AALBORG UNIVERSITY
DENMARK

Aalborg University Copenhagen
A.C. Meyers Vænge 15
2450 København SV

Title:
Privacy and Data Protection Compliance for Applications

Semester:
10th Semester

Project Period:
Spring Semester 2023

Semester Theme:
Master Thesis

Supervisors:
Lene Tolstrup Sørensen

Study secretary:
Charlotte Høeg

Members of the Group:

- Cherie Mai Caloyloy Hansen, No. 20184306
- Zohra Amini, No. 20193553

Page Number:
75 pages

Date of Completion:
1st of June 2023

Abstract:

This project is a cyber security master thesis that is examining and researching how to become compliant with data protection laws by providing recommendations, guidelines, best practices through an evaluation of the current state of the art. Firstly, our motivation for the project is given in order to set the scene for the thesis, which is to contribute by evaluating, assessing and analyzing GDPR, LGPD and the most well known frameworks, standards and models such as ISO:27001, Transfer Impact Assessments, Data Protection Impact Assessments, documentations on how to implement and incorporate regulations and risk management within an organization. Our background provides the theory on data protection laws and their interpretations and its practical enforcement. We are systematically conducting our research by a SOTA to get an overview, following an empirical research by observing and gathering data on-field. Next, we make risk assessments to identify and prevent those detected risks. Lastly, we are using the case study method by specifically conducting the DPIA, TIA and Privacy notice, as it is required for our case study Educado, a mobile educational platform built in Denmark, targeted Brazilian waste pickers. We are covering and discussing the main challenges, that an organization working with applications to stay compliant, are facing by having Educado as a focus.

Privacy and Data Protection Compliance for Applications

Cherie Mai Caloyloy Hansen and Zohra Amini

Aalborg University Copenhagen

Acknowledgements

First and foremost, we would like to extend our heartfelt thanks and gratitude to our supervisor Lene Tolstrup Sørensen, for her unwavering support, whose commitment to our master thesis have been truly inspiring. Her guidance and mentorship have been instrumental in shaping our understanding of cyber security principles, practices, and emerging trends. We also want to express our sincere appreciation to our Professor Jens Myrup Pedersen who has supported us in our academic journey to Brazil. Furthermore, we would like to thank our Brazilian collaborators and all the people involved with SDG Challenge, namely, Mateus Halbe Torres, Professor João Mello da Silva, Professor Paulo Celso dos Reis Gomes, Anonymous Employer from Recycling Complex, for their unique perspectives and collaborative spirit that have enriched our work. Lastly, we are grateful for the opportunity of working with the students from University of Brasília, Luiza Oliveira de Araujo (BSc, Engenharia de Produção) Yasmim Bezerra Oliveira Altoé (BSc, Engenharia de Produção) and Antônio Guimarães (BSc, Engenharia de Produção) who has enhanced the quality and depth of our research outcomes.

Contents

Abbreviations

AAU = Aalborg University

ALM = Avid Life Media

ANPD = Autoridade Nacional de Proteção de Dados

API = Application Programming Interface

AWS = Amazon Web Services

CCPA = California Consumer Privacy Act

CIA = Confidentiality, Integrity, Availability

CPF = Cadastro de Pessoa Físicas (Natural Persons Register)

CPRA = California Privacy Rights Act

DPA = Data Protection Authorities

DPIA = Data Protection Impact Assessment

EC2 = Elastic Compute Cloud

ECJ = European Court of Justice

EEA = European Economic Area

EU = European Union

GDPR = General Data Protection Regulation

HTTP(S) = Hypertext Transfer Protocol (Secure)

ICO = Information Commissioner's Office

ICT = Information and Communication Technology

JSON = JavaScript Object Notation

LGPD = Lei Geral de Proteção de Dados (General Data Protection Law)

NoSQL = Not Only SQL

PET = Privacy Enhancing Technologies

RDS = Relational Database Service

RIPD = Relatório de Impacto à Proteção de Dados Pessoais (The Personal Data Protection Impact Report)

S3 = Simple Storage Service

SCC = Standard Contractual Clauses

SDG = Sustainable Development Goals

SME = Small- and Medium-sized Enterprise

SOTA = State of the Art

SQL = Structured Query Language

TIA = Transfer Impact Assessment

UnB = University of Brasília

UN = United Nations

1 Introduction

Online Privacy becomes more and more important as the number of global internet users are increasing. As of January 2023, there were 5.16 billion internet users in the world. This is 64.4 percent of the global population and 59.4 percent were on the social media [1]. Furthermore, the number of Internet of Things (IoT) devices, that are connected to the internet are 15.14 billion and is forecasted to increase to 29.42 billion in the year of 2030 [2]. These numbers are indications of how much data there will be generated and collected in every field. With the progress and advancements in technology, the number of consumers rapidly grow.

Today, Industry 4.0 has revolutionised how manufacturing executes between Information Technology and Operational Technology and across different industries. Not only are connected devices increasing by digitization of manufacturing but also within internet-based platforms such as social media. These big tech giants collects enormous amount of data on a daily basis such as Google being the most visited website in 2022 with 88.4 billion of monthly visits, on average [3]. Data breaches has increased too by 15 million data records revealed in the third quarter of 2022. However, this is smaller compared to data exposure in 2020 by approximately 125 million data records getting leaked [4]. Abuse of the data in any form and shape has lead to cyber security issues, cyber crime, and increased the cyber threats. Many different vulnerabilities have been exploited by social engineering, third-party exposure, identity theft, tracking and trading of personal data [4]. Therefore, many privacy risks have arisen along with big data such as access control and consent with data sharing. Hence, privacy is getting a crucial role when managing, developing and processing data as it handles the principles such as accountability and transparency. Privacy are therefore enforced by laws and regulations in different countries and the implemented through for example user authentication and access control, anonymity and Privacy Enhancing Technologies (PETs) [5][6].

The *General Data Protection Regulation* (GDPR) is used in all European Economic Area (EEA) countries, and was enforced on May, 2018. The motivation behind the laws was to make sure that "*Everyone has the right to respect for his private and family life, his home and his correspondence*" [5][6]. When having an organization based in European Union(EU) that collects data from users, it is mandatory to abide by the data protection law, GDPR. This is essential when data transfer and storage are being made. In order to be compliant with GDPR, companies must conduct specific documentations that proves what, how, where and why they collect the data. These are documented by Data Protection Impact Assessments (DPIA), Transfer Impact Assessments (TIA) and privacy notices. The objectives of these documentations are to ensure that companies are not abusing the gathered data and only process it in such a way that user consent is obtained.

With better data protection ensured by the GDPR, a more sustainable approach of data handling is being made. The main focus of United Nations (UN) on sustainability within relevant fields, for instance technology, can be used to take action for people, planet and prosperity [7][8]. This is why UN highlight *The Sustainable Development Goals* (SDG) in which they state the goals "*provides a global blueprint for dignity, peace and prosperity for people and the planet, now and in the future*" [9][7].

The Global Students SDG Challenge is one of many initiatives made to raise awareness on global issues, where seven events have been confirmed since 2018 [10]. Here, University of Brasília (UnB) and Aalborg University (AAU) collaborate to improve the waste management and life quality of waste pickers in Brasília, Brazil. As the waste dump in Brasília with 2000 illegal waste pickers closed off, who had to find an alternative to make a living. Lúcia Fernandes was a waste picker for 20 years in order to provide for her four children. She moved to the recycling management centers, where employers' safety and working environment improved. When she describes working in the dump, she states that "*People lost their lives working here*" [11].

