TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Aditya Iqbal Bagaskara 184065IVSB

# Privacy-Oriented Web Design and Analytics: A Case Study of Estonian Higher Education Institutions' Websites

Bachelor's thesis

Supervisor: Kaido Kikkas

Doctor of Philosophy
(PhD) in Engineering

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Aditya Iqbal Bagaskara 184065IVSB

# Privaatsusele orienteeritud veebidisain ja -analüütika: Eesti kõrgkoolide veebilehtede juhtumiuuring

bakalaureusetöö

Juhendaja: Kaido Kikkas
Tehnikateaduste doktor

Tallinn 2021

# Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Aditya Iqbal Bagaskara

17.05.2021

# Abstract

The GDPR and the ePrivacy Directive are the legal acts produced by the European Union that aim to create a more privacy-respecting environment in electronic communication media. There has been a considerable amount of research to identify websites' compliances on GDPR and ePrivacy Directive, but it is often focused on more popular and bigger websites. The author raises concern about the state of compliances in the education sector and specifically Estonian higher education institutions' websites.

In this thesis, the author evaluates Estonian higher education institutions websites' privacy by design concept on their web analytics implementation, third-party cookie usage, the clarity of privacy policies, and obtaining user's consents. The author uses the case study method from five out of fifteen examined websites and creates SWOT analysis to better explain the good examples and violations of GDPR and ePrivacy Directive. The analysis will indicate the common violations as well as good examples that can be used by other organizations and web publishers.

The finding of this research will help Estonian higher education institutions as well as web publishers and digital marketers to embed privacy into their website's user experience using the GDPR and ePrivacy Directive as the legal framework.

This thesis is written in English and is 70 pages long, including 11 chapters, 19 figures, and 2 tables.

# Annotatsioon

GDPR ja e-privaatsuse direktiiv on Euroopa Liidu koostatud õigusaktid, millede eesmärgiks on luua privaatsusest lugupidav keskkond elektroonilistes suhtlus- ja infokanalites. Veebisaitide GDPR-i ja e-privaatsuse direktiivile vastavuse kohta on tehtud mitmeid uuringuid, aga paraku on need sageli olnud suunatud populaarseimatele ja suurimatele kodulehtedele. Autoris tekitab muret seadusele vastavus haridussektoris - eriti just Eesti kõrgkoolide veebilehtedel.

Selles uurimustöös hindab autor olukorda Eesti kõrgkoolide veebilehtede privaatsuse kontseptsioonide kasutamist külastusanalüüsi meetodite rakendamisel; kolmandate osapoolte küpsiste kasutamist; privaatsuspoliitikate selgust ja kasutaja nõusoleku omandamist. Autor kasutab juhtumiuuringu meetodit ja SWOT-analüüsi viiel veebilehel uuritud viieteistkümnest, et paremini esile tuua GDPR-i ja e-privaatsuse direktiivi nii korrektset kui ka ebakorrektset kasutamist. Analüüsi tulemus loob ülevaate levinuimatest rikkumistest ja ka headest näidetest, mis võiksid olla eeskujuks teistele organisatsioonidele ja kodulehtede koostajatele.

Selle uurimustöö tulemused on abiks nii Eesti kõrgkoolidele kui ka teistele veebilehtede koostajatele GDPR-i ja e-privaatsuse direktiivi raamistike juurutamisel kodulehtede privaatse kasutuskogemuse tagamiseks.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 70 leheküljel, 11 peatükki, 19 joonist, 2 tabelit.

# Acknowledgement

The author of this thesis wishes to express his sincerest gratitude and appreciation to the following persons who have helped the process of crafting ideas, research, formulation, and structuring this bachelor thesis.

I would like to thank Mr. Kaido Kikkas as my supervisor who has helped me to formulate my ideas and give continuous support for me to develop the main goal of my research.

Secondly, I would like to thank my colleague and friend, Vicente Felippe Alvarez-Retamal. From him, I gained insight towards the startup business in which the whole responsibility of running a company and products fall into a limited number of people. His insight towards building compliances on his company's website makes me realize how important it is as a business owner and website owner to comply with GDPR and ePrivacy Directive that respects their customer's privacy. He has also given me insight towards the digital marketing and web analytic platform and introduced me to different possible approaches on complying with GDPR including the usage of Privacy-Oriented Web Analytics.

In addition, I would like to thank Uku Täht, the founder of Plausible Analytics and a digital-privacy enthusiast. The author receives various insights about digital privacy, neutrality, and independence on the internet. The support and knowledge that I earned from him helped me to understand the goal and importance of my research topic.

# List of abbreviations and terms

| | |
|---|---|
| CCPA | California Consumer Privacy Act |
| CJEU | Court of Justice of the European Union |
| CMP | Consent Management Platform |
| DNT | Do Not Track |
| DPA | Data Protection Authority |
| EEA | European Economic Area |
| EDPB | European Data Protection Board |
| EU | European Union |
| FLoC | Federated Learning of Cohorts |
| GDPR | General Data Protection Regulation |
| HTTP | Hypertext Transfer Protocol |
| PDPA | Personal Data Protection Act |
| PII | Personally Identifiable Information |
| SWOT | Strengths, Weaknesses, Opportunities, and Threats |
| UK | The United Kingdom |
| URL | Uniform Resource Locator |
| UUID | Universally Unique Identifier |
| UX | User Experience |
| WCAG | Web Content Accessibility Guidelines |

# Table of contents

1 Introduction ..... 12
2 Theoretical Background ..... 14
2.1 Legal Background ..... 14
2.1.1 The GDPR ..... 14
2.1.2 The ePrivacy Directive ..... 15
2.1.3 Data Privacy Regulations in Estonia ..... 15
2.1.2 The Upcoming ePrivacy Regulation ..... 16
2.1.5 Comparison Between Data Privacy Legal Framework ..... 17
2.1.5.1 GDPR and CCPA ..... 17
2.1.5.2 National implementation of ePrivacy Directive in Estonia and Belgium ..... 18
2.2 Cookies ..... 20
2.2.1 Type of Cookies ..... 20
2.2.2 Obtaining Consent to Use Cookies ..... 22
2.3 Web Analytics ..... 24
2.3.1 Ethics in Web Analytics ..... 24
2.3.2 Privacy-Oriented Web Analytics ..... 26
3 Related Works ..... 28
4 Methodology ..... 30
5 Case Studies ..... 33
5.1 Tallinna Tehnikaülikool ..... 33
5.2 Tartu Ülikool ..... 36
5.3 Eesti Kunstiakadeemia ..... 38
5.4 Tallinna Ülikool ..... 40
5.5 Sisekaitseakadeemia ..... 42
6 Results of Observation ..... 45
6.1 Placing Cookies Before User's Active Consent ..... 45
6.2 Respecting User's Choice ..... 45
6.3 Cookie Banner Notification ..... 45

6.4 Usage of Privacy Friendly Analytic Tools ..... 46
6.5 Privacy Policy Availability and Content ..... 47
7 Improving Privacy on Web Analytics ..... 49
7.1 Google Analytics ..... 49
7.2 Open-Source Privacy-Oriented Web Analytics ..... 51
8 Discussion ..... 54
8.1 The Role of GDPR and ePrivacy Directive on Internet Privacy ..... 54
8.2 Promoting Active Consent and Web Accessibility ..... 55
8.3 The Future of User Tracking Mechanisms ..... 56
9 Recommendations ..... 57
10 Further Research ..... 59
11 Summary ..... 60
References ..... 61
Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis ..... 68
Appendix 2 – Additional Screenshots ..... 69

# List of figures

Figure 1. Request Header when DNT is set to True. .....23
Figure 2. Cookie banner notification on TalTech's website. .....33
Figure 3. Cookie consent configuration on granular level on TalTech's website.....34
Figure 4. WAVE inspection of TalTech cookie consent banner.....34
Figure 5. TalTech Cookie banner with pre-ticked box as default. .....35
Figure 6. SWOT Analysis on TalTech's Website. .....36
Figure 7. Cookie consent banner from the University of Tartu website. .....37
Figure 8. SWOT Analysis on the University of Tartu Website. .....38
Figure 9. Cookie Banner Notification on EKA's website. .....39
Figure 10. Minimized shortcut to EKA's privacy policy page. .....39
Figure 11. SWOT Analysis on EKA's Website .....40
Figure 12. Cookie Banner Notification on Tallinn University's website. .....41
Figure 13. SWOT Analysis on Tallinn University's Website. .....42
Figure 14. Request for user's consent to place cookie for Facebook's widget. .....43
Figure 15. SWOT Analysis on Estonian Academy of Security Science's Website. .....44
Figure 16. Initial cookie placement on EDPB website. .....69
Figure 17. Matomo Analytic cookies on EDPB website. .....69
Figure 18. Revoked cookies storage on EDPB website. .....70
Figure 19. IP Anonymization in Google Analytics. .....50

# List of tables

Table 1. Observed institutions, websites, and date of access. ..... 30
Table 2. Observation on privacy policy availability and content. ..... 48

# 1 Introduction

Achieving transparency and accountability in web content is the long goal to reverse the negative impact of the digitalisation era. In the era where user demands more transparency due to privacy concern on the internet, the concept of privacy-by-design and privacy-by-default become an obligation for web publishers when creating a site.

Privacy-by-design and privacy-by-default are principles that should be implemented by web publishers from the beginning. We should expect this principle to be adopted as we visit websites, with users being offered the most privacy-friendly choices. To access and process user data, web publishers must first obtain the user's consent. Obtaining user consent is also necessary when placing user tracking mechanisms such as tracking cookies.

Since its implementation on May 25th, 2018, the effect that the GDPR brings has extended beyond the border of the European Union. Its objective is quite clear which is to regulate companies and stakeholders to be responsible for collecting and processing user’s personal data.

Complying with the GDPR has become a top priority for many companies and organizations that are based in the EU/EEA or dealing with customers from that region. According to the IAPP-EY Annual Governance Report 2019, GDPR enforcement is a top priority for 58 percent of businesses [1].

For a long time, the use of third-party cookies, including for web analytics purposes, has been a source of contention. Before GDPR, its advantage was quite clear for web publishers and advertising platforms, to identify unique users who visits the website, as well as to observe their behaviour across the web to deliver a well-tailored targeted advertisement. The second benefit carries privacy concerns and makes users uncomfortable, especially since this data can be accessed by anyone.

Personal data privacy violations could result in a hefty fine. Vueling Airlines, a Spanish airline carrier, was fined by the Spanish Data Protection Authority for €30,000 because their website did not enable users to customize the usage of cookies in a granular way [2].

It is evident that big corporations still struggle to comply with GDPR. It begs the question of whether companies with far fewer resources have trouble complying with and following this legislation. There are many research that have been done to identify a website's compliances, but it is often focused on more popular and bigger websites. The author raises concern about GDPR compliances in the education sector and in addition the ePrivacy Directive (Cookie Law) which is planned to become a regulation in the future. There is a lack of research that covers this sector and in particular for Estonian higher education institutions. The author's main research questions are as follows:

- What is the state of compliances of Estonian higher education institutions' websites regarding the usage of cookies for analytical purposes and other purposes?
- What are the approaches taken by Estonian higher education institutions to respect users' privacy on their implementation of web analytic tools?
- What are the most common violations of the GDPR and ePrivacy Directive in Estonian higher education institutions' websites?
- Which Estonian higher education institutions' website embraces the most privacy-friendly experience?

By answering these questions, we can gain insights on how these institutions try to be compliant with GDPR and ePrivacy directive and learn from some mistakes or good examples to improve the current state of compliances in other higher education institutions websites. This research can also be used to help other web publishers to reach top comply better with GDPR and ePrivacy Directive and embed privacy into User Experience.

# 2 Theoretical Background

This chapter covers insight towards legal aspect, regulation, and other legal acts regarding user privacy in the European Union and Estonia, and additionally California Consumer Privacy Act. This chapter will also bring insight on cookies, web analytics, ethical aspects on web analytics, and privacy-oriented web analytics.

## 2.1 Legal Background

Governments as regulator creates regulations, directives, and other legal acts to guarantee the right of the people they govern are not violated. The rise of data privacy regulations is expected to bring protection for consumers from personal data mishandlings and hold accountable companies and organizations who do so.

