal system.

2. GDPR – General Data Protection Regulation

„The Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data [3]." It makes sure that personal data in the EU is collected in a fair, responsible and lawful way by data collectors and processors. It also prevents organizations from collecting more personal data than they actually need in order to provide the certain service. For instance, you don't need to tell an e-commerce online shop your gender or nationality when you buy a camera or kitchen appliance products. Data controllers are organizations, institutions, companies and data processors are their suppliers. They often use personal data to deliver products and services and they must both ensure that the data is managed safely and securely. Sometimes data processors receive the requests and may have to help data controllers fulfill them. Under the GDPR the persons, whose data is used, are data subjects and they can check and control how their data is being used and if it is safe enough. These controls are the new rights for data subjects. Data controllers have a legal obligation to respond to requests from data subjects and provide information on how their data is handled.

Protecting rights of people

The new law outlines specific rights for individuals (Figure 1) – subjects of personal data, concerning processing their personal data or GDPR rights. It also makes sure these rights are followed.

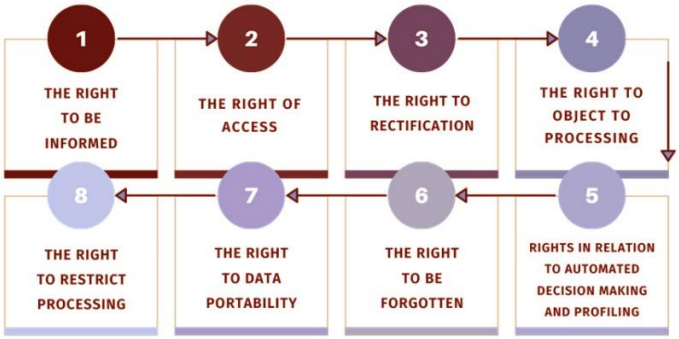

Figure 1. GDPR rights of people

1. The right to information – the right to be informed about the processing of their data. Data controllers have to give clear and concise, understandable information in this regard. It includes also requiring the consent of subjects for data processing.

2. The right to access of personal data free of charge and in an accessible format.

3. The right of rectification – editing, renewing with up to date data, completing the data.

4. The right to object processing of their data or part of their data if they have not given their consent.

5. The rights in relation to automated decision making and profiling.

6. The right to be forgotten - erasure of collected data, right to be forgotten/deleted, used only for a certain period of time.

7. The right to data portability of personal data to themselves or to another controller.

8. The right to restrict processing – to stop processing data for certain things.

GDPR also includes the following *requirements* to data handlers:

- Consent of subjects for data processing
- Providing data breach notifications
- Safely handling the transfer of data across borders
- Requiring certain legal entities to appoint a data protection officer to oversee GDPR compliance
- Anonymizing collected data to protect privacy

3. Understanding and Consent to Sites Collecting Data and Using GDPR Protection by People

According to Eurostat's 2020 Community Survey [4] on Communication Technologies (ICT) and their usage in households and by individuals, 1 in 2 people aged between 16-74 years refused to allow the use of their personal data for advertising purposes, when using the internet for private purposes in the preceding 3-month period. Moreover, 46% reported that they only allowed restricted access to their geographical location, or refused access to this information entirely. Only 40% of EU citizens read privacy policy statements before providing personal data. Similarly, 40% have limited access to their social networking site profiles, content or shared online storage. Meanwhile, only 33% checked that the website where they provided their personal data was secure. The highest results on private data usage trust in sites were observed in the Netherlands (73%), Finland (70%), Denmark and Germany (both 63%), and Spain (62%). In contrast, the lowest shares were recorded in Bulgaria (10%), Romania (20%), Greece (29%), Slovakia (30%) and Latvia (32%).

Pew Research Center's survey [5] about personal data shows that 81% of Americans think the potential risks of data collection by companies about them outweigh the benefits. 77% of Americans say they have heard or read at least a bit about how companies and other organizations use personal data to offer targeted advertisements or special deals or to assess how risky people might be as customers. 79% of Americans are not confident about the way companies will behave when it comes to using and protecting their personal data. Roughly 7 in ten or more say they are not too, or not at all, confident that companies will admit mistakes and take responsibility when they misuse or compromise data. Akamai Research shows that 54% of the respondents are highly likely to walk away from a business that requires them to provide highly personal data (such as email or phone number), in order to conduct business with them.