One of the projects introduced within the Global Students SDG Challenge is *Educado*, a focus on mobile education for waste pickers [10]. Educado is built with the purpose of helping the waste pickers such that they will be able to learn about finance and earn digital certificates by completing courses. Learning about finances can both benefit the waste pickers personally by letting them know how to responsibly spend their

income, but also professionally by teaching them other job opportunities with better working conditions than doing illegal waste picking [12][13].

This project, Educado, is created by AAU students who also founded the company SomethingNew I/S. In collaboration with AAU, SomethingNew started this initiative with the objective of helping the Brazilian waste pickers transition to employment by providing them an educational platform. Since the mobile app will have potentially many users, it needs privacy and security implementations and mechanisms as it lacks these properties.

With the need to apply personal data in the app, their privacy must be considered. Users of Educado need to be protected, whether it means to keep confidential data hidden or anonymize profiles. There is no security or data protection in mind in the development of Educado, as we are introduced to the project. However, with our understanding of cyber security, we are able to contribute on this aspect, which both improves the app for the user and from a legal point of view. Both we and SomethingNew are aware that the app must be compliant with the data protection laws in order to be usable for the waste pickers.

As the development team of Educado is located in Denmark, all processing and analysis of data must be compliant with the data privacy laws used in Denmark. In Brazil, another privacy data protection law, *Lei Geral de Proteção de Dados* (LGPD), was passed in September 2020, enforced in August 2021, which should be considered as the mobile education platform is used by waste pickers located in Brazil [14]. GDPR and LGPD have many similarities, and some of the definitions of terms in LGPD echo the GDPR's definitions, meaning being compliant with both data protection laws at the same time should not raise any issues. Both ensure that users must know what their data is used for, in the system [14][15].

For this project, we will study the relevant laws and security measures needed, in order to understand how compliance is achieved. We therefore apply our knowledge to recommend and provide guidelines on best practices. By realizing these approaches and techniques, we demonstrate by a case study in a real-life scenario, Educado.

1.1 Problem Formulation

As mentioned in the introduction, the focus of the project is to make the Educado mobile education usable for waste pickers, to support their opportunities on learning finance. This includes prioritizing the privacy of the users and making the app compliant with the data protection laws. To understand what is needed to be compliant for an application such as Educado, we define the problem formulation:

How can we document best practices and recommendations to ensure privacy and data protection for applications?

To make sure the mobile app can be compliant with the data protection laws, the sub-questions below are used to specify which direction or technologies that are used in the project. The following sub-questions are thereby used to support the main problem formulation mentioned above.

- How can a case study approach be used to emphasize the importance of implementation on privacy and security measures in a real-life context?
- What strategies, rules, principles, privacy and security mechanisms are required in order to be compliant with GDPR?
- What is necessary for Educado as a case study to create a DPIA, a TIA and a privacy notice?

1.2 Delimitation

The delimitations listed in this section are the challenges we have encountered throughout our thesis. Each of the challenges have shaped the scope of the project and set the direction on certain parameters that needed to be considered.

1.2.1 State of Educado

When the project of Educado Ecosystem was initially pitched for us during the beginning of the semester, the condition and state of Educado was under development as many groups were working on the same repositories. The functionalities and features were limited, no security mechanisms were implemented and privacy was not considered at all. Due to these factors, there were many potential directions and takes that we could work on. Almost two months within the project, changes were made for the scope of the project. These changes included revert of all the new code branches and clean state was now the reality. The consequences of this very significant change challenged our scope, as we could no longer implement a PET nor security mechanisms as the basic functionalities of the mobile was just not existing and it did not run. A lot code review, migration of cloud technologies and API changes were necessary. This was entirely out of our scope as our thesis is about privacy and security not on app development.

In other words, the development state of the ecosystem, during semester start 2023, has been conflicting as many factors had to be managed and sorted out such as migration from one cloud service to another and many more. Furthermore, there has not been any functional code that make the mobile app usable. In order to add privacy features and mechanisms it requires a lot of code reviewing or to completely start from beginning. As this thesis is not about coding and/or code review the implementation has been deselected.

SomethingNew began the production of Educado in 2021, and the project has since then been presented to partners and stakeholders. As of writing this report, there are many stakeholders involved in the production of Educado, such as SomethingNew, Aalborg University and University of Brasília. Department of Computer Science from Aalborg University is one of the contributors with their Software Engineering students who develop and work on the Educado Ecosystem for one semester. These students follow requirements given by SomethingNew. Furthermore, Brazilian students are working on the educational platform too as part of the SDG Challenge. The influence of these stakeholders has been significant and has had an impact on our project. Progress of implementation work has been strongly dependent on the decision making of the co-founder of Educado, which resulted in a change of our project in such a way that we did not continue with further involvement of SomethingNew. In this case, we have taken the scientific freedom to make hypotheses and apply that as baseline for our research.

Due to theses factors, we made a decision of changing the project to recommendations on best practices, guidelines on how apps can become privacy compliant and secure, with Educado as a case study and not the focus of the project.

1.2.2 Case Study

This project is focusing on how to ensure privacy and security in applications and conduct a research on how to be compliant with data protection laws. Therefore, a case study of Educado will be examined in order to showcase how and which precautions, privacy features and security mechanisms are required to implement within that specific application.

The Educado system consists of the mobile platform targeted waste pickers as well as the web app intended for content creators. Researching about the data protection laws is relevant for both the mobile and web app, however for this project, the focus is to protect personal data of the mobile users in the system.

The analysis in the report is made with the idea of implementing compliance in the app, meaning the discussion will include how implementation would be realised.

1.2.3 Focus on the developer's point of view

We are studying Cyber Security, which is a Master of Science in Engineering. Our experience in law is limited compared to lawyers, and looking into the data protection laws of different countries is seen as a challenge. The project is thereby made from the engineers point of view, with technical backgrounds and knowledge on app developments capabilities and functionalities. However, external support from

law students or professionals are required for verification to ensure compliance with GDPR and LGPD is achieved. We can only request for verification however we cannot expect a legal documentation as approval for our assessments.

1.2.4 Data Protection Laws

This report focuses on the data protection law used within Denmark and Brazil. Though, services used in the Educado ecosystem are not necessarily based on these countries; Amazon Web Services (AWS) for instance is a US-based company. Though, AWS states that their services are GDPR compliant, and they make use of customer control. Meaning the data can be stored at the customer's desired location, and customers can manage their own encryption keys [16]. With the customer control concept, the data protection law used in the US are not relevant for this project, and the focus is thereby GDPR, which is used in Denmark, and LGPD, which is used in Brazil.

1.2.5 Language Barrier

When searching for sources on our topic, it has been challenging to find relevant papers in English. We identified a number of research papers regarding LGPD implementation written by Brazilian professors, which looked very promising based on its English abstract, however, the remaining of those articles and papers were written in Brazilian Portuguese which made it very difficult to read and assess its content. In these cases, Google Translate would not give a proper translation and we chose to only focus on papers written in English. Mostly, material search on LGPD has given some issues due to them being in Portuguese, when we translated by Google, the same terms or glossaries gave different meanings or words. A good example was the ten data processing principles of LGPD, whereas the third principle in Portuguese was translated to *Necessity* and *Need*. Therefore, when referring to other sources (in papers, articles or websites) they were defined differently.

2 Methodology

This section covers the approach and decisions we made along the process in order to complete the project, including case study as a method. To work on the case study, we had to gain the knowledge on relevant aspects of data protection. Information on data protection laws in general gave us an idea on how the GDPR specifically has a lot of rules to follow in order to comply, and in regard to our study case, how Educado can comply. The research part of our project is therefore documenting requirements to keep in mind, when we proceeded to start our risk analysis.