### 2.1.1 The GDPR

The GDPR replaces the 1995 Data Protection Directive, which was enacted during the early days of the internet [3] The GDPR is a legal act in a form of a regulation, which is a binding legislative act that is applicable in its entirety to all EU/EEA member states without the need for national interpretation. [4]. The regulation was published in the Official Journal starting from 4 May 2016. On the 25th of May 2018, the regulation became effective in all EU/EEA Member States. [5].

The GDPR impacts organizations, individuals, or companies that provide an online service on their methods of data controlling, including processing personal data of their users. The GDPR will apply to data that are processed manually or automatically in various mechanisms.

Personal data is defined as any information relating to a registered or identifiable natural person, such as a person's name, address, biometric identity, email address, IP address, and gender, as defined in Article 4 GDPR [6]. Under this article, there are three main parties that are covered under the GDPR:

- Data Subject: “Natural person from which the personal data are obtained.”
- Data Controller: “Natural or legal person, public authority, agency, or other body which determines the purposes and means of the processing of personal data.”
- Data Processor: “Natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.”

According to these definitions, website owners or publishers are the data controller. The data controller has the responsibility of determining what information they collect from the users. It is quite common or even becomes a norm for web publishers to implement an analytic strategy to measure the performance of their website. In most cases, web publishers implement various analytics and tracking tools that are prone to include Personal Identifiable Information (PII) intentionally or unintentionally. The problem rises as if the user does not give consent to pass this information to third-party data processors. The consequences of GDPR violation can reach up to €20 million or up to 4% of the annual worldwide turnover [7].

### 2.1.2 The ePrivacy Directive

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (amended in 2009) also known as ePrivacy Directive is the EU directive on data protection and privacy that concerns the processing and protection of personal data in the field of electronic communications [8]. This regulation is regarded as the earlier version of GDPR and is still being implemented to this day.

The ePrivacy directive is also known as EU cookie law even though it is not a law but instead a directive. A directive is an EU legal act that requires each member country to implement and adapt it to comply and accommodate the directive [4].

### 2.1.3 Data Privacy Regulations in Estonia

To elaborate, supplement, and provide implementation standards of the General Data Protection Regulation, Estonian Personal Data Protection Act (Isikuandmete kaitse seadus) was enacted on 15 January 2019 [9]. Additionally, ePrivacy directive is adopted under Electronic Communications Act which was passed on 8 December 2004 [10].

Currently, there are no specific regulations that implements Article 5(3) of ePrivacy Directive in Estonia that regulate the usage of cookies on websites, but it is still necessary to let users know about the use of cookies as well as giving them the option to either accept or reject it [10][11]. Most common practices come from the implementation of the ePrivacy directive and the opinions of the European Data Protection Board [12]. In general, there are requirements to give clear and understandable notice about cookie use and purpose and using cookie walls to force user's consent is not allowed [11]. Consents are required when the cookies contain or can detect personal information, using third-party cookies, and for purposes unrelated to the website visit [13]. Nonetheless, when the ePrivacy regulation becomes effective, there will be some changes that specify the usage of cookies.

The most reliable way to make good examples of web transparency and compliance with the regulation that applies to one country or region is by observing the government's official website. The author takes an example from the Estonian Government's official website (Homepage: https://valitsus.ee). The technology lookup shows that the website currently uses Google Analytics for analytic purposes. However, Google Analytics cookies will not be placed in the user's browser until the user agrees or it will not be placed if the user rejects to give consent

### 2.1.4 The Upcoming ePrivacy Regulation

The ePrivacy regulation is an EU act that has purposes to renew and update the past ePrivacy Directive. As the technology has evolved, there is an increasing need to modernize the 2002 ePrivacy directive to guarantee personal information in the electronic communication sector across all member states. The regulation is supposed to come at the same time as the GDPR and give more specific regulation in the domain of personal data protection in the electronic communication sector.

There are some expectations that are made from European Data Protection Board (EDPB) about this future legislation that the audience measurement shall be limited to non-intrusive practices that are not likely to create a privacy risk for users [14]. Member of European Parliament, Marju Lauristin (Estonia, S&D) presented the report in June 2017 the report to Civil Liberties Committee with an objective to improve the confidentiality of communications in the era where machine-to-machine communications take a major role in the industry [15]. The most recent progress has been made on 10 February 2021

where the member states have settled on a mandate for negotiations with the European Parliament [15].

### 2.1.5 Comparison Between Data Privacy Legal Frameworks

Understanding how data privacy regulations are applied in other regions of the world would help us to gain insight into legal obligations on personal data security when we want to expand an organization's business in the future. The comparison can also show how different regions form regulations and requirements as they can be affected by several factors such as existing legislation, culture, history, geopolitics, and ideology.

#### 2.1.5.1. GDPR and CCPA

An example of a similar regulation to GDPR is the CCPA (California Consumer Privacy Act) of 2018 in the state of California, United States of America. CCPA is a state legislative act and has been effective since 1 January 2020 which affects businesses that deal with Californian residents [16]. CCPA provides several rights for Californian residents regarding their personal data [17]:

- The right to know about how the business collect and with whom personal information are shared to.
- The right to delete collected personal information.
- The right to opt-out and prevent the business to sell their personal information.
- The right to non-discrimination from the business for exercising their CCPA rights

There are several similarities and differences between the two regulations [16]:

- **Territorial scope**

  The most obvious difference is the territorial scope of the regulation where CCPA applies for business that collects and process information for Californian residents while GDPR apply for EU/EEA citizens [16]. The regulations apply regardless of if the organization/business has a physical presence in these regions.

- **Personal scope**

The two regulations aim to protect natural persons and not legal persons such as institutions and organisations while the data controller/business is the party that has the intention of processing the data subject/consumer personal information [16]. There are some differences in CCPA in which the regulation is applied to the organization such as if the organization is for-profit, does business in California, and has annual revenue of more than $25 million. On the other hand, GDPR applies to every natural or legal person regardless of the organizations' size [6][18].

- **Personal Data and Consent on Cookie Usage**

Both GDPR and CCPA classify persistent cookies as personal data/information as they are considered unique identifiers [18]. GDPR and CCPA consent requirements for cookies are a bit different. CCPA does not require an organization to use a cookie banner to obtain user's consent, but it is recommended to do to avoid the risk as using third-party advertisement cookies could be considered as "selling" personal information [19].

- **Monetary Fines**

Both GDPR and CCPA will impose military penalties for non-compliances. GDPR can reach up to 4% of global annual turnover or €20 million, whichever is higher [6]. CCPA's civil penalties amount up to $2,500 for each violation and $7,500 for each violation if the violation is proven to be intentional [20].

#### 2.1.5.2 National implementation of ePrivacy Directive in Estonia and Belgium

As a directive, the ePrivacy Directive requires each member states to accommodate it into a national-level regulation. Cookie usage is the subject that is often talked about since its implementation is very common, and each country's regulation often varied on how strict their requirement is. In June 2014, the Estonian government proposed a draft act that included the provision of cookie usage which was rejected because further research and analysis are needed [21].

In terms of imposing ePrivacy Directive implementation and GDPR, *Gegevensbeschermings-autoriteit / l'Autorité de protection des données* as Belgian Data

Protection Authority (DPA) requires a higher standard of implementation than the equal regulations in Estonia. These requirements are specified directly into the law or DPA-issued recommendations. The stricter requirement is also shown through court case decisions.

- **Presenting information and notice**

Both countries' regulations require information notice to be clear, visible, and comprehensive. Belgium through their DPA recommendations requires websites and organizations to give thorough information about the usage of cookies and obtaining valid consents [22]. Belgian DPA requires that privacy or cookie policy be easily accessible and easy to find on the website's homepage [23].

- **Depth of information and notice**

The law in Belgium requires any information concerning cookies to be shown in a pop-up banner or similar method [11]. The cookie banner needs to carry out a statement such as a possibility for users to refuse the consent to the cookie usage and at least references on how to adjust browser settings to adjust with their further cookie preference although it is still required to gain user's active consent on the first place. In Estonia, there is no detailed local guidance regarding this subject except that both countries state that usage of cookie wall is illegal [11][23].

- **Granular consent**

The Belgian Commission for the protection of privacy suggests a granular approach that provides users options to reject cookies based on their type and purposes [22]. There has been no local guidance or recommendations from Estonia DPA on this subject [11].

- **Legal case**

On 17 December 2019, the Belgian Supervisory Authority imposed a €15000 fine on a website that provides legal information due to insufficient information about the deployed cookies and non-legitimate consent to place cookies including first-party analytic cookies [24]. The court realized that this issue is surrounded by legal uncertainty, nevertheless, it decided to apply the strictest possible requirement in this

case [24]. Meanwhile, there has been no recent enforcement on cookie non-compliances in Estonia [11].

The author took an example from Universiteit Antwerpen (Homepage: https://www.uantwerpen.be/nl/) in Belgium. On the first visit, the website asked for user consent regarding the use of cookies and not placing any non-essential cookies beforehand. Until the user chose to accept all cookies or to allow only certain cookies.

## 2.2 Cookies

An HTTP cookie (web cookie, browser cookie) is a small piece of data that contains information that is sent from the server and placed into the user's web browser to store information to be reused for the stateless HTTP protocol [25]. Cookies can be an essential part of a web application to be able to run certain functionalities and the entire website in general such as to store items in the shopping cart. Cookies can be set from HTTP response websites or by JavaScript running on the client-side.

### 2.2.1 Type of Cookies

Cookies can be defined by the duration it is stored, the party who sets it (provenance), and its purpose [26]:

**Purpose:**

- Strictly necessary cookies

  Strictly necessary or essential cookies are cookies that are regarded as essentials to keep the integrity and functionality of the website. It is not necessary to obtain the user’s consent to use and implement this cookie. Nonetheless, it is recommended that users be informed about the intent of the implementation.

- Preference cookies

  These cookies are also known as functionality cookies. Its purpose will be to improve the user's experience and to consider the user's previous choices. Cookies that remember cookie preferences or language to serve a particular user are examples of this.

- Statistics cookies

These cookies, also known as efficiency cookies, are used to help web publishers understand how users interact with their websites. These cookies are considered secure, and web publishers should not be able to identify the user as a result of their usage. However, the use of these cookies also requires the users' permission.

- Marketing cookies

These cookies are cookies that raise the most concerns about user's privacy. These cookies can track user's activity across the internet outside of the webpage where this cookie is given to help advertisers to give the most relevant advertisement to users.

**Duration:**

- Session Cookies

Session cookies are cookies that persist only for a session. Web browsers will remove this cookie when the user closes the browser, and it makes this type of cookie considered to have minimal privacy risk. Session cookies do not have an expiry date.

- Persistent Cookies

Persistent cookies are cookies that remain in the browser even when the browser is closed. Persistent cookies have a long expiry date which means that they will stay in the user's browser and could be used as a tracking mechanism to identify user's behaviour and preferences when browsing on the internet. Persistent cookies are considered to have a higher security risk.

**Provenance:**

- First-party cookies

First-party cookies are cookies that are set by the website or domain itself. Some examples are to store the language of the user or to remember the consents that the user has given.

- Third-party Cookies

  Third-party Cookies are set to the device, not by the website itself. Instead, the cookies are set by third-party vendors with the permission of the website owner. These cookies are used for advertising purposes and analytics.

### 2.2.2 Obtaining Consent to Use Cookies

The ePrivacy directive is the law that also regulates the usage of cookies, and it is still undergoing revision to be updated in the upcoming ePrivacy Regulation. Currently, GDPR is the regulation that plays the most significant role in personal data protection in the European Union. Despite the significant repercussion that the usage cookies have, cookies are mentioned only once in GDPR recital 30 [27]:

*"(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags."* [28]

Regarding the usage of cookies, it is mandated that organizations require user consents as it is strengthened on the GDPR. EDPB released guidelines in May 2020 on obtaining valid consents based on Article 4(11) of the GDPR [29]. Valid consent must be:

- freely given
- specific
- informed
- unambiguous

The process of obtaining user consents aware discussed in PDP 16th Annual Data Protection Compliance as follow [30]:

- Implied consent cannot be constituted as a legitimate consent

  Consent must be indicated by the user's affirmative act (active consent). Using implied consents is assuming users simply accept cookies if they continue browsing or not adjusting the browser's settings.