One of the results in Emarketer's e-commerce research is that 80% of the respondents stated they would be comfortable sharing personal information directly with a brand for the purposes of personalizing marketing messages. However, only 16.7% said they would be OK with sharing this type of information through third parties.

From all stated research we can make the suggestion that the majority of users, who know that their personal information is collected and used, when they visit a site and receive a service or product, via cookies or other software and data collection method, are ok for their information to be used, as long as it is secure, not misused and not shared with third parties for other purposes without consent.

Personal data collectors should put more effort in securing their sites and developing GDPR protection mechanisms in order to keep the trust of the people.

4. Definition of Personal and Sensitive Data and Bases for Processing

Personal information or personal data is any information about a person that identifies him/her in any way as an individual. People can be

identified or classified by many criteria, not only by their name. Their characteristics and personal data are protected by personal data rights and not meant for everybody to know. *Personal data,* subject to GDPR protection can include, but is not limited to:

1. Name, identification number and documents
2. Family and demographic information – age, sex, location, marital status, children, etc.
3. Fingerprints, signatures and genetic information
4. Health information and state, medical records
5. Financial information
6. Home and work information
7. Online and offline behavior patterns and interests
8. Used devices and IP addresses
9. Economic, cultural and social identity
10. Leisure activities and hobbies
11. Travel history

Organizations do not always need to seek consent to process personal data. Consent is only one of six lawful grounds for processing personal data according to Article 6 in GDPR law [3], and the strict rules regarding lawful consent requests make it the least preferable option.

There are six lawful bases for processing personal data[3]: 1) giving consent for processing with certain purpose; 2) processing is necessary for a contract; 3) processing is necessary for compliance with a legal obligation to which the controller is subject; 4) processing is necessary in order to protect the vital interests of the data subject or of another natural person; 5) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority; 6) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (for example for insurance or debt payment). However, consent is needed to process sensitive personal data [3]. Sensitive personal data should be protected better than other personal data. It is often encrypted and/ or pseudonymised [6].

Sensitive data includes the following information about an individual:

1. Sexual orientation and life, gender reassignment
2. Disabilities, as well as health and mental conditions (includes pregnancy)
3. Union memberships
4. Political opinions and group memberships
5. Religious beliefs, race, ethnic origin
6. Genetic and biometric data

If an organization has identified that the data they are handling is or could be special category data, then they need to comply with the requirements under Article 9 of the GDPR [3]. Conditions for processing special category data are:

(a) Explicit consent

(b) Employment, social security and social protection (if authorized by law)

(c) Vital interests

(d) Not-for-profit bodies

(e) Made public by the data subject

(f) Legal claims or judicial acts

(g) Reasons of substantial public interest (with a basis in law)

(h) Health or social care (with a basis in law)

(i) Public health (with a basis in law)

(j) Archiving, research and statistics (with a basis in law)

Substantial public interest conditions may include: statutory and government purposes; administration of justice and parliamentary purposes; equality of opportunity or treatment; regulatory requirements; preventing fraud; insurance; political parties; support for individuals with a particular disability or medical condition; Counseling. Understanding of substantial public interest conditions may vary in different countries and practices and is yet to be understood better in practice.

Sites in the health care sector, both private and public, containing sensitive data of vulnerable individuals must provide more protection to sensitive personal data and pay special attention to GDPR regulation. With the help of cloud-based technology, systems containing patient data are often transferred or shared among hospitals, institutions, GPs, pharmacies in order to serve patients best. But how should this sensitive data be processed and shared according to the GDPR?

For example, a cloud-based system often used within healthcare is the Dutch MedMij, which

creates a personal health environment (PHE) to manage and share medical data. It involves a set of agreements between stakeholders like software developers, healthcare providers and patients, as well as a financing system and information standards, to facilitate data sharing and also mitigates concerns around data privacy, awareness, and interoperability.

Points of access and double authentication of authorized personnel is also necessary to prevent breaches in information security. Regular software checks should be done and notifications must emerge automatically if there is an unauthorized access, suspicious data transfer or breach in security. Sharing data to third parties should also have lawful basis and/ or consent.

5. Definition of Web Accessibility

Web accessibility means that websites, tools and technologies, are designed and developed so that people with disabilities can use them. More specifically people can: perceive, understand, navigate, and interact with the Web; contribute to the Web; Web accessibility encompasses all disabilities that affect access to the Web, including: auditory, cognitive, neurological, physical, speech, visual (Figure 2).