The risk analysis consists of mandatory impacts assessments that was discovered in our research. By conducting a DPIA and a TIA, we understand that these are usually assessed and managed by lawyers. Therefore, we planned to seek validation from experts, both within Denmark and Brazil, to ensure our attempt is similar and appears realistically close to the industry in general.

2.1 Case Study

A case study is being applied as a research method in which Educado will be the main focus. This research method is providing an analytic generalization based on knowledge gathering on the identified research questions. As this method is non-experimental, the outcome of this case study will be efficient for answering the *how* and *why* of our problem formulation. By exploring all the relevant materials and information on how to be compliant with data protection laws, we are following some procedures in a systematic manner. This research method comprises of six steps that needs to be followed as follows [17]:

1. *Plan*: In this phase, we determine which type of research method to use that is relevant for our specific case. By having identified and created our research questions we know that the form is a *how* and *why* we decide to go for a case study in comparison to, for instance, a survey. Furthermore, we are understanding that it has its strengths and weaknesses being that case studies are very difficult to write as it can take long and can result in enormous documentation. However, its strength lies within giving us the ability to conduct an analytical generalization as the case study will be used to highlight and result in conclusions on how to document the security and privacy mechanisms in any mobile application, and provide guidance that can actually be realised within a real-life context such as the Educado system. It is also important to emphasize that we are conducting a single-case study and not multiple-case studies as a research method.

2. *Design*: The research design is all about making a clear idea on how to collect sufficient data and which strategy to use when studying. There are five components in the research design which are important to address:

    2.1 *a study's questions;* Here we are being very explicit about what type of research questions we are solving, how to make these questions on whether these questions are relevant and can be explored further or not. This has been covered in the Plan. We found our problem statement and the supporting research questions by doing a problem analysis on privacy and security measures on applications and then narrowing down the scope to our case study, Educado. By getting an overview of the problem domain, we could derive our question to steer the project.

    2.2 *its propositions, if any;* By now, we are interested in finding out what we are studying and what should be investigated or examined.

    2.3 *its unit(s) of analysis;* The case is being defined, and in our project, it is the privacy related to Educado which is being the primary unit of analysis.

    2.4 *the logic linking the data to the propositions and;* Analysis will be made about the propositions identified earlier and connections to the collected data is being made, if any.

    2.5 *the criteria for interpreting the findings.* In this last part, other explanations to our findings will be given. Justification of our findings will take place, and in this way create a plan for future studies and cover other aspects as well.

All the above mentioned components is helping to create preliminary theory on our study about privacy and data protection laws. In other words, the theory development will establish the basis for the rest of the study as it will be done before collecting any data which is different comparing to other methods. In consequence, this theory development helps to conduct the data collection and also generalization from the case study.

3. *Prepare*: This phase is about preparing collection of data. Our approach was preparation of relevant questions for the waste pickers before visiting the recycling complex. In order to be able to ask proper questions we collaborated with the Brazilian students; writing the questions in English and making them as easy to understand as possible for our target group, recording of the interview was prepared and a translator was given our questions. Furthermore, we planned to protect the human subjects in our case study by asking for permission of we can record the interview with the waste picker in our project. Before applying any figures or illustrations in our report we sent a written request for applying those researchers work in our project. We are being aware and our obligations to the privacy and ethical practices of conducting our research. This was executed by gaining informed consent from all of those involved in our project. The project was also initiated by asking for access to several systems from the stakeholders, such as access to Educado's database, file storage and code repositories. During this phase, we uncovered problems in regards to our project and addressed our research team's capabilities. This was done by addressing and pointing out all the limitations that we would encounter during the process, such as time zone difference with correspondence to our Brazilian contacts, language barriers (Portuguese resources that needed translations), technical limitations and time constraints, and finally our lack of legal expertise (as we are engineers, not lawyers). The positive aspects was addresses at our very helpful and native-Portuguese speaking collaborators who works with LGPD on a daily basis. We also got to find out how much it will cost have a lawyer to review an assessment, and an estimation of the expected time to have legal work approved. We made sure to have sufficient resources such as access to the main stakeholders, in this SomethingNew who provided us access to their code base, opportunity to get interview with an actual waste picker in Brazil and to see from that person's point of view on the mobile app and opinion on privacy and security in general. Additionally within the field procedures, we made sure to make it possible for asking help of people who got more experience and expertise within law enforcement and data protection laws. Lastly, we plan how to make a case study considering how to document the case study report and a basic outline that will help us to collect the relevant data to support it.

4. *Collect*: This is the most practical phase in which all the necessary and relevant case study evidence are being gathered. These come from different sources and therefore requires to follow different data collection procedures. We collected data through documents (standards and laws), interview with a waste picker, direct observation when we visited the recycling complex when in Brazil and observation of one brief and limited demonstration of how the Educado Mobile App was being used by the co-founder. Although, the app was very limited and did not work properly, we got an idea of how it would look like. By doing a field observation and single interview in Brazil, it gave us a more realistic picture of who the target of the mobile application are and in what conditions the app will be applied. Another important source was the documentation of the Educado Ecosystem through the co-founders. It was their bachelor thesis on the creation and implementation of Educado Ecosystem which provided the foundation for the case study. This was unobtrusive, meaning that it was not created or outcome of the case study, but actually prior to it. The bachelor thesis was written almost three years ago. As a starting point, it was a good source, although it had its limitations. The issues were that it was outdated, a lot of technical decisions has been made and implemented since then. Since many stakeholders are involved now and the fact that it has been an ongoing project the report only gave the fundamentals and why it was created. Interview was another source of gaining information on Educado, this was mainly targeted and was focused on privacy and mobile apps. It was insightful since we got a better understanding on how much privacy the users actually are aware

of and how important it is for them. The direct observations was helpful too as we saw the realities of the users in real time and that gave a lot of context and supported some of the points covered in the report by the co-founders of Educado. Another important source is our email correspondence with a Brazilian lawyer who is an LGPD expert and works with data protection laws and privacy on a regular basis. The Brazilian lawyer provided information on regarding how complex it can get a formal assessment approved, including an estimate of how many professionals are needed, along with an estimation of amount of hours to spend.

5. *Analyze*: In this phase we were drawing conclusions empirically by data analysis. This means, that we analyzed the collected data from the previous stage in strategically analytic manner by prioritising the findings. Based on the weight of the data, we determined and examined how to draw conclusions in such a way that it can be evaluated and kept examining, categorizing, comparing and analyzing until our problem formulation and the supporting questions were answered. There exists four different general strategies to analyze; relying on theoretical propositions, usage of qualitative and quantitative data, developing case descriptions and examining rival explanations. We have been analyzing by relying on theoretical propositions. In other words, simply answering our identified research questions.

6. *Share*: As the final step, the outcome of the analysis and studying are being shaped into a report containing the findings and results. In our project, we use the case study as one method amongst a few others for the entire thesis.

This methodology has been used as an approach to our study and research by focusing on a single and specific case. By gathering data and using the analytic techniques we gain an insight into how to give specific example within a real-life context on how to provide guidance to ensure privacy and data protection for applications in a generalized manner [18].