- Advice to adjust browser settings will not be sufficient

  Advising users to adjust browser settings such as blocking third-party cookies and browse in private mode does not align with the principles of Privacy by Default.

- Providing opt-out options

  Users have a right to withdraw their consent. Ideally, a website should provide useful information on how they can opt-out from giving consent such as on advertising cookies. This option is more relevant and easier to manage by the website owner in a condition where the user signs up for a service because the web publisher has more control of the user's data compared to the user's personal data that are transported to third-party organizations.

- Response to Do Not Track browser requests

  When the browser sets Do Not Track (DNT) request headers in their browser settings, it indicates their preference to receive personalized or non-personalized content. If the value of DNT: 1, the users prefer to not be tracked on the site. Meanwhile, DNT: 0 means that the user allows tracking, and DNT: null indicates that the user does not have any preference regarding site tracking.

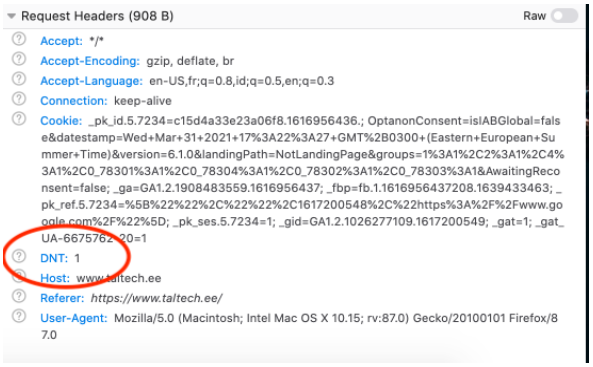



Figure 1. Request Header when DNT is set to True.

- Granular consent control for different cookie purposes

Recital 32(5) GDPR stated that when the data processing has multiple purposes, each consent should be given for all of them. In the context of

distinct types of cookies based on their purposes, ideally, users should be given choices on which cookies they allow and explain each type of cookie's purposes concisely [31].

## 2.3 Web analytics

Web analytics is a part of modern digital marketing strategy. The functionality and benefits of analytics not only help to view daily activities but also to forecast and see the future trend. The most popular client-side web analytics tool currently is Google Analytics which offers a free analytic tool with various functionalities [32]. Most analytics tools inject a snippet of JavaScript into the web page's code to "tag" it [33].

Web analytic tools can provide audience data, audience behaviour, and campaign data to web publishers. [33]. Audience data is defined as combined, detailed information about the user of the website and helps web publishers to know the demographic and typical audiences of your website [34]. The web publishers utilize this tool to obtain information about new and returning users and information like the device that they use. An example of how this data can be used is the ratio of users using mobile vs desktop. Understanding this data can help the web publisher to set priority on their website development such as providing mobile-friendly websites or mobile applications [34]. Web publishers also able to obtain data on user's behaviour on the page such as the most common landing page, exit page, most frequently visited pages, and bounce rates. Campaign data can be used to measure the success of a marketing campaign and the most used keyword for search engine optimization [34].

### 2.3.1 Ethics in Web Analytics

Data that are obtained from web analytics are based on user's data thus there are ethics to consider when implementing them especially when users' data are stored in a third-party server that provides the analytic service and often users are not aware of this transfer of data which can be used or sold for advertising purposes [35]. Therefore, it raises some concerns on the ethical aspects of Web Analytics.

Some minimum requirements that organizations should consider when collecting users' data for Web Analytics are outlined by Kenny, Pye, and Pierce:

- the customer is the owner of information about them
- the customer should be informed on the information the organisation is collecting and for what purpose the information is being collected.
- the customer should have the option not to participate.
- the customer's information should be protected from third-party access.
- appropriate governance on management and destruction of customer data is established.

These requirements were stated in their conference paper, “Ethical Considerations and Guidelines in Web Analytical and Digital Marketing: A Retail Case Study,” [36].

Tools such as Google Analytics by default implement cookies on their web analytics platform. According to the ePrivacy Directive, analytic cookies are not classified as strictly necessary cookies thus it requires the user’s consent before this cookie is placed on the user. The high standard of privacy applied in the European Union tries to minimize the potential of user identification without consent. The analytics process could potentially transmit personal data such as IP address, geolocation, device information, and user’s online activity.

The data collection process plays a vital role at the first stage of the analytic process. An organization needs to determine beforehand what information needs to be collected from users [37]. This stage creates challenges since identifying connections and meaning between variables is often impossible [37]. Thus, there is a tendency to obtain as much information as possible in which some of them are not beneficial for the analytics process, yet they might fall into the category of personal data.

In the case of standard features on Google Analytics, google lineout explicitly under their Terms and Service agreement (Last Updated: 31 March 2021) which requires website owners and publishers to post a privacy policy that discloses that Google Analytics is used, how data is collected and processed, and notifying of the use of cookies [38].

Another popular tool that is used to measure user behaviour on the website is Hotjar. Hotjar offers abilities to explore user interaction in a more detailed way such as with

heatmap or screen recording. Hotjar realizes that implementation of the features of their services requires consent from their website visitor. Hotjar terms of service state that their customer's terms and service and privacy policy should effectively communicate to their users on the usage of Hotjar and other similar services. The objective of this recommendation is to prevent GDPR violations and penalties [39].

### 2.3.2 Privacy-Oriented Web Analytics

Google Analytics is owned by Google, which is a giant technology company that obtains its revenue through advertising. With a strong brand name as the most visited website, Google is committed to building secured protection emphasizing data theft prevention [40]. However, their commitment to preventing personal information theft does not reflect in their approach to collecting user data and profiting from it for their advertisement business [40]. According to Google's privacy policy, they will only anonymize their advertising data by removing part of the IP address only after 9 months. Then, Google will finally delete stored cookie information after 18 months [41].

The popularity of Google Analytics in the digital marketing and web analytics industry is mainly because it is free and has numerous features and the capability to create a website traffic measurement. We all have heard the popular phrase "There ain't no such thing as a free lunch." There are doubts and suspicions that a giant company like google will take advantage of wide usage of their analytic tools to create and profile the end-users of websites that use Google Analytics. The dependability of web publishers with Google Analytics products for analytics purposes has become a concern for many and with the implementation of GDPR, these tools gain more popularity to be used by web publishers to build less invasive and transparent websites.

One of the biggest advantages in terms of transparency on privacy-oriented web analytic tools is most of them are open source. As a non-proprietary tool, open-source tools embrace transparency as there is no way to hide the mechanism of how the data are processed. Self-hosting is often offered as an option if the publisher wants to have full control of the collected information. Some popular examples of this tool are Matomo (Formerly Piwik), Plausible Analytics, Simple Analytics, and Fathom [32].

One of the downsides that might affect the willingness of web publishers to switch to privacy-focused web analytics is less accurate data [42]. An example is that Google

Analytics places cookies in users to distinguish a new visitor from returning visitor. In some analytic tools such as Plausible Analytics and Simple Analytics, web publishers are not able to know if this user has visited their website previously or if they are a new user. Currently, cookies are still seen as the most rational and common way to distinguish between returning users and first-time users. Using privacy-focused web analytics can add additional costs. Even though the cost often is not exorbitant, justifying this extra cost for web publishers who are still used to paying nothing for Google Analytics can be difficult. These additional costs can come either from self-hosting cost, licensing, or when using their cloud service.

# 3 Related Works

There are various works regarding personal data protection, Web transparency, and compliance to GDPR. Under the more specific scope, some of this research focuses on the web transparency aspect as well on achieving compliances and performing audits on Data Protection law in the EU. There are some research that focuses on the ethics of digital marketing even before various data protection laws became concerns as it is currently.

To gain insight into the use of cookies across several industries, Deloitte conducted the research using a sample of 167 websites across 12 EU / EEA across six industries [43]. The survey of websites was conducted between October 2019 to November 2019. The report also points out the practice of nudging which encourages users to give consent to the usage of cookies occurs in 43% of the websites in the scope. The examples of nudging techniques are featuring a big green button that says “Accept Cookies” while the “Reject Cookies” button uses faded colour or red colour which discourages users from accepting that choice [43].

Kenny, Pierce, and Pye from the School of Information Systems, Deakin University, Australia discuss the ethical considerations of digital marketing which collects customer data during the Australian Institute of Computer Ethics in 2012 in their conference paper, “Ethical Considerations and Guidelines in Web Analytics and Digital Marketing: A Retail Case Study” [36]. The paper discusses how ethical standards can help organizations make better decisions. In their perspective, gathering more fine-grained data to provide a unique and tailored experience is vital for a company's marketing campaign, but that should not exceed the boundaries of consumers' privacy [36].

Montana State University through A National Forum of Web Privacy and Web Analytics produced a paper that focuses on the use of web analytics in libraries. The concern was raised as a library is historically known to provide a safe environment for intellectuals that are committed to privacy for the pursuit of information and knowledge [44]. The

forum result is followed up with the release of a practice-oriented action handbook that contains two main parts: Technical and Social Implementation [45].

Between December 2017 and October 2018, the authors of the research paper “We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy” analysed the top 500 most popular websites, according to Alexa country rankings, in every 28 European Union member states [46]. Over this period, the research found positive development on the number of websites that update their privacy policy to comply with GDPR [46]. The study reveals that key web protection mechanisms such as the same-origin policy face some challenges in implementing GDPR-compliant consents. Third-party vendors must cooperate to provide a practical and accessible process for opting out of third-party cookies [46].

# 4 Methodology

The website's observation was done in April 2021. The author observed 13 Estonian higher education institutions' websites which are listed on Eesti.ee [47] and added two additional private higher education institutions into the list, Estonian Business School and Estonian University of Applied Science.

| No. | Name of Institution | Website | Date of Access |
|---|---|---|---|
| 1 | Tallinna Tehnikaülikool | www.taltech.ee | 07/04/2021 |
| 2 | Tartu Ülikool | www.ut.ee | 07/04/2021 |
| 3 | Tallinna Ülikool | www.tlu.ee | 07/04/2021 |
| 4 | Eesti Maaülikool | www.emu.ee | 06/04/2021 |
| 5 | Eesti Muusika- ja Teatriakadeemia | www.eamt.ee | 06/04/2021 |
| 6 | Eesti Kunstiakadeemia | www.artun.ee | 07/04/2021 |
| 7 | Kaitseväe Akadeemia | www.kvak.ee | 06/04/2021 |
| 8 | Eesti Sisekaitseakadeemia | www.sisekaitse.ee/et | 13/04/2021 |
| 9 | Tallinna Tehnikakõrgkool | www.tktk.ee | 06/04/2021 |
| 10 | Tallinna Tervishoiu Kõrgkool | www.ttk.ee | 08/04/2021 |
| 11 | Tartu Tervishoiu Kõrgkool | www.nooruse.ee | 06/04/2021 |
| 12 | Eesti Lennuakadeemia | www.lennuakadeemia.ee | 06/04/2021 |
| 13 | Kõrgem Kunstikool Pallas | www.pallasart.ee | 06/04/2021 |
| 14 | Estonian Business School | www.ebs.ee | 06/04/2021 |
| 15 | Estonian University of Applied Science | www.euas.eu | 14/04/2021 |

Table 1. Observed institutions, websites, and date of access.

From these 15 websites, the author selects 5 institution's websites that can give examples of the suitable or unsuitable way on informing users about their usage of cookies (cookie banner), availability of privacy policy information regarding personal data usage, transparency about web analytics tools that they implement, and overall, how they embed privacy into the user experience (UX).

From each study case, the author will provide a table that outlines a SWOT analysis of the website approach on complying with the ePrivacy Directive, GDPR, and creating a

privacy-first user experience for the users. The strength will explain the good examples of privacy by design user experience and the weakness is the opposite of it. The opportunities explain what can be improved to respect the end user's privacy as well as the benefit that it carries with the website's approach and design. The threat will explain the possibility of violations and uncertainty within the legal aspects and to the website's view from the perspective of the users regarding respecting their privacy.

The research methodology currently has some limitations. The author is focussing on the homepage of each institution's website. The author does not perform the inspection using automation and website crawling methods since the author intends to analyse the UX perspective as a website visitor. Due to this limitation, unfortunately, this research cannot screen through each subpage of the website which might place different cookies on their subpages.