Figure. 2. Types of Disabilities, Source: https://commons.wikimedia.org/wiki/File:Disability_symbols.svg

Visual impairment includes a partial or total inability to see or to perceive color contrasts.

Hearing impairment includes not just deaf people, but also people with reduced ability to hear.

Motor or physical disabilities: People with difficulty moving parts of their bodies, including making precise movements (such as when using a mouse).

Photosensitive seizures: Conditions such as epilepsy can cause seizures that are often triggered by flashing lights.

Cognitive disabilities: There are also many conditions that affect cognitive ability, such as dementia and dyslexia.

To work around these issues, many people use assistive technologies and software to browse the internet. This includes screen readers that vocalize the text on each page, speech recognition software that converts speech into text, Braille terminals, and even alternative keyboards that accommodate special needs.

As disabilities can vary a lot it is hard and nearly impossible to make a site accessible for all types of disabilities. Most of the sites focus on providing suitable content for people with visual, hearing impairment and people who might have photo sensitive seizures or mental vulnerability to sensational, shocking, depressing or violent content.

According to Eurostat statistics in 2017 a quarter of the EU population aged 16 or over reported long-standing disabilities [4]. This means that they felt some, or severe limitations in performing their everyday activities for a period of six months or longer. The EU and its Member States are committed to improving social and economic situation of persons with disabilities. Respectively this will affect not only institutions, but also service providers and organizations. Internet and sites must be accessible and provide equal access and equal opportunity to people with diverse abilities. Accessibility supports social inclusion for people with disabilities as well as others, such as older people, people in rural areas.

6. Recommendations for Making Websites More Accessible and GDPR Compliant

The following recommendations were gathered for making websites more accessible, using analytical research reviews of sites with accessibility, as well as frequently outlined points by web developers [6] and specialists about GDPR and disabled people for testing.

It is necessary to determine GDPR requirements on the site before it is even designed, if that is possible. It is harder to redesign already existing, complex cloud

connected sites and platforms in a way that they can comply with GDPR multilevel personal data security requirements. Transfer of data to new sites or systems can also be challenging in terms of security and preventing breaches.

6.1. GDPR Compliant Site Recommendations

Sites of organizations should be more *simple and functional* than flashy and beautiful in order to comply with both GDPR and accessibility.

Content should be well organized and not neglecting impaired people's needs. It is better that they would not need to find a special button in order to be sent to another singular page or content, which is only accessible. First, this way it is harder for them to reach the content, second it may not have the full actual content and functionality of the rest of the site and third, separating vulnerable, disable people's content from the rest of the site content can pose a threat for GDPR related personal and sensitive data usage.

Sites should collect less data of the users or only the necessary data in order to fulfill their services. Every unnecessary additional data for marketing purposes can be questioned and judged in court if used for other purposes and the person did not allow this explicitly with consent.

Informing consent forms and revoking forms for personal data usage, *cookies usage and general regulations pages* on the sites must be easy to enter, understand and use in any moment. Visually or motor impaired people often have difficulties with pop-up windows on sites. Using such pop-up windows is a common practice that should be reconsidered or improved.

Methods for secure storing, protection, processing and transfer of personal data on sites must be implemented and consulted with a GDPR lawyer or specialists while sites are developed or improved. Double access authentication security measures and processes for updating personal information are recommended for users on the sites to protect their data.

Collected information on sites should be used only for the reasons it is initially collected and by the same legal entities. When public interest is in place or statistical usage of the information then individual values of the information should be *pseudoanonymized* [7].

Personal data must not be collected and stored longer than needed. For example, if the personal data is given for applying a credit, then this personal data must be deleted after the individual has paid and covered in full the credit or the individual should agree again when closing the credit, for personal data to be used further by the collector for marketing purposes.

A site or platform must have a clear and easily accessible process for *revoking and deleting personal data* if demanded by the user and not necessary for further services, statistical or legal reasons or public interest.

Sensitive data can, and in many cases must, be *pseudonymized or anonymized.*

The GDPR does not apply to anonymous data, which means that such data can be used more freely. Anonymization of personal data means that data will no longer be linked to an identified or identifiable natural person and therefore not be considered as personal data. Anonymization is a method that replaces original clear data with a value that is both unrelatable to the original data and permanently irretrievable. Anonymization is most often used when the original source of data never needs to be, or is not allowed to be, disclosed, such as in the case of a medical study.