2.2 Empiricism

Our research has been heavily empirically focused and therefore it chosen to conduct an empirical research before initiating the project work. Prior to systematically collecting data and analyze it with comparison to our previous knowledge, we had to gather evidence that could be verifiable later in the process. Therefore qualitative research method has been applied to help draw conclusion based on the findings on this. This was carried out by us travelling to the federal capital of Brazil, Brasília. Our academic journey had one objective, to work on the SDG Challenge, Educado with our Brazilian collaborators. In relation to our problem, we had to see the context, scope and define the purpose of our research. As an essential part of the journey, we had to visit the recycling complex in Brasília. Here, we observed how the target group, the waste pickers worked, their working conditions and listened to presentations on the issues that waste pickers face and how large the problem is in reality. By observing the complex we could gather more information which gave us a deep insight into how the working conditions were and what it would mean for them to use Educado mobile app in that setting. Furthermore, we had a one-on-one interview with one waste picker, who was within our focus group. By conducting that interview with our Brazilian colleagues who translated the questions, we gained an insight into how important privacy is for them. By observing, asking targeted and specific questions and being there on the field, it gave us a fuller understanding and ground on what measures of privacy are necessary. We were able to narrow down the scope of our project and examined the problem by a real-life lens. This motivated us immensely, as we met these people who had difficult life conditions and we believed that our contribution of making their data private and giving the security for the education platform that would give them a better future for themselves and their children.

2.3 Research

In order to decide the best practices and recommendation for the specified case study mentioned above, multiple methods must be considered, including understanding the relevant data protection laws as well as how compliance of the laws are achieved. A background section is thereby used to develop an understanding of relevant terms within Privacy and Data Protection. Having a basis understanding of privacy includes looking into the terms that are well known within Cyber Security, and which technical measures that are applied to ensure privacy of personal data. The Europeans adopted the GDPR and were compliant with the law by following the requirements listed herein, and these required measures are used to ensure a secure system, which is the goal for Educado.

However, not all requirements in the project are pre-defined by the laws, some requirements are also defined based on the research of the State of the Art (SOTA). The SOTA is where similar products and/or solutions, that already exists on the current market, are compared with the current state that Educado is in.

Assessing how other businesses and organizations are successfully achieving compliance can used to gain knowledge and inspiration on how to accomplish more success on Educado and its current ecosystem [19]. As the project is privacy-focused, the success scenarios must be related to the problem formulation and thereby law-based. However, it is also essential to analyze examples where compliance has not been considered, and understand how that product became less successful.

Specifically, SOTA is used in this project to serve as a starting point for the current research and development within this project scope. By finding research papers based on some specific criteria and parameters, we lay the foundation for the discussion of our report. This search of relevant material on implementation and of data protection compliance and noncompliance has been through Google Scholar in which we defined and assessed whether they have any relevance for our problem statement that we are analyzing. By conducting a thorough, selective and deep search on existing solutions and similar cases as ours we can clarify and define the focus of our problem as well as shedding light on the problem that we have chosen to focus on. By going through a search of research papers and projects, we are able to get an overview of what has been already done in this scope and what has not. Therefore, searching, reading, assessing and evaluating, comparing different methods, analyzing the outcome of others work and link the different sources are the initial stage of this analysis of the problem domain. The outcome of the SOTA will provide us the basis for our contribution to this project.

Hence, Literature review has not been the approach as we only focus on the most recent and updated techniques and implementations of compliance on the chosen data protection laws. As the legislations and laws can be changed, it is more beneficial to conduct a SOTA. The actions that we have been taken is defining the scope of the project, searching for relevant sources and gather information on this field by reading, taking notes, organizing our references and analyse this. This step has been done to help us identify all the issues and missing research points that have not been made. We have had criteria regarding information search and gathering in such a way that we look at relevant sources and the recently published ones from large and well known conferences. This includes sources with the latest news and updates on the relevant data protection laws, as some laws are revised as of writing this report, meaning other measures are to be considered in the future. Furthermore, we have been collecting information from national governmental websites when it comes to Brazilian laws and regulations as well as identified communities working in this field. In order for us to get exact and precise information we have contact persons in Brazil that we have seeked advice on the Brazilian laws, by UnB professors who are in charge of the recycling complex transition of the waste pickers, and we have consulted with an Brazilian lawyer whose work area is compliance with LGPD with many more. Additionally, we have selected some articles that are scholarly, published from universities and paid attention to the impact factor of journals and number of citations and when it has been published. By keeping an overview, we have kept a track of references by just normalising bib entries, taken notes while reading and discussing each source identified as relevant for the problem.

2.4 Risk Analysis

As the research has identified a plethora of examples on compliance and noncompliance, we were able to apply our understanding into relevant risk analysis approaches, which in this project are the DPIA and TIA, both impact assessments used when referring to the GDPR.

Applying risk analysis means establishing an overview of potential critical risks in a system by identifying different types of threats and vulnerabilities and assessing the consequences of each vulnerabilities being exploited [20][21]. Usually, the risk management contain many types of categories to consider, and it is highly recommended for companies to identify their vulnerabilities [20][21][22], however this project is focused on the privacy aspects of the system, and the risks chosen are thereby only privacy related.

A DPIA helps identify risks regarding data protection, as GDPR requires companies to handle high risks that are a threat to potential privacy impact [23][24]. The aim of a DPIA is to make sure that companies working with data and processing of information must be compliant with the data protection legislations. It is recommended to carry out a DPIA early in the project and is also required to be updated accordingly. Therefore, one method to protect personal data in our project is by conducting a DPIA early in the stage of a project plan. By applying DPIA, it might happen that modifications and changes will be added to the ongoing project. This method will help identifying any issues that might affect process and the data of the users. Educado is responsible for carrying out DPIA and anyone involved with the security aspects should take it into consideration. Hence, we will determine whether we need a DPIA or not, how we will conduct one and what measures should we take in order to mitigate any identified risks. By initiating the DPIA with a screener, the decision on whether one should be carried out or not will be well documented along with its reasoning. Based on this evaluation, one can answer a couple of questions called "*DPIA Screening Questions*" which help determine whether a DPIA is required or not [23]. In this case, a screener has been filled as seen in Table 20 in Appendix A to confirm that this project requires a DPIA.

We will be conducting an assessment based on how we collect data, store data, use the data, who will have access to which data, to whom the data is being shared, security measures and what are the high risks. Furthermore, we will be describing and getting an overview of the capacity of the data with its type of data, how sensitive the data is, how we process the data based on how long and where. We will be analyzing where the data comes from, how much control users have over their data, the users' age and which technologies are being used and is security implemented or considered.

We will explain why we made a DPIA and relate it to requirements in which the Educado Ecosystem must follow. This will be done through a document in which we detail in systematically order provide arguments. Hence, any data flow and connections between systems, users and data controllers will be given. The DPIA that we are conducting are seen in the following steps [25]:

1. Identify need for a DPIA
2. Describe the processing
3. Consider consultation
4. Assess necessity and proportionality
5. Identify and assess risks
6. Identify measures to mitigate risk
7. Sign off and record outcomes
8. Integrate outcomes into plan
9. Keep DPIA under review

To carry out a DPIA, a template for *professional services / general use* is selected, as Educado is a service built by SomethingNew, instead of the research project template [24]. The template provided by University College London showcases which factors a service must consider, to prevent high risks. However,

some risks might be more relevant for other products than Educado, and therefore not all questions in the DPIA can be answered, as it depends on the product and demographic, where as the templates used is focused on European products that comply with GDPR. There are examples of questions in the template that depends on products and they are not highlighted in the DPIA risk analysis in the report, however they will be discussed by the end of the results, to which extend the question can become relevant.