The author implements guidance from Deloitte's Cookie Benchmark study to give more accurate observations [30]:

1. Determining object of observation

   Assessing a self-check for an organization's website needs to comply with existing regulations and the organization's policy. Since the author's objective is to measure the compliance of Estonian higher education institutions' websites with the ePrivacy directive and observe if these websites live up to the expectations of this directive, the author came with this checklist:

   - Cookie notification complies with the transparency requirement
   - End-users can accept or decline cookies
   - Are there any non-strictly necessary cookies placed on the user's browser before active consent is obtained?
   - Cookies are placed accordingly to the given consent
   - Ability to effectively withdraw given consents

2. Using a clean browser and unrestricted internet connection

Deleting all browsing data, cache, and installed cookies will ensure previously obtained cookies do not interfere with the result. Depending on the location and internet service provider, filtering done by the Internet Service Provider could filter out some cookies and tracking mechanism

3. Visiting the website as a new visitor

By deleting the browsing history, the website should not be able to remember if it is the first visit. Usually, a cookie consent banner is given when the website cannot find cookies that store the user's prior consent. There are several observations that the author needs to take in mind at this step; Notifications regarding the use of cookies, Explanation of the notification about the type and purpose of the cookies that will be given, Ability to reject the use of cookies.

4. Adjust the cookie preference options

If the website offers granular cookie consents the website should inform users about the type and name of cookies that will be placed on the user's browser. The author then assesses this preference to verify whether the placed cookies are in line with the given consent.

To perform the cookie audit, the author uses Firefox developer tool in Mozilla Firefox Developer Edition Version 88.0b9 and in some cases Google Chrome Version 89.0.4389.128 to utilize additional extensions. The author uses regular mode (Non-private mode) to demonstrate the default mode that regular end-user uses. To further examine the web analytics technology that this website uses the author uses Wappalyzer, a technology profiler that provides information on what technology is used to build a website.

Cookie usage notifications which are commonly demonstrated in the form of banners are the most significant object of observation. The author will inspect if the cookie banners that they use respect the cookie choice of preference, transparent, and informative. The two most important cookie types to observe are marketing cookies and performance cookies. These cookies have the most significant concerns on the end user's privacy experience since they could provide third-party data transfer and surveillance.

# 5 Case Studies

This chapter covers analysis of 5 institutions websites: Tallinna Tehnikaülikool, Tartu Ülikool, Eesti Kunstiakadeemia, Tallinna Ülikool, and Sisekaitseakadeemia.

## 5.1 Tallinna Tehnikaülikool

Tallinna Tehnikaülikool or TalTech website is taltech.ee. TalTech name will be used interchangeably to Tallinna Tehnikaülikool. The homepage of TalTech is taltech.ee. TalTech's website utilizes Google Analytics, Matomo Analytics, Facebook Pixel, and LinkedIn Insight Tag for their analytics purposes.

The author was only shown the banner in English even when visiting the website's homepage in Estonian. The cookie banner is placed at the bottom of the page. This approach is quite less intrusive and yet still visible for users to notice. TalTech website is the only website from all observed websites that offer options to give granular consent for the users to choose which cookies will be set in the user's browser. The cookie banner that is provided by the OneTrust Consent Management Platform shows three types of cookies with explanations of each type of cookie's purpose: Strictly Necessary Cookies, Strictly Necessary Cookies, and Targeting Cookies.


Figure 2. Cookie banner notification from TalTech website.

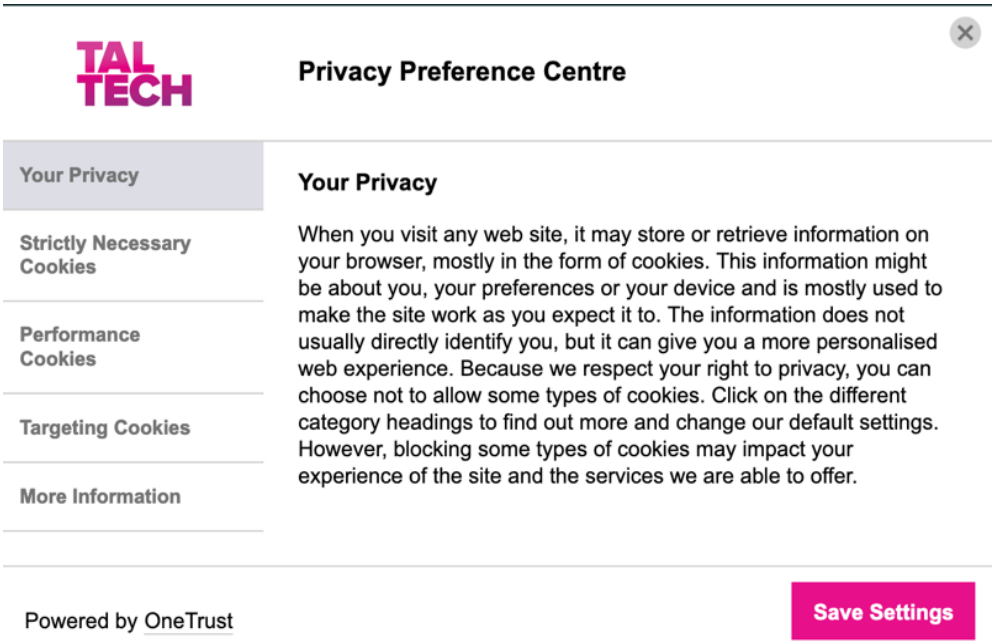



Figure 3. Cookie consent configuration on granular level on TalTech's website.

TalTech website adheres to the WCAG 2.0 AA accessibility criteria, which are a set of guidelines to accommodate accessibility on the internet [48]. The implementation is also reflected on the cookie notice banner. The author inspected the accessibility of this cookie banner notice using the WAVE browser plugin.

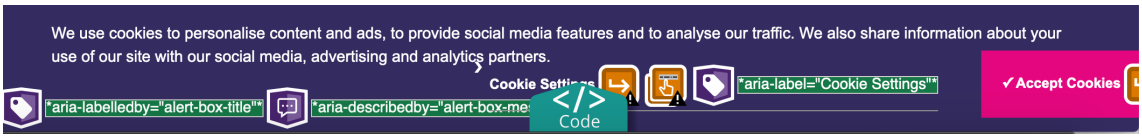
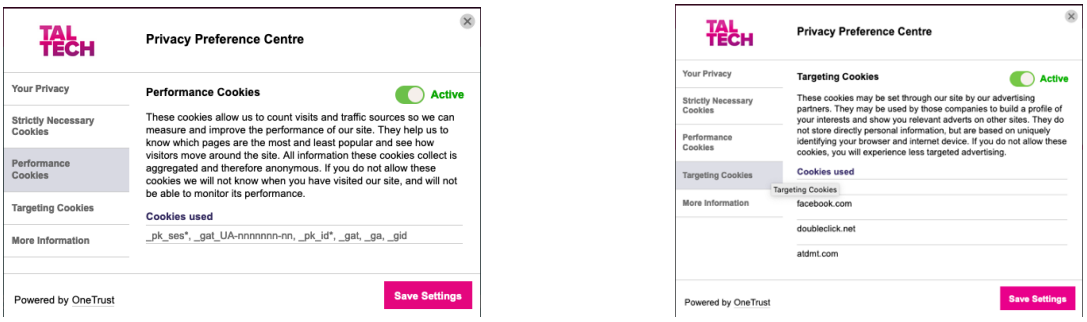



Figure 4. WAVE inspection of TalTech cookie consent banner.

The cookie banner notification places an aria-label "Cookie Settings" which will help screen reader users to find an element in the page. The cookie notification banner mentioned cookies that they use. The performance cookies are `pk_ses*, _gat_UA-nnnnnnn-nn, _pk_id*, _gat, _ga, _gid`. These cookies are used for the website owner to measure web analytics and statistics. The cookies such as `_ga, _gid` and _gat indicate that the website utilizes Google Analytics. The author noticed that TalTech also uses Matomo (indicated by `pk_ses*, and _pk_id` cookies). Matomo is a privacy-focused web analytic tool and this effort is appreciated to embrace user privacy.

When visiting the homepage for the first time, the TalTech website placed non-essential cookies such as Google Analytics and Facebook Pixel before the author gives their consent. There are observable nudging practices by hiding the option to reject all non-strictly necessary cookies. There is a potential violation in the cookie settings section since performance cookies and targeting cookies were by default active. Recital 32 of GDPR indicates that pre-ticked boxes should not, therefore, constitute consents [31].




**(a)** **(b)**

Figure 5. TalTech Cookie banner with pre-ticked box as default (a) Performance Cookies (b) Targeting Cookies.

When the author visits the website for the first time, the website places non-essential cookies before the user gives explicit consent to them. The author then tested the options that are given by the cookie banner notification. To test if the website still sends the data to Google Analytics and Facebook when rejecting the use of all but essential cookies, the author used a Chrome extension called Google Tag Assistant Legacy and Facebook Pixel Helper. The author tested it using Google Chrome since these extensions are only available in Google Chrome. After clearing cookies and cache, the author revisited the website and refused all cookie usage except for essential cookies. The author found that the website still sends data to Google Analytics and Facebook Pixel. The cause could be due to misconfiguration with their CMP manager.

| Strength | Weakness |
|---|---|
| ● Providing a choice to give granular consent<br>● The cookie notification banner is built to be accessible for screen reader user<br>● Using Matomo as a more privacy friendly analytic tool indicates potential in the future to entirely migrate from Google Analytics and less privacy-friend analytics. | ● Non-essential cookies are placed before user's active consent<br>● Nudging practices in the cookie settings choice by setting is on by default<br>● Performance and advertising cookies are still placed in the browser and data keeps transmitted to third-party organizations even when the user does not give consents for it. |
| **Opportunities** | **Threat** |
| ● Compliant way of obtaining consents can improve the trust of the institution as the biggest public university in Tallinn.<br>● Switching entirely to Matomo cookie-less implementation will remove the need to use cookie banners. | ● Unprepared migration to Matomo could create a problem on existing marketing and analytics<br>● Violations such as cookie placement before consents can be categorized as GDPR and ePrivacy Directive violation |

Figure 6. SWOT Analysis on TalTech's Website.

## 5.2 Tartu Ülikool

Tartu Ülikool or the University of Tartu is a public university that is based in Tartu, Estonia. Its homepage website is ut.ee. The technology lookup using Wappalyzer shows that The University of Tartu website utilizes Google Analytics, Moat, and Facebook Pixel to create analytic measurements on their websites.

The University of Tartu implements cookie usage notifications as a footer on their website. Based on the interaction type of this cookie banner, it is classified as confirmation-only [46]. On their first visit, the cookie banner offers an affirmative text informing the user that the website uses cookies to enhance user experience and uses Google Analytics and Facebook Pixel. This notification is provided in two languages

(Estonian and English) out of the three languages that the website is served in (Estonian, English, and Russian).

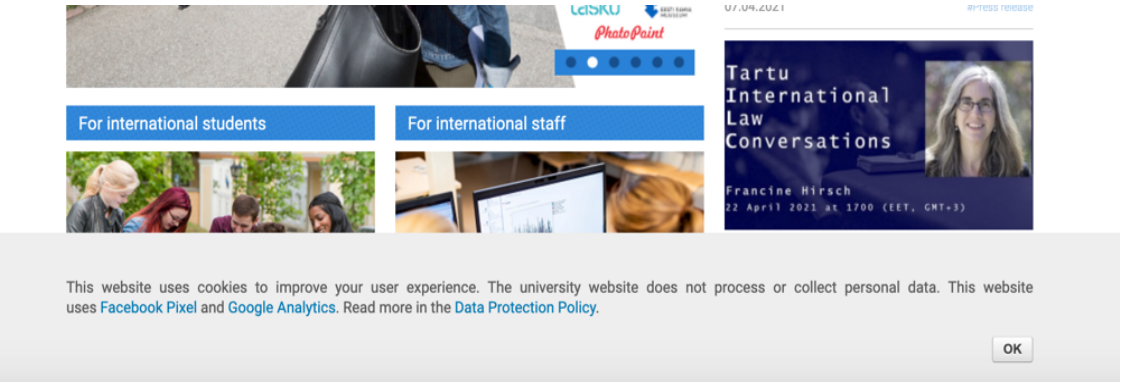



Figure 7. Cookie consent banner from the University of Tartu website.

The problem with this approach is clear that the website does not give an option for users to refuse the usage of cookies and thus does not satisfy the required expectation of GDPR and ePrivacy Directive.