The process of anonymization can be used for personal data protection and GDPR compliance in two main ways: 1) as part of the "privacy by design" strategic work – with the goal to improve the protection of the processed data; or 2) as part of the "data minimization" strategy – where data can be anonymized, used and transferred without the risk of harming the data subjects.

Pseudonymization is a method and technique used by site security experts or government officials to hide the personally identification information in order to maintain data structure and privacy of information and comply GDPR regulations without needing to ask specifically for consent or if data needs to be transferred to an outsourcing service data handler without disclosing the data. Pseudonymization takes identifiable data and replaces it with a value that

cannot be linked to a specific individual without additional "key" interpreting information that can be accessed elsewhere.

Pseudonymization [7] is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. A single pseudonym for each replaced field or collection of replaced fields makes the data record less identifiable while remaining suitable for data analysis and data processing. GDPR Article 25 [3] identifies pseudonymization as an "appropriate technical and organizational measure". Article 25 requires controllers to: "…implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed [3].

One way to decide whether certain personal data needs pseudonymization is to consider not the data set, but the level of access. Typically, in pseudonymized data, people cannot be identified without an encryption key. Assuming other organizational safeguards are in place, if a holder does not have the key, those data should be considered anonymized in the hands of the holder. Pseudonymized data can be restored to its original state with the addition of information which then allows individuals to be re-identified, while anonymized data can never be restored to its original state.

6.2. Information Structuring and Design of Accessible Sites

6.2.1. Structuring and Design

The accessible sites usually have soft, clear colours, without shadows and sudden colour tone shifts, suitable for people with colour sensitivities or colour perception disorders. Colours containing big amount of red and green can be not suitable for dalnonists.

Alt text description can be added to all images in order for a person with impaired vision to understand their content.

Automatic flash and lighting media must be avoided as it can be confusing, frightening, surprising and hard to turn off. For people with photosensitive seizers such flash media can be not just posing discomfort, but also a health threat.

Text should have a contrasting different colour and bigger font size. If possible, without confusing the site design and structure, text can be resizable for people with impaired vision that need bigger letters to read. Resizable text is also useful for making the site to be adjustable to different screen sizes and devices, including mobile and big TV screens.

In order to structure content on the site correctly, each field should be *clearly labeled with headers*. This helps not only for accessibility and easier finding of content on the site, but also for SEO optimization – easier finding of the site by search engines.

Forms for text writing can be designed with plug-ins like Caldera Forms builder to be accessible.

Tables design on the sites should be avoided except for tabular data, or if necessary to put such on the side then HTML markup is needed to indicate header cells and data cells and define their relationship. Site developers can use tutorials like *WAI Tutorial* [8].

Simplicity and Easy Functionality, Hyperlink connections, Search option

People with cognitive conditions and even normal people can have difficulties reading and understanding long complicated sentences. That is why, when preparing text and content on the site it should be made with accessibility in mind – simple explanations and sentences, short sentences, descriptive names where it is necessary, and more anchor hyperlink texts, less buttons and complicated design with many pictures and media.

Adding a search field on a site helps both impaired and other people to navigate and find easier information on a site. Some search fields and forms can operate also with voice control.

For the search option to be fully accessible and useful, site developers also need to make sure that all pages are indexed, and that the sorting of the search results is helpful.

Assistive Technologies for people with motor disability [9,10]

People with motor disabilities can choose

from a variety of assistive technologies to navigate in the Internet. Common motor assistive technologies include head wands, mouth stick devices, a single switch device with a large button or a touch-sensitive pad. Special software is often necessary to translate those assistive technologies into computer commands.

Eye-tracking devices are used by people with less or no hand muscle control to navigate the web.

Voice recognition software offers some users the option to navigate the web via direct voice commands smoothly. Some searches on sites, platforms and applications are also using voice recognition and control.

Most of these motor assisting technologies work with, or emulate, a keyboard interface. Despite the wide variety of motor disabilities, assistive technologies are often designed with broad purposes that can apply to multiple types of disabled individuals.

Unfortunately, assistive technologies by themselves are often not enough to make the web accessible to users with disabilities if sites do not have accessibility compatible content and design.

6.2.2. Making Sites Suitable for Only Keyboard Navigation and Usage

Despite the availability of oversized and adaptable models, people with motor disabilities often find it impossible to use a mouse. Most assistive technologies that people with motor disabilities use emulate a keyboard in some way. By making a website, platform or application *effectively usable with a keyboard*, you can also enable users of these assistive technologies, in particular by reducing the number of actions that require too many key presses, which can be complicated and tiring for people with motor impairments.