Another method that will be applied is a TIA which will ensure that any risks related to the data transfer within Educado, across different fields will be handled and documented properly. Since, there are transfer of personal data of Brazilian citizens data between Brazil and Europe, it is important to be in compliance with all associated authorities. As the DPIA, TIA is mandatory according to GDPR whenever data is transferred outside EU, and must be conducted and documented [26].

The importance of the TIA is more specifically shown when data from EU is transferred to countries that are not listed as a country with adequate level of protection. Some countries out of EU are already trusted without the need to conduct a TIA, however Brazil is considered as a third country without an adequate level of protection [26].

We chose a template from Health Service Executive, a healthcare system in Ireland. Applying material from a healthcare system, we believe their transferring of data is prioritized to protect their users, and we thereby choose to make use of the provided template [27].

When conducting a TIA, one must define who the data exporters and data importers are, in order to present how the data is transferred internationally between organizations and companies [26]. Multiple stakeholders are involved in the development of Educado, however it is only SomethingNew that handles the data transferring. The TIA of this case study has therefore some differences from other TIAs, as the data is collected directly from Brazilian users though the mobile application, and transferred to Europe for processing and storage handled by SomethingNew. The data exporter and data importer is thereby the same instance: SomethingNew. The result of the TIA thereby appears different, however it has been assessed that conducting the TIA for this specific case study is still relevant and educative for us, to reflect a realistic approach to comply with the GDPR in general.

2.5 Validation

Both the DPIA and TIA requires to be approved according to the GDPR in order to confirm compliance, however with our limited resources as Cyber Security Engineering students, we have restricted options to obtain approval and legal advise on both impact assessments. Approving these assessments is usually done by data protection officers within the concerning organization (if available), or other relevant experts and stakeholders [25][28].

We will be seeking consultancy by different individuals who can help us shed some light on the processing of the data and ask for guidance and advice by our Brazilian collaborators along with lawyers and Brazilian students working with LGPD. As the DPIA template is from the GDPR perspective, the validation from the Brazilians also confirm that the assessment is approved from an international point of view, where the LGPD in Brazil is complied with as well.

When the impacts assessments are conducted, and perhaps approved, a privacy notice is expected to be written based on the decisions from the analysis. Specifically the DPIA contain information on how the storage of data is protected and the TIA contain information on transferring of personal data internationally. A privacy notice can thereby be used to highlight the important points of the assessments, which are relevant for the users. According to both GDPR and LGPD, the privacy notice is also mandatory, as it is also used to inform the users about their rights [14].

There does exist a distinguishing between a Privacy Notice and a Privacy Policy. Although both terms are used interchangeably and can arise confusion as to when to use what. The core differences are that Privacy Policy are more directed towards internally for an organization or service whereas a Privacy Notice is applied externally. According to the International Association of Privacy Professionals a Privacy Policy is defined as internal documents on how to manage personal data [29]. By contrast, a Privacy Notice is defined as a statement on handling of personal data showcased for the data subjects [30].

The template we utilize to conduct our own privacy notice is provided by Information Commissioner's Office (ICO), who regulates data protection in United Kingdom. We find them reliable, as they offer advice and guidance on GDPR compliance [31]. However, the privacy notice within GDPR has some changes to the LGPD version, so we choose to study the LGPD privacy notice requirements and merge those with the GDPR template, to comply with both data protection laws [14].

3 Privacy and Data Protection

Privacy and data protection laws are essential in order to establish an understanding of how the Educado platform can be compliant. Terms that apply in both privacy and cyber security are therefore defined to establish a common ground. The terms that are introduced in these sections are used throughout the rest of the report. The GDPR will be introduced as well, including their relevant processing principles, data subject rights and assessments. Furthermore ISO, a separate framework, is specified to highlight tools used globally.

3.1 Privacy

The data protection laws are used to ensure privacy to users as well as letting users gain more control of what data is shared and used in a system [5]. User privacy is ensured by protecting what GDPR refers to as *personal data* [14] and lets a user know what their rights are, in terms of a system's data use. The term privacy can thereby be linked to Alan Westin, as he defined privacy is "*The claim or right of individuals to exercise a measure of control over the collection, use and disclosure of their personal information*" [32].

Based on this definition, personal data must therefore not be exposed, which also relates to the gray box on the right in Figure 1 below which highlights privacy risks. Compared to the security risks in the orange box on the left, the privacy risks are more focused on the personal data and data processing. However, the green box in the middle of Figure 1 highlights the intersection between security and privacy risks. The common ground of security and privacy risks refers to the privacy issues within cyber security caused by wrongly handled processing of data [33]. With the use of data protection laws, implementing secure data processing is a necessity along with other privacy risks found in the gray/right box. The distinguishment between security and privacy risks in this project are thereby defined by the Venn diagram in Figure 1, where the green/middle and gray/right boxes are the focus throughout this project. These risk are essential to touch upon, as it relates to citizens' fundamental right to privacy [34] and must also be compliant with GDPR by law, which is further elaborated in Section 3.2.

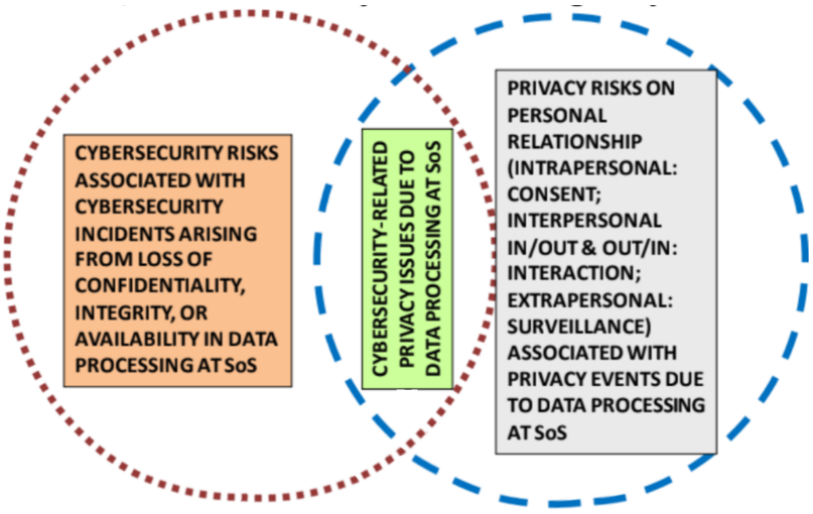

Figure 1: Modified Venn Diagram of Privacy and Security [33]

Even though the focus of this project is not on the cyber security risks in general in the orange/left box in Figure 1, it is still relevant to define some of the terms within that are commonly applied [33][35]. As seen in the orange/left box, these terms are Confidentiality, Integrity and Availability, shortly known as the CIA triad. There terms are commonly used for categorising and identifying vulnerabilities in a system. Their categorization gives an idea of which measures should be considered, when developing a product.

All three standards should be met to ensure better security, to protect a product on all aspects. Each standard is further elaborated below [35]:

1. *Confidentiality*: When collecting (personal) data, we must ensure that data is kept secret by for instance enforcing strict policies on people's necessary privileges and encrypt the data. Confidentiality is compromised if data is shared without proper authorization, and it is therefore important to prevent others from stealing the data and avert exposure of data by human error.
2. *Integrity*: Integrity means keeping data accurate. The data collected must not be tampered with, as data will appear unreliable, and the data controller will appear untrustworthy since someone was able to modify with (personal) data in the system.
3. *Availability*: When a user is utilizing a system, that system must be available. If someone with malicious intend were to disable the communication, network and/or application of a service, no user would be able to use that service.