The website placed cookies such as Facebook Pixel and Google Analytics directly into the user's browser before any consent are given to the user. Providing that the cookie banner notification does not give an option to give consents for cookie usages, the author did not expect this action would happen.

| Strength | Weakness |
|---|---|
| • Advertising and analytic partners are mentioned in the cookie consent banner<br>• Easy to find privacy policy | • No option to reject the use of cookies<br>• Privacy policy does not state the use of cookies when visiting the website<br>• Direct placement of cookies on the user browser |
| **Opportunities** | **Threat** |
| • Privacy policy should contain more information regarding advertising partners, analytics, and their cookie policy<br>• Provide option to reject the use of cookies<br>• Introducing privacy-oriented web analytics tools for audience measurements | • The website still has a lot to work on to achieve compliances as expected by the ePrivacy Directive<br>• Violations such as cookie placement before consents and no option to reject non-essential cookies usage can be categorized as GDPR and ePrivacy Directive violation |

Figure 8. SWOT Analysis on the University of Tartu Website.

## 5.3 Eesti Kunstiakadeemia

Eesti Kunstiakadeemia (EKA) is an Estonian public university based in Tallinn that focuses on art and design. The website's homepage is artun.ee. The technology lookup using Wappalyzer shows that the EKA website utilizes Google Analytics, TrackJS, Hotjar, and Facebook Pixel to create analytic measurements on their websites.


Figure 9. Cookie Banner Notification on EKA's website.

The cookie banner is shown as a pop-up box at the bottom of the website as a binary selection that explicitly shows an offer to accept or reject. The language of the banner is provided in both English and Estonian depending on the choice of language that the user chooses. It explains the usage of cookies is intended to deliver statistics and offer the best experience. The clause of offering the best experience is rather subjective and requires a more detailed explanation of how it can be achieved.

The notification also provides a link where users can read more about their cookie policy both in Estonian and English. One user experience approach that is done by the EKA website is the user can opt-out easily after giving consent regarding the use of cookies by providing a widget at the bottom of the screen to show the banner again and reject the use of cookies. When the author rejects the use of cookies, the author was redirected to the Terms of Use and Privacy Policy page which includes the explanation of cookies usage and advertising partners. The page recommends the user adjust browser settings to limit the cookies installed in the browser.


Figure 10. Minimized shortcut to EKA's privacy policy page.

In the first visit to the home page, EKA placed non-essential cookies such as Facebook Pixel and Google Analytics. Ideally, consent on cookie placement must be obtained

through active consent in which the user confirms by pressing the “Accept” button on the cookie consent banners.

| Strength | Weakness |
|---|---|
| • Cookie banner notification is minimized and provides a shortcut for users to reject the cookies and read more about their privacy policy.<br>• No nudging practices. The design of the consent banner is neutral and clear.<br>• Option to refuse cookie usages | • Non-essential cookies are placed before user’s active consent<br>• The website keeps sending data to Facebook Pixel and Google Analytics after the user rejects cookie usage. |
| **Opportunities** | **Threat** |
| • Providing direct opt-out option in the privacy policy<br>• Mentioning Hotjar in their privacy policy<br>• Introducing privacy-oriented web analytics tool for audience measurements<br>• Giving granular options for cookies choice | • Cookie placement before user’s active consents can be categorized as GDPR and ePrivacy Directive violation |

Figure 11. SWOT Analysis on EKA’s Website.

## 5.4 Tallinna Ülikool

Tallinna Ülikool (Tallinn University / TLU) is an Estonian university located in Tallinn. Their website homepage is tlu.ee.

Tallinn University’s website informs its user visitors about their use of cookies in a form of a footer banner at the bottom of the page. The cookie notification banner does not offer an option for users to reject cookie usage. It provides a link to their cookie policy. Both

the banner and the cookie policy are only in Estonian despite the website being served both in English and Estonian.


Figure 12. Cookie Banner Notification on Tallinn University's website.

Tallinn University's website uses Google Analytics and Facebook Pixel for the analytic and audience measurement. However, the cookie banner neither their cookie usage policy mentions Google nor Facebook.

When the author further explores pages on the website, the cookie banner disappeared even though the author did not press the button "Jah, nõustun" (Yes, I agree). This behaviour can be assumed that the user's action to keep browsing is considered as consent. This is an example of implied consent. Implied consent is not a legitimate way to obtain a user's consent as CJEU stated that consent must be obtained through active consent [49]. Just like most of the observed websites, non-essential cookies are placed into the user's browser before the user gives an active consent.

| Strength | Weakness |
|---|---|
| • Easy to find privacy policy | • No option to reject the use of cookies<br>• Non-essential cookies are placed before user's active consent<br>• The website keeps sending data to Facebook Pixel and Google Analytics after the user rejects cookie usage.<br>• Using implied consents assuming the user accepts cookies if they keep continue browsing |
| **Opportunities** | **Threat** |
| • Introducing privacy-oriented web analytics tool for audience measurements<br>• Providing option to refuse non-essential cookie and opt-out options | • Implied consent should not be constituted as a valid consent and can be considered as a violation<br>• Cookie placement before user's active consents can be categorized as GDPR and ePrivacy Directive violation |

Figure 13. SWOT Analysis on Tallinn University's Website.

## 5.5 Sisekaitseakadeemia

Sisekaitseakadeemia or Estonian Academy of Security Science is a public vocational university that is based in Tallinn. Their website homepage is sisekaitse.ee. From the Wappalyzer technology lookup through, the Estonian University of Security Science uses Matomo Analytics as the only web analytics and audience measurement tool.

The Estonian University of Security Science provides information regarding personal data protection when visiting their website. The policy outlines the usage of cookies for the purpose of distinguishing users [50]. Google Analytics cookies are mentioned as the

only analytic cookies used in their website even though when the author examined their website, Google Analytics cookies are no longer placed into the browser. It seems that they priorly used Google Analytics and have migrated to Matomo but have not updated this detail in their privacy policy. Currently, the website offers no options for users opting out Matomo cookies from their browser except by adjusting the browser setting. The website includes a Facebook widget to interact with the university. Here, the author found the agreement on giving consent for placing a session cookie in the user's browser when using this feature as a guest. The cookie was not placed until the author gave active consent.

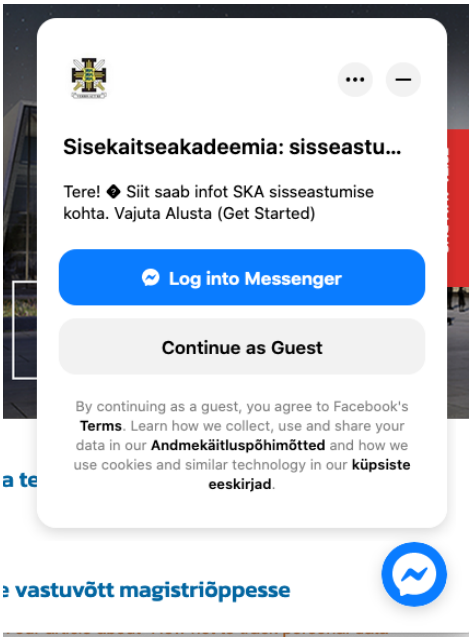



Figure 14. Request for user's consent to place cookie for Facebook's widget.

Based on Matomo's guidance to avoid cookie consent banners, Matomo suggests web publishers follow some steps such as enabling cookie-less tracking, providing an opt-out option and mentioning Matomo in their privacy policy [51]. If the Estonian Academy of Security Science wants to avoid cookie banners, they should apply these adjustments.

| Strength | Weakness |
| --- | --- |
| • Using only privacy-oriented web analytic tools (Matomo).<br>• No cookie banner creates less annoyance to the user yet their approach to not use cookie-banner notification can be justified by only using Matomo.<br>• Detailed information regarding the use cookies in the websites on user's visit. | • The privacy policy has not been updated with the most recent changes.<br>• There is no direct opt-out option from Matomo tracking cookies. |
| **Opportunities** | **Threat** |
| • The privacy respecting approach on user analytics increase the reputation and trust on the website and therefore the institution<br>• Providing opt-out option for Matomo tracking cookies<br>• Using Matomo cookie-less mode will justify not using cookie consent banner for analytics purposes. | • Placing Matomo cookies without active consents and opt-out options still falls into the gray area in terms of GDPR and ePrivacy Directive. |

Figure 15. SWOT Analysis on Estonian Academy of Security Science's Website.

# 6 Results of Observation

This chapter covers the summarized analysis of elements that we considered in the methodology chapter from all observed websites.

## 6.1 Placing Cookies Before User's Active Consent

Based on the observation, the most common violation of the GDPR and ePrivacy Directive in Estonian higher education institutions' websites is cookie placement before users give active consent. This action occurs on all 15 observed websites although, for the Estonian Academy of Security Science, the deployed cookies were Matomo cookies.

## 6.2 Respecting User's Choice

On the websites that provide options to refuse the use of cookies, the author found that the user's choice to either refuse cookies entirely or partially was not respected. The example that the author wants to highlight is from TalTech's website. The author noticed that the tags on the website keep sending data for Google Analytics and Facebook Pixel even though the author refused to use all cookies and opt-out from analytics. This problem could be easier to manage if the non-essential cookies are not obtained before the user gives active consent. The same thing happens to websites that offer the option to reject the use of cookies integrated into its cookie banner notification.

## 6.3 Cookie Banner Notification

During the observation, 7 out of 15 observed websites uses cookie banner notifications to obtain user consent to place non-essential cookies on their page. Basing on the classification from Degeling M, Utz C, Lentzsch C, Hosseini H, Schaub F, Holz T., report about GDPR measurement on the web privacy, the author encountered several types of cookie banner based on the way it interacts with the user [34]:

a. Confirmation only

The cookie banner does not provide direct information to reject the use of cookies. It can be also assumed as an implied consent as the users are assumed to give consents and the only way to get rid of the cookie banner is by pressing “OK” or “Agree”. The example can be found on the websites from The University of Tartu (Figure 7) Tallinn University (Figure 12), and Estonian Academy of Music and Theatre.

b. Granular Consent

Granular consent gives the user the possibility to only accept several cookies which live up to GDPR expectation. The only website that offers this option is TalTech website (Figure 3 and Figure 5).

c. Binary choice

A Binary choice is a way to obtain legitimate consent by accepting all or refusing all cookies. This type of banners can be found from the websites of EKA (Figure 9. and Figure 10), Estonian Business School, and Sisekaitseakadeemia’s Facebook widget (Figure 14).

## 6.4 Usage of Privacy-Friendly Analytic Tools

The author found that all observed websites use various Web Analytic tools for various purposes such as audience measurement and user behaviour analytics. Google Analytics is used in 14 out of 15 observed websites. There is only one website that belongs to Sisekaitseakadeemia that currently only uses Matomo as their web analytics tool. TalTech website is the only other website that also implements Matomo but tandemly still uses Google Analytics.

Matomo (_pk*) cookies on Sisekaitseakadeemia’s website are considered less disturbing and raise less concern to users. There is still a note about this implementation. The cookies are placed in the browser before the user gives consent to place this cookie. Even though it is less intrusive, it will comply more with the ePrivacy directive if the user is given a choice to reject this cookie. A good example is demonstrated on the EDPB website. The website uses Matomo for analytics purposes. Users are given the option to reject the use of cookies when visiting the website (Figure 16.) and only when the user gives consent, the _pk* cookies are placed on their browser (Figure 17.). The website also offers an

option to opt-out from their tracking on their cookie policy page. Users are given full control to retract their consent by clicking the “Refuse” button and _pk* cookies are deleted from their browser (Figure 18.).

## 6.5 Privacy Policy Availability and Content

Privacy policy can be found in 14 out of 15 observed websites. From 14 websites that provide a privacy policy, 11 of them explain their cookie policy specifically when a user visits the website. Three websites provide an option to reject the use of cookies on their website without the need to adjust the user's browser. Most of the websites did not specify options to reject cookie usage in their website. Instead, some of them clearly “obtain consent” through implied consent.