All content on the sites should be easily accessible. Tags can be put on the content of the page. Dynamic content can be tagged as a *"live region,"* which enables screen readers and similar devices to understand the content as it changes or *ARIA Landmarks or skip-to-main links*, which are invisible links that let users skip menus. It is crucial to make navigation easier as it lets users skip directly to specific content.

This way, users with impairment will not need to tab through every menu item just to get to your main content and can easily pass over other link-heavy sections. *WAI-ARIA Guidelines* can be also used for making elements on web pages accessible via keyboards and keyboard emulators [8].

Practical ways to navigate on the site with only a few clicks can include a *skip-to-the-end, skip-to-content* or search function on long pages and long lists. Another way to reduce the keyboard clicks, needed for navigation, is to *structure navigation menus as a multi-level tree*. Instead of scrolling through an entire list of available pages, users can jump to the section of the navigation that they are looking for with only a few clicks.

III. Conclusion

The recommendations above can be used for creating a methodology and good practices guidelines for accessible, GDPR complying, sites and platforms. Security of personal data and GDPR are important topics for institutions, business, international organizations, NGOs, statistical agencies and service providers, especially when they interact and transfer data or use complex cloud technology for access, which can pose security threats.

GDPR regulations are still being clarified on their meaning and practical use [11]. Some situations and cases can make precedents and this poses new legal and ethical questions on how GDPR should be applied in specific areas and situations. For example, when is public interest for processing data really valid? Or what happens if a person's consent is revoked but data has already been used and the person did not understand? What if a disabled person cannot understand or reach GDPR site's general rules and explanations about processing his personal data on a site? The common rules of the site might imply consent for processing or transferring such information to third parties but an impaired person might not understand that.

The health care sector and accessibility on sites are related to sensitive personal data and,

therefore, such sites and platforms should be especially careful for GDPR violations to vulnerable people or security data breaches and data stealing.

Another matter of concern and future research is: Where is the border between collecting data for public and personal interest, or statistical reasons, and misusing this data for something else due to the broadly written consent agreement? The matters of training of personnel concerned with GDPR, as well as finding good guidelines for software developers and managers, and defining levels of access in security systems concerned, are also important.

GDPR personal data security methods and practices applied in different sectors and institutions have to be explored further in order to show good and bad examples and how security systems and methods can be improved.

ACKNOWLEDGEMENTS

This research was funded by the National Science Fund of Bulgaria (scientific project "Digital Accessibility for People with Special Needs: Methodology, Conceptual Models and Innovative EcoSystems"), Grant Number KP-06-N42/4, 08.12.2020.

REFERENCES

[1] Wikipedia, List of data breaches, 19.05.2021, https://en.wikipedia.org/wiki/List_of_data_breaches

[2] Privacy Perfect, Healthcare institutions and GDPR compliance in a digital world, 7.05.2020, https://blog.privacyperfect.com/healthcare-institutions_gdpr-compliance-in-a-digital-world

[3] Proton Technologies AG, *Complete guide to GDPR compliance*, Article 1, Article 6, Article 9, Article, 25, https://gdpr.eu/tag/chapter-2/

[4] Eurostat, How do EU citizens manage their personal data online? 1 in 4 people in the EU have a long-term disability, 2018; 2020, https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20210128-1 , https://ec.europa.eu/eurostat/web/products-eurostat-news/-/EDN-20181203-1 https://dataprivacymanager.net/100-data-privacy-and-data-security-statistics-for-2020/

[5] Data Privacy Manager, 100 Data Privacy and Data Security Statistics, 20.08.2020.

[6] Dreamhost.com, Make your websites accessible, Tutorials, https://www.dreamhost.com/blog/make-your-website-accessible/

[7] Wikipedia, Pseudonymization, 22.05.2021, https://en.wikipedia.org/wiki/Pseudonymization https://www.w3.org/WAI/standards-guidelines/

[8] Web Accessibility Initiative, WAI-ARIA – W3C Accessibility Standards Overview, 09.09.2020.

[9] *Assistive Technologies and Computer Access for Motor Disabilities*, IGI Global book series. 2014, ISSN: 2327-9354; eISSN: 2327-9370.

[10] Progress-Telerik, Motor Disabilities and What You Need for Accessibility, 30.07.2019, https://www.telerik.com/blogs/motor-disabilities-and-what-you-need-for-accessibility

[11] ICO - Information Commissioner's Office, Special category data, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/