As these terms are mostly used within the cyber security field in general, not all risks in this standard are included when discussing privacy risks. Confidentiality is the most used standard within privacy however, as it is used to ensure private data is kept private.

Besides ensuring confidentiality in privacy, another goal is also important to ensure when talking about preserving privacy. There exists many security mechanisms and implementations that plays a crucial role when identifying potential risks. Most important techniques are the hashing and cryptography mechanisms.

In order to maintain the integrity of data, hashing can be applied. In simple words, hashing is a technique or more exact an algorithm that takes plaintext as input, do some mathematical operations on it, and output ciphertext. This output is usually called the hash value. These hash algorithms or functions are one-way, meaning that you cannot take an output or the hash value and convert it back to the original form. Hash functions play a crucial role when authenticating messages. A good example of a secure hash algorithm is the HMAC which stands for Hash-based Message Authentication Code. Cryptography is another concept that is very closely related to hashing. As hashing ensures data integrity, cryptography ensures confidentiality of the data by a variety of encryption methods and securing data communication. Cryptography takes plaintext and perform computation which is encrypting it and making it unrecognizable for any adversaries without having the key to decrypt the message. Usually, cryptography can be divided into two major categories: symmetric encryption and asymmetric encryption (also known as public key encryption). Cryptography helps secure storage, communication, transfer, processing and sharing of data. To be more specific, web browsing are being kept secure by Hypertext Transfer Protocol Secure (HTTPS) where it encrypts the data shared between the client and server, authentication and access control in which digital signatures and/or certificates are being applied, password protection, and many more [36].

Cryptography plays a significant role when it comes to privacy enhancing technologies. PETs are technological mechanisms that may be implemented in order to ensure protection of data, by for instance anonymizing personal data. PET are still not commonly used, however, they are recommended, especially for large companies [37][38]. A company can not simply add a PET into their system, as it requires an overview of the data within the company as well as understanding the technical capabilities and mechanisms used regarding data protection in the company.

Differential privacy is where noise is added to the processing of personal data, meaning the data might not appear exact when analyzing user activity, however, the data of user's activities can not be linked to the users account [39][40].

Federated Learning is another PET mostly used on edge devices, such as mobile phones, and is known for turning a centralized system into decentralized data. This machine learning technology is used to process personal data locally within the user's device by applying a locally trained model and anonymize data by merging multiple trained models together, without sharing raw user data to a company's central database. Feeding the database with encrypted, anonymized responses regularly allows the company to improve the central model, by processing user data, while federated learning allows privacy and protection of the individual user's information [39].

3.2 GDPR

In this section, the laws and regulations regarding data privacy protection relevant to Denmark is described. As data protection laws are used to ensure the privacy and security of personal data [6], it is important to understand how organizations or companies collect, store, use and share personal information about its users. Hence, GDPR will be introduced since the law exist in order to protect natural persons or individuals from having their sensitive information misused by entities [6]. Later in the report in Section 4, it will be elaborated on how data protection laws vary depending on the geographical placement. GDPR is the European privacy regulations, however it can be compared to other data protection laws, as all of them share a mutual goal of preserving individual privacy rights [14].

The GDPR is EU's data protection law, which is relevant for this project as Denmark is part of EU [5]. It is a requirement for SomethingNew by law to be compliant with GDPR, resulting in fines in case of violation. All the requirements that organizations must comply with since May 28, 2015 may be a lot to consider for smaller companies, as GDPR is known as the most strict privacy and security law in the world [5][6]. However, more people are depending on their personal data and expects their data to be handled securely. A user on the Educado app is considered a *data subject*, and by applying GDPR, they have the right to have more control over any information that is related to them as a person, called *Personal data* [6]. SomethingNew being the *data controller*, they are handling the *data processing*. It is SomethingNew's responsibility to process the data, including handling any data of any sort, which could potentially be considered personal data [6][16].

In order for European companies to be compliant with GDPR, they must follow the data processing principles, known as *Principles for relating to processing of personal data* in Article 5 (See Section 3.2.1), where companies are expected to abide by the principles in order to ensure proper protection of personal data. However, the principles are simply 1 out of 99 articles in total [5]. Some rules to highlight are the data subject rights (See Section 3.2.2), DPIA (See Section 3.2.5) and Privacy notice (See Section 3.2.6), which must be implemented if personal data of users are processed by a company.

3.2.1 Personal Data Processing Principles

Both GDPR and LGPD have a list of principles for personal data processing, which are fundamental for the data protection laws. These principles ensure security and accountability of personal data, resulting in companies being better protected against data breaches if all principles are applied [14][41][42]. From the user's perspective, these principles also provide more user-control. With a privacy notice (See Section 3.2.6), the user can establish an overview of how their personal data is processed in a company [43][44].

The data protection principles in GDPR's Article 5, *Principles relating to processing of personal data*, are applied for all data processors, whenever personal data is processed [6][41]:

1. *Lawfulness, fairness and transparency*: Documentation and policies of data processing must be visible for relevant parties, including the data subject.
2. *Purpose limitation*: The data shall only be collected for legitimate and specific purposes, and further processes cannot occur if they do not correspond to the initial purposes.
3. *Data minimisation*: The data shall be limited to the purpose for which they are processed.
4. *Accuracy*: The accuracy of the data must be ensured, where inaccurate personal data is erased.
5. *Storage limitation*: Identifiable data must only be kept if necessary, where as other personal data may be stored for longer, for instance for applying scientific or statistical purposes.
6. *Integrity and confidentiality*: The data must be secured against unauthorized processing, which shall include use of trusted tools.
7. *Accountability*: As the controller is responsible for data processing, the controller must document and demonstrate that they are compliant with all the aforementioned principles.

3.2.2 Data Subject Rights

GDPR provide the data subject rights. The users must be informed that they have these rights, due to the transparency principle [14]. The data subjects usually find these rights in a privacy notice, where all rights are written in clear and plain language. Below is the list of rights [14][45]:

1. *Right to be informed*: Before processing of personal data is allowed, it should be clear towards the data subject what personal data is collected, and how that data is processed. This is the right mentioned in Article 13. A privacy notice with these information shall be provided by the service, easily accessible to the data subjects [45][46]. Privacy notices are elaborated in Section 3.2.6.
2. *The right of access:* The data subject can request to access their personal data, where the data controller must reply within a month along with a list of elements found in Article 15. In the response, points that must be included are for instance the purpose of the processing, the categories of personal data concerned, etc. [45][47].
3. *The right of rectification*: If the data subject already has personal data stored in a service, they can according to Article 16 update and/or correct inaccurate personal data [45][48].
4. *The right to erasure*: As personal data is processed in a service, a user might wish to stop the processing and have their data removed. With Article 17 of GDPR, *Right to erasure ('right to be forgotten')*, users have the right to freely erase use of personal data. If personal data deletion is requested, the data controller must act, as well as inform the third parties that happen to process the aforementioned personal data, to ensure data is not processed without the user's consent. A list of exceptions are listed in Article 17 [14][49].
5. *The right restrict processing*: If it is not wanted to be fully removed from a system, the data subject can instead request to restrict the processing of personal data, if one or more conditions apply in the list mentioned in Article 18 [45][50].
6. *The right to data portability*: If requested by the data subject, their personal data can be transferred to the data subject that it concerns. Article 20 mentions how this personal data can be forwarded to a third party in its original form, if requested by the data subject [45][51].
7. *The right to object*: In case the data subject does not wish to have their personal data processed, they can according to Article 21 object to the processing. However this may not be possible, depending on if the data controller fall under one of the expectations, for instance if it is necessary for legal claims [45][52].
8. *Rights in relation to automated decision making and profiling*: There might be decisions system that is based solely on automated processing, where Article 22 mentions that the data subject can reject these automated processes, and ask to not take automated decisions whenever their personal data is applied [45][53].