The author took an example from Tallinna Tervishoiu Kõrgkool (Tallinn Health Care College / TTK). Their privacy policy on cookie usage says: “Kasutajad loetakse küpsistega nõustunuks, kui veebilehitseja seadistustes on lubatud küpsised.” or in English “Users are considered to have accepted cookies if cookies are enabled in their browser settings.” [52]. It’s another example of implied consent which is not considered as valid consent according to CJEU [49].

| No. | Name of Institution | Providing Privacy Policy | Informing about cookie usage | Information about third-party vendors |
|---|---|---|---|---|
| 1 | Tallinna Tehnikaülikool | Yes | Yes | Yes |
| 2 | Tartu Ülikool | Yes | Yes | Yes |
| 3 | Tallinna Ülikool | Yes | Yes | Yes |
| 4 | Eesti Maaülikool | Yes | No | No |
| 5 | Eesti Muusika- ja Teatriakadeemia | Yes | Yes | Yes |
| 6 | Eesti Kunstiakadeemia | Yes | Yes | Yes |
| 7 | Kaitseväe Akadeemia | Yes | No | No |
| 8 | Eesti Sisekaitseakadeemia | Yes | Yes | Yes |
| 9 | Tallinna Tehnikakõrgkool | Yes | Yes | Yes |
| 10 | Tallinna Tervishoiu Kõrgkool | Yes | Yes | Yes |
| 11 | Tartu Tervishoiu Kõrgkool | Yes | Yes | Yes |
| 12 | Eesti Lennuakadeemia | Yes | Yes | Yes |
| 13 | Kõrgem Kunstikool Pallas | Yes | No | No |
| 14 | Estonian Business School | Yes | Yes | Yes |
| 15 | Estonian University of Applied Science | No | No | No |

Table 2. Observation on privacy policy availability and content.

# 7 Improving Privacy on Web Analytics Process

The choice of web analytics depends on many factors. These factors can be from the objective of measurement, the conversion rate of sales, or many more specific objectives. Various tools often have capabilities or advantages that are not owned by others. Other factors could be the familiarity of the tools with the public or internally in the company. The author realized that complete transitions from Google Analytics to privacy-oriented web analytics do not apply to every organization instantly. Based on that consideration, the author divides this section into improving privacy in Google Analytics and other privacy-oriented web analytics tools.

## 7.1 Google Analytics

Many organizations have invested sources and knowledge to build their Google Analytics to produce comprehensive and measurable results according to the organization's goal and key performance indicator (KPI).

Google as the owner of Google Analytics realized the need to adapt to the GDPR by providing ways to increase users' privacy. However, since these measures could affect Google's core business as an advertising company, these measures are not implemented by default when web publishers start to implement Google Analytics on their websites. It becomes the responsibility of the web publisher as a data controller. Joe Christopher outlines actionable steps to be taken to make the use of Google Analytics compliant with GDPR [53]:

a. Prevent Capturing Personally Identifiable Information

This best practice is not only in particular for Google Analytics, but also as the best practice when designing an application. Web publishers can potentially leak user's personal data into Google Analytics. Requests such as GET parameters can potentially leak personal information when personal data information such as

“zipcode=xxxxx” or “email=xxxx is used in the URL. These data will be captured and accidentally sent to the analytic tools. Aside from keeping this data from being sent to analytic tools, these data will be stored in the server log and browser history. Thus, it is important to audit request parameters to prevent leaking user’s personal data. Always use POST parameters to prevent leaking PII. We also need to note to not use UUID or any parameters that can indicate the data subject’s identity which can be captured by Google Analytics.

b. IP Anonymization

Turning on IP Address anonymization or IP masking is one option that is offered by Google Analytics. In this process, the IP address will be masked after the data is sent to Google Analytics. The user's IPV4 address's last octet, and in the case of IPV6, the last 80 bits, will be set to zero [54]. This feature can be set on Google Tag Manager. On the test website that the author deployed with gtag.js library. To turn on this function, web publishers need to update the config property by setting the value of the `anonymize_ip` parameter to true.

```
<script>
    window.dataLayer = window.dataLayer || [];
    function gtag() {
        dataLayer.push(arguments);
    }
    gtag('js', new Date());
    gtag('config', [redacted]);
    gtag('config', [redacted], {
        'anonymize_ip': true
    })
</script>
```

Figure 19. IP Anonymization in Google Analytics.

c. Providing Opt-Out options

The GDPR and ePrivacy Directive requires users to be able to retract their consent. Providing an option to opt-out is commonly found on the privacy policy page. The easiest way to opt out from Google Analytics tracking is by clicking a button that will trigger a function that sets this property.

When using the Universal Analytics library (gtag.js), Google has provided a possibility for web publishers to provide this feature. To prevent the site from sending data to Google Analytics, this window property needs to be set to true [55].

```
window['ga-disable-UA-XXXXX-Y'] = true;
```

Replace the `UA-XXXXX-Y` with the site's Analytics measurement ID

Setting this property to true will prevent Google Analytics from placing cookies or sending data to the Google Analytics server since it will examine this property before actions are taken.

d. Updating Privacy Policy

Based on the observations, it is still common that the website does not mention the usage of Google Analytics on their cookie notification banner or privacy policy page. As indicated by Google Analytics terms and conditions of usage [38], it is noted that Google Analytics needs to be mentioned in the company's privacy policy. Failing to mention external parties which act as a data processor could result in a violation of GDPR and other data privacy regulations.

e. Placing cookies only after the user gives an active consent

This is often where violation happens since publishers do not want to risk opt-out by the majority of their users. It is advised to let the user have granular level consent on analytics and advertising cookies.

## 7.2 Open-Source Privacy-Oriented Web Analytics

There are several reasons from the web publisher side on why they use open-source privacy-oriented web analytics. One of the benefits is to prevent privacy violation and as it is ethically more correct to prevent passing user's / visitor's personal data to other third party which may use it for their own benefits. Additionally, a disclaimer about the usage of cookies could affect user's perception as a nuisance of the visiting website experience or as a threat to their privacy which could affect the organizations or company's reputation [56].

On top of the transparency as open-source software, the appeal from the user's privacy data protection of these tools is the ability to self-host. Self-hosting your own analytics can limit data transfer to other third parties which live up to the idea of full control of your data and being fully compliant with various regulations in many countries or territories such as the GDPR, ePrivacy Directive, California Consumer Privacy Act (CCPA) or UK's Privacy and Electronic Communications Regulations (PECR) [57]. Self-hosting also gives you control to choose where the server is hosted and thus we can keep these data to stay in the EU.

The trade-offs of using these tools are often the contrast "advantage" of using Google Analytics. These trade-offs are:

- More efforts on the installation process for self-hosting vs Google Analytics instant set-up
- Cost from self-hosting or to unlock some key features vs Various available features for free by using Google Analytics.
- Adjusting the data processing procedure vs Integration to Google's services such as Data Studio with Google Analytics

Between the choices of open-source web analytics itself, there are various types of models with different approaches to ensure privacy-friendly data collection. There are two models which are with cookie and cookie-less analytics.

Cookie less analytics is used by Simple Analytics, Plausible Analytics, and Fathom. Each vendor uses different methods of implementing it into their analytic tool. Plausible Analytics and Fathom use their own methods to generate user's identifier to remember returning visitors and new visitors daily and run it through a hash function with a daily rotating salt.

Plausible Analytics:

```
hash(daily_salt + website_domain + ip_address +
user_agent)
```
[58]

Fathom:

```
hash(daily_salt + ip_address + website_id + user_agent +
day_of_the_year)
```
[59]

Using cookie-less analytic tools means that there is no need to put cookie banner notifications and therefore create less annoyance for the user. The downside of these analytic tools is the inability to differentiate returning customers from different days since the hash will be different due to rotating daily salt.

Matomo by default uses cookies although it has a cookie-less option. Cookie-less implementation will result in a less accurate measurement compared to the measurement with cookies.

# 8 Discussion

In this chapter, the author discusses some of the issues on internet privacy and GDPR and ePrivacy directive implication related issues. In addition, the author brings up a discussion on some undermined topics like accessibility and its correlation with web privacy and how to achieve equal participation in web privacy and the future of user tracking mechanisms.

## 8.1 The Role of GDPR and ePrivacy Directive on Internet Privacy

The need to maximize the potential of the internet for the development of organizations creates the demand for tools and features that can support their business and needs. Users, publishers, and many stakeholders on the internet often take only the benefits of using platforms and take it for granted. All the services and platforms that are commonly used by people are created by multiple tech giants with different intentions and commitments to individual privacy.

Many of us have probably heard the phrase “Data is the new oil”. This phrase indicates the potential that data can create to earn as much information about the users which can be used to categorize and profile individuals. Advertising companies such as Google and Facebook have reached this step for their business interests, delivering advertisement which suits the user’s interest. These data may be sold to other unknown parties without the acknowledgment of the users. Such valuable information could be used by anyone to do more disturbing actions. Profiling an individual into very secretive personal information such as gender, religious affiliation, sexual orientation, ethnicity, etc. could potentially harm more vulnerable social groups.

GDPR and other regulations related to personal data open a new era of transparency and privacy for users worldwide. The aim of these legislations is not to earn as many fines as possible or create more hassle for business. The main objective of it is to provide legal accountability on handling their customer’s personal information. Some ambiguity sparks

from it and thus until ePrivacy regulation takes effect and highlights the required GDPR implementation in terms of cookies and other electronic communication media, it is better to take the most precautious option to respect users' privacy.

The effort to comply with the expectations of the ePrivacy Directive should be considered by organizations in Estonia. Complying with those requirements will bring more ease of complying with the ePrivacy Regulation when it becomes effective. Some observed institutions have made more efforts than others on creating a more privacy-friendly user experience and web analytics for users.

## 8.2 Promoting Active Consent and Web Accessibility

Web Accessibility is an initiative to create the internet to be more inclusive for everyone. With the transformation of many services from offline to online, the need for information to be able to pass as well as giving equal access to everyone is regarded as a necessity.

There is still a lack of research on the relationship between accessibility and user privacy. Nevertheless, giving an equal user experience to users with a screen reader, screen magnifiers, and other assistive technology on their privacy when visiting a website should be delivered in a simple and not obstructive way. This initiative can promote active consents for users who use assistive technology.

Bogdan Cerovac in his article wrote about cookie consent banners and accessibility aspects. According to Cerovac, the best approach to place cookie banners is as a modal window on the top of the page [60]. Léonie Watson from the London Web Performance group demonstrated the accessibility of cookie consent notices for screen reader users [61]. A good example that she brought up is Atlassian's website. The screen reader can recognize the cookie consent banner as the first heading on the page as well as providing clear and understandable statements on the banner [61].

From the Estonian higher education institutions' websites, it seems necessary for most of them to improve their accessibility of the websites in general. TalTech website can be used as an example of implementing WCAG 2.0., the standard for accessibility purposes especially on the less touched part on promoting active consent for every user.

## 8.3 The Future of User Tracking Mechanisms

GDPR is created as a general provision regulation in any personal data, not only in the electronic communication media. GDPR does not specifically highlight cookies as it is meant to cover every known technology that has the possibility of obstructing user privacy. The known methods are storing and counting IP addresses with the combination of User-Agent, Browser fingerprinting, or using browser cache (ETag Tracking) [58].

Google has announced its plan to restrict the use of third-party cookies in Google Chrome Browser which is surprising news for an ad-based revenue company [62]. Google will not plan to switch entirely their business sector and instead plan to create a more privacy-respecting environment called Federated Learning of Cohorts (FLoC). With this approach, Google will still be able to track user's activities when using Google Chrome, but the advertiser will target their ad based on the cohorts instead of personalizing individual users. Even though it seems promising, there are scepticisms around this plan, and is seen as Google's effort to walk around regulations such as GDPR. FLoC, according to the Electronic Frontier Foundation, could make fingerprinting users easier while also making it more difficult to detect and evade browser fingerprinting [63].

# 9 Recommendations

Based on the analysis and observations, the author proposed these recommendations for Estonian higher education institutions to follow to help to comply with GDPR and ePrivacy Directive.

The recommendations are divided into two steps: Minimal and Optimal. Minimal recommendations need to be considered immediately by the institutions to comply with GDPR, Estonian Personal Data Protection Act, and Estonian Electronic Communication Act. The optimal recommendations should be considered after the minimal recommendations have been implemented as it has stricter standards that are expected in the upcoming ePrivacy Regulation.