3.2.3 Implementation of Data Protection

To achieve GDPR compliance, companies must implement mechanisms and good practice that ensure data protection. GDPR's recommendations within implementation of data protection aims to protect personal data using principles and programs [14].

PETs have been one of the effective ways of ensuring data protection, which has been used before GDPR. The data protection law does not directly mention PET as a requirement, however, it is a recommended approach to apply, as it considered an appropriate mechanism and good practice [37]. There are different types of PETs, where some include minimizing the use of personal data to process or anonymization of personal data [54].

Within GDPR, Article 25, *Data protection by design and by default*, elaborates on how it is required to implement appropriate technical measures, including pseudonymisation and data minimisation, in order to

protect the user's data [55]. *Privacy-by-Design* is a concept that is applied to implement data protection, which is based on the aforementioned article. Seven key principles of Privacy-by-Design have been further defined by Dr. Ann Cavoukian, which is now commonly used to implement Privacy-by-Design and comply with GDPR. The principles are listed below [56][57]:

1. *Proactive not Reactive; Preventative not Remedial*: Be prepared by mitigating potential privacy risk, and prevent issues before they occur.
2. *Privacy as the Default Setting*: A user's personal data must be protected by default, meaning no user input should be required before protecting their data as the default setting.
3. *Privacy Embedded into Design*: When designing an IT systems, Privacy-by-Design must be embedded within the implementation of functionalities, as it is not effective to implement security as an add-on.
4. *Full Functionality – Positive-Sum, not Zero-Sum*: All legitimate interests must be considered in order to reach in a positive-sum, to achieve a "win-win" situation. It is not a trade-off between privacy or security, it should be possible to obtain both.
5. *End-to-End Security – Full Lifecycle Protection*: Whenever a product collects personal data, it is required to apply strong security measures to ensure the data remains confidential. The data shall be securely retained from start to end, whereas the full lifecycle protection requires the be securely destroyed, providing end-to-end data protection.
6. *Visibility and Transparency – Keep it Open*: The transparency principle assures all stakeholders that policies and promises are complied with, which strengthen the accountability and trust. With transparency, everyone involved will know the privacy measures and verify that privacy has been taken seriously.
7. *Respect for User Privacy – Keep it User-Centric*: Products that involve users, must make it user-centric by empowering user-friendly options. This includes for instance strong privacy defaults and appropriate privacy notices.

3.2.4 Transfer of personal data

When working with personal data, especially when it is of sensitive matter, it is crucial to understand how the data flow is being handled. In many systems, data are being stored in databases and hosted through any cloud or on-premise storage solutions. There are many aspects in transferring of this type of data such as which technologies to use, who should have access to what, network latency, the amount of data that can or should be transmitted and many more. However, the implementation must comply with the current legislations and laws.

Based on Article 44: "*General principle for transfers*" [58] processing of personal data, from EEA, that are being transferred to any third country or internationally is only allowed to happen when following strict rules under the GDPR. Therefore, an entire chapter called *Chapter 5: Transfers of personal data to third countries or international organisations* of the GDPR is dedicated to rules and restrictions on transfer of personal data [59]. The transfer is permitted when meeting specific requirements in Chapter 5 of the GDPR, where the conditions are listed in the following articles [59]:

- ***Article 44****: General principle for transfer*

  Transfer of personal data outside of EEA (third country) or to an international organization can only happen when met under certain conditions and rules. The transfer is allowed if the data subject's rights and freedom are retained. In other words, it addresses the principles in which transfer of personal data can occur across European borders.

- ***Article 45****: Transfers on the basis of an adequacy decision*

An adequacy decision can be issued by The European Commission that the third country provides or makes lives up to an adequate level of protection of personal and therefore transfer to these countries can be realised without more authorisation.

- ***Article 46****: Transfers subject to appropriate safeguards*

  If an adequate decision has not been obtained by Article 45, then the data controller/processor must ensure all the necessary safeguards. These safeguards are comprised of Standard Contractual Clauses (SCCs) by the European Commission, standard data protections clauses by Data Protection Authorities (DPA).

- ***Article 47****: Binding Corporate Rules (BCRs)*

  These BCRs makes transfer of personal data permissible with an absence of an adequacy decision. These rules are applied within companies, internal rules, which manages any transfer of personal data within the entire company. These still need to be approved by DPA in order to be applied when transferring data.

- ***Article 48****: Transfers or disclosures not authorised by Union law*

  A third country are only allowed to request information such as personal data from a data controller/processor if there exists an international agreement or legal treaty between this requesting third country and European member.

- ***Article 49****: Derogations for specific situations*

  These are exceptions as data subjects might consent to the transfer of their data or there has been an a contract between the company and the data subject.

- ***Article 50****: International cooperation for the protection of personal data*

  Ensuring that enforcement of the GDPR in all European member countries is accomplished and cooperation with the national data protection authorities is being enhanced.

In addition to this, an analysis called TIA is mandatory by European laws. The obligation of making a TIA comes from the European Commission in June 2021, where they published new SCCs. These SCCs is about any transfer of personal data collected from EU countries to outside of EEA. Transfers within EU is covered by GDPR. This is clearly stated in Clause 14 *(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request* [60] and under Screhms II decision. A TIA is conducted by a data processor/controller who analyzes whether there is an impact or security issues while transferring data outside of EEA when an adequacy is not found by the Commission. TIA contains a number of questions for each personal data and its processing activity. There is no specific standard or framework on how to make a TIA, but the core elements are that considering all the risks that could potentially have a security impact when transferring data. Hence, a TIA ensures compliance with GDPR and mitigates any risks before transferring data [60].

3.2.5 DPIA

The DPIA is part of Article 35 in the GDPR and is known as an assessment that identifies and aims to reduce high risks privacy impact [28]. The purpose of a DPIA is to ensure that companies are compliant with principles of the GDPR and any processing of personal data do not violate the privacy rights of data subjects or natural persons. Basically, a thorough analysis in an organized and systematic approach towards observe and detect any privacy risks and their impacts in relation to each processing activity. Not only, is it a comprehensive analysis for identifying risks but also to take proper measures on how to mitigate those. The process of conducting a DPIA is about identifying the nature, scope, context and purposed of processing of personal data. This means, that it is an ongoing process performed in a company where reviews are made regularly and updates in order to do monitor and address the privacy risks continuously [28]. A DPIA must cover all these aspects and before conducting one, a company can make a screener, which is a questionnaire, that determines whether a DPIA is necessary or not.

3.2.6 Privacy Notice

A Privacy Notice allows users to have more control of their own data, and stay informed of what the company collects about the user [43]. The privacy notice is a document that explains how data is handled, how it applies to the data protection principles in Article 5, and how to perform the data subject rights. Other than listing how the principles are applied, other information must be transparent as well, such as contact information which can be used in case a user wish to send a complaint regarding a business' data processing approach [43][44].

These points must be included in a GDPR privacy notice, as listed in Article 13 [14][43][46]:

1. *Contact and identification details* of data controllers.
2. *Contact details* of the affiliated data protection officer.
3. The *purpose* of processing data.
4. *Categories* of individual's personal data.
5. *Transfer of data* that is shared to third countries.
6. The *period of time* in which the data will be retained.
7. An explanation of rights defined within the GDPR, along with how to *exercise the user rights*.
8. The right to *withdraw consent* anytime.
9. The right to *lodge a complaint* to a supervisory authority.
10. *Existence of automated decision making* if any, along with details of its profiling, logic and consequences.
11. And if the data is not acquired directly from the data subject, a *source* must be documented.