**Minimal Recommendations**

- Organizations need to review their privacy and cookie policy especially when implied consent is still in use.
- The organizations that have not provided options to refuse cookie usage need to make it available as it is necessary according to the Estonian Personal Data Protection Act.
- Preventing placing non-strictly necessary cookies including analytics or performance cookies.
- The organization's digital marketing team should consider using self-hosted analytics and build a plan to integrate it into their analytics stack and marketing plan.
- For the organization that uses granular consents, the input box/toggle button for cookies preferences needs to be deactivated by default
- Providing an opt-out mechanism to withdraw consents

- The privacy and cookie policy should be updated if necessary, for example when integrating new services from new third-party vendors.

**Optimal Recommendations**

- Using Consent Management Platform (CMP) to help to verify all types of cookies that the website installs and provide detailed information such as cookie types, purposes, and durations.
- The organizations move their web analytics stack to a self-hosted web analytics platform to limit passing personal data to other third-party organizations.
- Cookie banner, privacy policy, and cookie policy need to be available in all languages that the website serves
- Using dropdown cookie banner design to make privacy and cookie policy easily noticeable even after consent is given.
- Develop a website with accessibility in mind including cookie banners notification in that aspect
- Establishing equal standards for every Estonian higher education institution on GDPR and ePrivacy Directive compliances.

# 10 Further Research

This thesis was written between March to May 2021 to capture the state of compliance of Estonian higher education institution's websites. As the web is always evolving, the result of this observation will be different over time. More web publishers and organizations try to implement their best effort and find the balance between digital marketing, analytics, and compliance towards GDPR and ePrivacy Directive. Further research should be done in a year and before the ePrivacy Regulation will take place to be able to compare the efforts that these organizations have made to create a privacy respecting user experience for their users.

To give insight towards migration from Google Analytics to Privacy Oriented Web Analytic tools, further research can focus to compare the implementation of both Google Analytics and several other privacy-oriented web analytics tools in a long-term implementation. The research should focus on the difference between the number of users captured by different tools and measure its accuracy compared to Google Analytics since Google Analytics currently is the most used and trusted source of analytic data for various purposes.

# 11 Summary

The observation into Estonian higher education institution's websites results in the finding that the majority of them made some basic violations of GDPR and ePrivacy Directive. These violations are not only affecting the legal aspect but also ethically violate users' right to privacy on the internet. A common violation among the observed websites is placing non-essential cookies into the user browser before the user gives active consent. Secondly, most websites do not give a direct option to refuse the use of cookies and using implied consent instead.

The author found that some institutions have moved forward in terms of protecting their user's privacy such as implementing a privacy-oriented web analytics tool either tandemly with Google Analytics or completely migrated to the new analytics platform. Some institutions have provided cookie banner notifications as a medium to communicate with their users to obtain their consent. Based on the observation, Sisekaitseakadeemia implements the best approach to protect their users' privacy when visiting their website. Other good examples to take are from TalTech's website which provides granular control of consent and accessibility-in-mind cookie banner design and EKA's website with its easy-to-find and no-nudging cookie banner design.

Even though the data protection regulation in Estonia is not as specifically demanding as some other EU/EEA for example in Belgium, it is recommended to follow the approved practices and guidance by EU and Estonian data protection authorities so the organization can easily adjust to stricter regulation such as the incoming ePrivacy Regulation.

The author advises Estonian higher education institutions through their data protection officer, website developer, and digital marketing department to pay attention to these violations and take a step to address these issues by reviewing their privacy policy and practice and considering the proposed recommendations to make sure their website is compliant with GDPR and ePrivacy Directive.

# References

[1] IAPP-EY Annual Governance Report 2019 [Internet]. International Association of Privacy Professionals. 2019. Available from: https://iapp.org/store/books/a191P000003Qv5xQAC/ [cited March 22, 2021]

[2] Llamas LV. The Spanish DPA fines VUELING with 30.000 EURO [Internet]. Blog der datenschutz nord Gruppe. Datenschutz Notizen; 2019. Available from: https://www.datenschutz-notizen.de/the-spanish-dpa-fines-vueling-with-30-000-euro-2123832/. [cited March 4, 2021]

[3] European Data Protection Supervisor. The History of the General Data Protection Regulation [Internet]. European Union; Available from: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. [cited March 4, 2021]

[4] Europa.eu. Regulations, Directives and other acts [Internet]. European Union; Available from: https://europa.eu/european-union/law/legal-acts_en. [cited March 18, 2021]

[5] Voigt P, Bussche Avon dem. The EU General Data Protection Regulation (GDPR) A Practical Guide [Internet]. 2017. Available from: https://lib.ugent.be/catalog/ebk01:3710000001632696. [cited March 6, 2021]

[6] Gdpr-info.eu. Art. 4 GDPR – Definitions [Internet]. Intersoft Consulting; 2016. Available from: https://gdpr-info.eu/art-4-gdpr/. [cited March 5, 2021]

[7] Gdpr-info.eu. Art. 83 GDPR – General conditions for imposing administrative fines [Internet]. Intersoft Consulting; 2016. Available from: https://gdpr-info.eu/art-83-gdpr/. [cited March 5, 2021]

[8] EUR-Lex. Document 02009L0136-20201221 [Internet]. European Union; 2009. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02009L0136-20201221 . [cited March 6, 2021]

[9] Personal Data Protection Act 2018 [Internet]. Riigi Teataja. Available from: https://www.riigiteataja.ee/en/eli/523012019001/consolide . [cited May 5, 2021]

[10] Electronic Communications Act 2004 [Internet]. Riigi Teataja. Available from: https://www.riigiteataja.ee/en/eli/ee/521052020003/consolide/current . [cited May 5, 2021]

[11] DLA Piper Blogs. European Law on Cookies Guide [Internet]. DLA Piper; 2020. Available from: https://blogs.dlapiper.com/privacymatters/european-law-on-cookies-guide/ . [cited May 6, 2021]

[12] Tsuiman A. Data Protection in Estonia: Overview [Internet]. COBALT Law Firm. 2020. Available from: https://www.cobalt.legal/files/data_protection_in_estonia_overview_12_08_2020.pdf . [cited March 18, 2021]

[13] Thomson Reuters Practical Law. EU Member State Cookie Directive Implementation Chart [Internet]. Thomson Reuters. 2020. Available from: https://uk.practicallaw.thomsonreuters.com/w-004-3742?originationContext=document&amp%3Bvr=3.0&amp%3Brs=PLUK1.0&amp%3BtransitionType=DocumentItem&amp%3BcontextData=%28sc.Default%29&amp%3BfirstPage=true&transitionType=Default&contextData=%28sc.Default%29

[14] Jelinek A. Statement 03/2021 on the ePrivacy Regulation [Internet] European Data Protection Board. 2021. Available from: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-032021-eprivacy-regulation_en . [cited March 14, 2021]

[15] Mildebrath H. Proposal for a regulation on privacy and electronic communications [Internet]. European Parliament. 2021. Available from: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-jd-e-privacy-reform . [cited May 10, 2021]

[16] Marini A, Kateifides A, Zanfir-Fortuna G, Bae M, Gray S, Sen G. CCPA, face to face with the GDPR: An in depth comparative analysis [Internet]. Future of Privacy Forum; 2020. Available from: https://fpf.org/blog/fpf-and-dataguidance-comparison-guide-gdpr-vs-ccpa/ . [cited May 8, 2021]

[17] Office of the Attorney General. California Consumer Privacy Act 2018 (CCPA) [Internet]. State of California - Department of Justice. Available from: https://oag.ca.gov/privacy/ccpa . [cited May 8, 2021]

[18] Law Section. California Civil Code, Section 1798.140 (November 3, 2020). [Internet]. California Legislative Information. 2020. Available from:

https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.140.&nodeTreePath=8.4.45&lawCode=CIV . [cited May 8, 2021]

[19] Zetoony D, Auty C, Ross K. Frequently Asked Questions Concerning Cookies and AdTech [Internet]. BCLP California Consumer Protection Act Information. 2020. Available from: https://ccpa-info.com/frequently-asked-questions-concerning-cookies-and-adtech/ . [cited May 8, 2021]

[20] Law Section. California Civil Code, Section 1798.155 (November 3, 2020). [Internet]. California Legislative Information. 2020. Available from: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.140.&nodeTreePath=8.4.45&lawCode=CIV . [cited May 8, 2021]

[21] Nõmper A, Liis M. Data Protected Estonia: Insights [Internet]. Linklaters. 2020. Available from: https://www.linklaters.com/en/insights/data-protected/data-protected---estonia . [cited March 20, 2021]

[22] Iubenda.com. Cookie Policy for Belgium [Internet]. Iubenda. Available from: https://www.iubenda.com/blog/cookie-policy-for-belgium/ . [cited April 20, 2021]

[23] Cookies et autres traceurs [Internet]. Autorité de protection des données. Available from: https://www.autoriteprotectiondonnees.be/citoyen/themes/internet/cookies . [cited May 6, 2021]

[24] Van Quathem K. Belgian Supervisory Authority Imposes Cookie Fine [Internet]. Inside Privacy. 2019. Available from: https://www.insideprivacy.com/data-privacy/belgian-supervisory-authority-imposes-website-cookie-fine/ . [cited April 6, 2021]

[25] MDN Web Docs. Using HTTP cookies [Internet]. Mozilla. Available from: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies . [cited Mar 5, 2021]

[26] GDPR.eu. Cookies, the GDPR, and the ePrivacy Directive [Internet]. Proton Technologies AG. 2019. Available from: https://gdpr.eu/cookies/ . [cited April 3, 2021]

[27] Irwin L. How the GDPR affects cookie policies [Internet]. IT Governance Blog. 2020. Available from: https://www.itgovernance.eu/blog/en/how-the-gdpr-affects-cookie-policies . [cited March 21, 2021]

[28] GDPR.eu. Recital 30 Online identifiers for profiling and identification (EU GDPR). [Internet]. Proton Technologies AG. 2016. Available from: https://gdpr.eu/recital-30-online-identifiers-for-profiling-and-identification/ . [cited April 3, 2021]

[29] European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679 2020. [Internet]. Available from: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en . [cited April 7, 2021]

[30] Cookielaw.org. GDPR Compliance Means Cookie Notices Must Change [Internet]. Cookie Law by CookiePro. 2016. Available from: https://www.cookielaw.org/blog/gdpr-compliance-means-cookie-notices-must-change/ . [cited March 12, 2021]

[31] GDPR.eu. Recital 32 Conditions for consent (EU GDPR). [Internet]. Proton Technologies AG. 2016. Available from: https://gdpr.eu/recital-32-conditions-for-consent/ . [cited April 3, 2021]

[32] Hotjar.com. Top 20 Web Analytics Tools Used by Experts in 2021 [Free + Premium] [Internet]. Hotjar. 2021. Available from: https://www.hotjar.com/web-analytics/tools/ . [cited March 20, 2021]

[33] Optimizely.com. Web Analytics [Internet]. Optimizely. Available from: https://www.optimizely.com/optimization-glossary/web-analytics/ . [cited April 11, 2021]

[34] OnAudience.com. What is Audience Data and how does it work? [Internet]. Blog OnAudience.com. 2020. Available from: https://www.onaudience.com/resources/what-is-audience-data-and-how-does-it-work/ . [cited April 8, 2021]

[35] Shaya O. Web Analytics [Internet]. 2015. Available from: https://www.researchgate.net/publication/281448685_Web_Analytics . [cited March 28, 2021]

[36] Kenny R, Pye G, Pierce J. Ethical Considerations and Guidelines in Web Analytical and Digital Marketing: A Retail Case Study [Internet]. 2012. Available from: http://hdl.handle.net/10536/DRO/DU:30043939 . [cited March 29, 2021]

[37] Schwartz PM. Privacy, Ethics, and Analytics. IEEE Secur Priv. 2011;9(3):66–9.

[38] Google Analytics Terms of Service [Internet]. Google Marketing Platform. Google; 2019. Available from: https://marketingplatform.google.com/about/analytics/terms/us/ . [cited April 10, 2021]

[39] Hotjar.com. Hotjar's Commitment to the GDPR [Internet]. Hotjar. Available from: https://www.hotjar.com/legal/compliance/gdpr-commitment/ . [cited April 1, 2021]

[40] Quintel D, Wilson R. Analytics and Privacy. ITAL [Internet]. 2020 Sep.21; 39(3). Available from: https://ejournals.bc.edu/index.php/ital/article/view/12219 . [cited March 20, 2021]

[41] Google Privacy & Terms. How Google retains data we collect [Internet]. Google; Available from: https://policies.google.com/technologies/retention?hl=en-US . [cited March 20, 2021]

[42] The rise of privacy focused analytics [Internet], Khrome. Available from: www.khrome.dev/the-rise-of-privacy-focused-analytics . [cited March 20, 2021]

[43] Sponselee A, Gooch P, Vreeman N, Luysterborg E, Haenebalcke E, Kostadinova Z, et al. Cookie Benchmark study [Internet]. Deloitte; 2020. Available from: www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-cookie-benchmark-study.pdf [cited March 30, 2021]

[44] Young SWH, Montana State University, Clark JA, Mannheimer S, Hinchliffe LJ, Montana State University, et al. A roadmap for achieving privacy in the age of analytics: A white paper from A national forum on web privacy and web analytics. Montana State University; 2019.

[45] Young SWH, Montana State University, Clark JA, Mannheimer S, Hinchliffe LJ, Montana State University, et al. A national forum on web privacy and web analytics: Action handbook. Montana State University; 2019.

[46] Degeling M, Utz C, Lentzsch C, Hosseini H, Schaub F, Holz T. We value your privacy ... Now take some cookies: Measuring the GDPR's impact on web privacy. In: Proceedings 2019 Network and Distributed System Security Symposium. Reston, VA: Internet Society; 2019.

[47] Riigi Infosüsteemi Amet. Kõrgkoolid - eesti.ee [Internet]. Eesti.ee. Available from: https://www.eesti.ee/est/kontaktid/korgkoolid_1 . [cited March 30, 2021]

[48] Accessibility [Internet]. TalTech. Available from: https://www.taltech.ee/en/accessibility . [cited April 7, 2021]

[49] Fazlioglu M. [Internet]. CJEU clarifies cookie consent requirements. International Association of Privacy Professionals; 2020. Available from: https://iapp.org/news/a/cjeu-clarifies-cookie-consent-requirements/ . [cited April 6, 2021]

[50] Isikuandmete töötlemine [Internet]. SISEKAITSEAKADEEMIA. Available from: https://www.sisekaitse.ee/et/isikuandmed . [cited April 13, 2021]

[51] Matomo Frequently Asked Questions. How do I use Matomo Analytics without consent or cookie banner? [Internet]. Matomo. 2020. Available from: https://matomo.org/faq/new-to-piwik/how-do-i-use-matomo-analytics-without-consent-or-cookie-banner/ . [cited April 13, 2021]

[52] Privaatsuspoliitika [Internet]. Tallinna Tervishoiu Kõrgkool. Available from: https://ttk.ee/et/privaatsuspoliitika . [cited April 18, 2021]

[53] Christopher J. 5 actionable steps to GDPR compliance with Google Analytics [Internet]. 2018. Available from: https://www.blastanalytics.com/blog/5-actionable-steps-gdpr-compliance-google-analytics . [cited April 18, 2021]

[54] IP anonymization with gtag.js Universal Analytics for Web (gtag.js) [Internet]. Google. Available from: https://developers.google.com/analytics/devguides/collection/gtagjs/ip-anonymization . [cited April 18, 2021]

[55] User Opt-out - Analytics for Web (analytics.js) [Internet]. Google Developers. Google; Available from: https://developers.google.com/analytics/devguides/collection/analyticsjs/user-opt-out . [cited April 18, 2021]

[56] Kulyk O, Hilt A, Gerber N, Volkamer M. “this website uses cookies”: Users’ perceptions and reactions to the cookie disclaimer. In: Proceedings 3rd European Workshop on Usable Security. Reston, VA: Internet Society; 2018.

[57] Matuszewska K. Self-hosted web analytics: 5 definite advantages - piwik PRO blog [Internet]. Piwik.pro. 2017 Available from: https://piwik.pro/blog/5-definite-advantages-can-gain-self-hosted-web-analytics/ . [cited April 10, 2021]

[58] Plausible: GDPR, CCPA and cookie law compliant site analytics [Internet]. Plausible Analytics. Available from: https://plausible.io/data-policy . [cited April 20, 2021]

[59] Ellis J. How we built a GDPR compliant website analytics platform without using cookies [Internet]. Fathom Analytics. 2019. Available from: https://usefathom.com/blog/anonymization . [cited April 20, 2021]

[60] Cerovac B. Cookie consent banners and overlays – thoughts on accessibility, usability and SEO [Internet]. Bogdan on Web Accessibility A11y. 2020. Available from: https://cerovac.com/a11y/2020/07/cookie-consent-banners-and-overlays-thoughts-on-accessibility-usability-and-seo/ . [cited April 24, 2021]

[61] Watson L. Screen readers and cookie consents. LWP May: Regulation and compliance. London Web Performance Group; 2020. Available from: https://www.youtube.com/watch?v=Uaqo4FOI_DY&t=686s . [cited April 24, 2021]

[62] Schuh J. Building a more private web: A path towards making third party cookies obsolete [Internet]. Chromium Blog. 2020. Available from: https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html . [cited April 26, 2021]

[63] Cyphers B. Google's FLoC Is a Terrible Idea [Internet]. Electronic Frontier Foundation. 2021. Available from: https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea . [cited April 26, 2021]

# Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I, Aditya Iqbal Bagaskara

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Privacy-Oriented Web Design and Analytics: A Case Study of Estonian Higher Education Institutions' Websites”, supervised by Kaido Kikkas
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

17.05.2021

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

# Appendix 2 – Additional screenshots

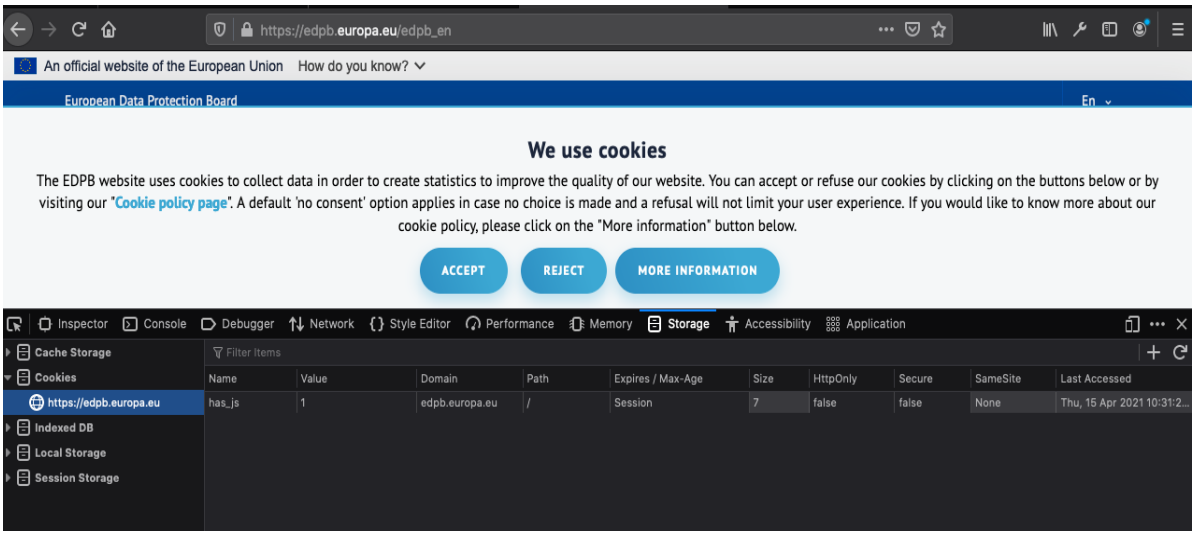



Figure 16. Initial cookie placement on EDPB website.

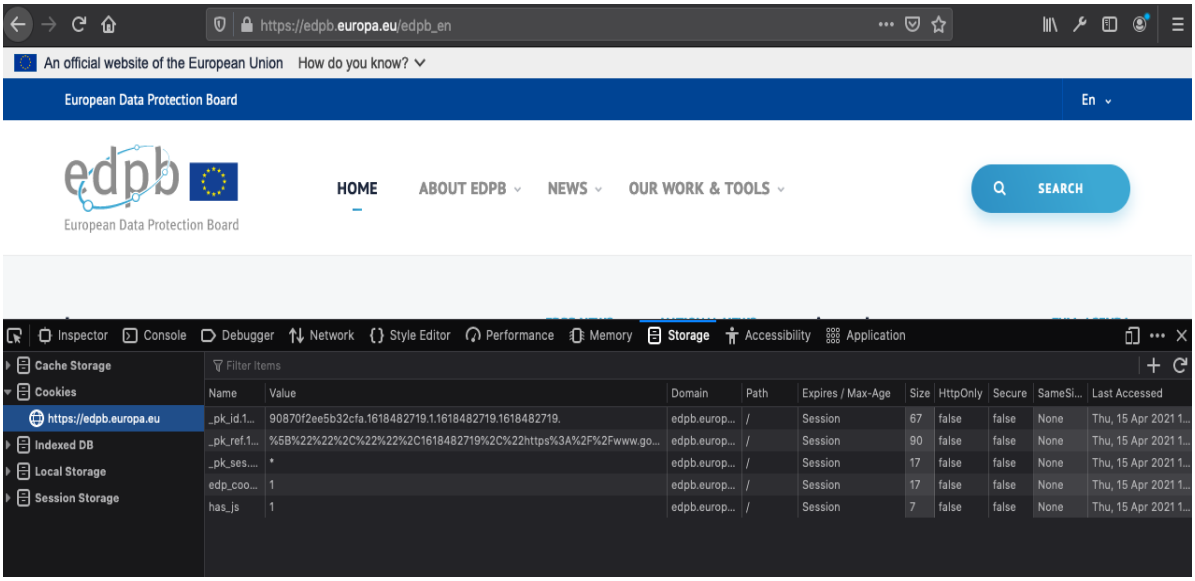



Figure 17. Matomo Analytic cookies on EDPB website.

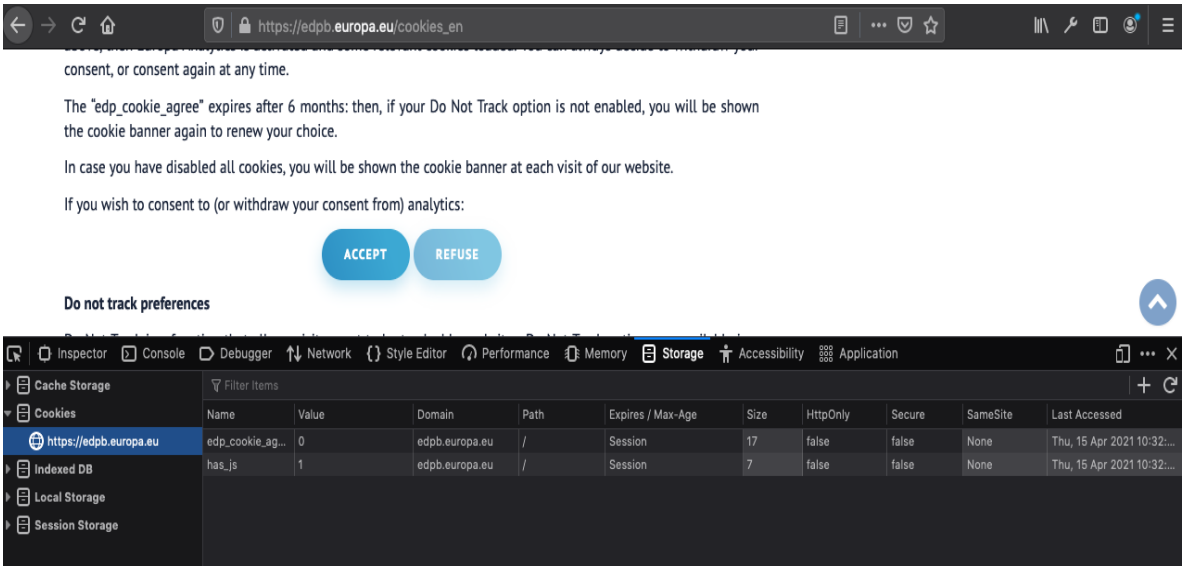



Figure 18. Revoked cookies storage on EDPB website.