3.3 ISO Standards

International Organization for Standardization also known as ISO is an non-governmental organizations located in Geneva, Switzerland. The purpose of their organization is to assemble experts from all over the world to create international standards in collaboration with 168 member nations. The outcome of their work is documents that has been through a process of approval before being published [61].

There are being made different standards for every field and they are all widely recognized and applied internationally for their efficient, high quality, up to date and best practices. Amongst one of the most well known is the ISO 27001 which is about Information Security and Management Systems. This standard gives recommendations and best practices on cyber security. By providing the standard it documents what measures to take for any organization in order to be secure such as being able to do identification of potential vulnerabilities, maintenance, improvement of cyber security. Organizations can benefit a lot by implementing this standard, as it will help them to identify and detect risks and vulnerabilities early on and at the same time being able to demonstrate and showcase for any involved that all security measures have been considered and protection of data is prioritised in a systematically strategy.

The third edition of ISO 27001, also known as ISO 27001:2022, covers different aspects of cyber security. To follow this standard, one must first define the scope, set references and select terms. Then a list of sections must be followed [62]:

1. **Context of the organization**: Relevant and involved parties within an organization are being determined with their requirements. The context of the organization in relation to the information security management and its scope are being determined as well.
2. **Leadership**: The leader must ensure that any obligations and work related to the information management system are executed. Ensuring and supporting that improvement, integration and communication are the leader's responsibilities. It is the leaders duty to establish the policy and the top management must clarify all the authorities, responsibilities and roles within the organization.

3. **Planning**: This entire section is about identification and addressing risks and opportunities and what actions to take. An information security risk assessment must be conducted that identifies the risks, analyses and evaluates them. By addressing these issues, the risks have to be treated as well which is done by documentation. Lastly, it must be clear how to achieve the information security objectives and which actions must be taken.
4. **Support**: All the necessary resources should be provided by the organization for the information security management system. Having the right people with the right competences to do the work in regards of qualification by either training, experience, relevant education or others. Awareness is another key aspect in which people within the organization are up to date with the security policies, their contribution and impact. A good understanding of communication is crucial in an organization and therefore it must be clear how to and whether the need to communicate internally/externally must be done, such as what to share, to whom, when and how. Documentation is required and it must be updated regularly with good format, reviewed, and well described. This documentation must be controlled, accessible when needed, ensuring the CIA goals and proper version control.
5. **Operation**: With planning of the entire process, information security risk assessments/treatments must be conducted and documented as well.
6. **Performance evaluation**: Documentation on monitoring, measurement and the analysis hereof with evaluation of it must be done. Furthermore, internal auditing must be performed and also the management must review any issues whether they come internally or externally of the organisation.
7. **Improvement**: Continually improvement must be done by the organization necessary actions must be taken to correct the issues.
8. **Annex A (normative) Information security controls reference**: The Annex contains all the information security controls. One of them would be "Information transfer" in which the control is to ensure that all transfer rules, agreements and procedures are set when transferring data between organizations.

4 State of the Art

Data protection laws vary depending on the geographical placement. GDPR is the European privacy regulations, however it can be compared to other data protection laws, as all of them share a mutual goal of preserving individual privacy rights [14]. The most relevant data protection law for this project other than the GDPR is the LGPD, which is enforced in Brazil.

This section introduces the existing solutions and cases with implementation and law enforcement of GDPR and LGPD, where other examples of a data protection law are mentioned as well to highlight the differences and similarities depending on demography. This SOTA serves as a starting point for our analysis and research of this problem. Different examples of approaches, tools or frameworks that are being used to make sure compliance with GDPR in Europe and LGPD in Brazil, and how to implement those to achieve data privacy will be described.

Furthermore, California Consumer Privacy Act (CCPA) will be introduced to analyze the data transferring according to data protection laws, where US have different requirements that Brazil. Noncompliance is introduced as well to highlight what issues can arise when organizations are being noncompliant with a data protection laws, and what consequences that has been experience for those noncompliant.

4.1 Complying with GDPR

The following examples are works of organizations and experts that successfully complies with the GDPR based on their experiences and frameworks. Their approaches, results, and success might be useful for Educado's own success and are thereby compared and assessed.

Martin Brodin wrote the paper "*A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises*" targeted small- and medium-sized enterprises (SMEs) with less and limited resources in EU to ensure that SMEs are compliant with GDPR [63]. The framework consists of the three phases shown below [63], and it was tested on multiple organizations to prove the phases do support GDPR compliance:

1. **Analysis**: Determining the current app's state of security and information control. The framework does this through a couple of steps:

    - *Information Analysis*: Identify all personal data used in the system; each individual type of personal data are processed on each Post-it and establish an overview. Connect each Post-it to location of processing; is the information processed on paper or digitally? Document if a Post-it is processed externally (which potentially require a data processing agreement).
    - *Information flow analysis*: Define the flow and how the personal data moves between systems.
    - *Information classification*: Classify the personal data according to GDPR.
    - *The legal ground for personal data processing*: Assess the legal ground of each Post-it's documented personal data.
    - *Information and IT security analysis*: Ensure that the personal data is secured.

2. **Design**: Routines, policies and templates are carried out in this step. For instance applying a DPIA on the system here would be beneficial.

    - *Updating routines where personal data are processed*: Ensure the personal data is handled correctly.
    - *Creating routines for managing requests from data subjects*: Companies must strengthen and respect the individual's rights and requests.
    - *Create or update process for data breaches*: Incidents on breach of personal data must be reported to the regulatory authority within 72 hours.
    - *Update personal data policy*: Laws older than 2018 must be up to date and follow GDPR's policy.

- *Create templates connected to routines and policies*: Ensuring the team follows the same solutions. Data processing agreement is recommended.

3. **Implementation**: As the management of personal data is handled, implementation ensures a long-term structure. Throughout time, policies and routines might be adjusted.

   - *Communication*: Everyone in the team must be informed about the changes to be made.
   - *Education*: GDPR must be in mind whenever new data is used, the team must be up to date and understand the laws.
   - *Adjustments*: If anomalies in the structure appears, instructions and documentation must be adjusted, education towards the team must be updated.

The evaluation of the framework showcases how the three phases are used to control data in a secure way, as well as establishing long-term solutions to ensure the compliance becomes continuous. There were three chosen organizations to test this framework, where all three were reviewed and approved by experts [63]. The results thereby do show that this approach can be a useful and structured way of ensuring GDPR compliance, however the framework is only tested on a couple of Swedish SMEs.

While this approach is focused SMEs, other approaches are assessed as well.

Hitchen, Denleyis and Foulsham all have more than 30 years of experience within IT and Technology, when they got together and wrote the book "*GDPR - How to Achieve and Maintain Compliance*" [44]. The audience of the book seem to be very general, however they do seem to highlight companies who apply Business as Usual (BAU) as they have advantages adapting to the approach they describe in their book. The authors choose to list tips, not in a specific order, and not every point is needed for every company, but all points are relevant to consider for companies that must be compliant with GDPR [44]. Not all tips are listed below, as some of them are background knowledge focused, for instance the tip "*This is a business project, not just IT*", instead, this section highlights the action-focused points of the book.

- **GDPR Tools** are recommended for assisting with GDPR compliance, including *Microsoft*, *SNOW*, *Nymity*, *Totalprogramme*. They highlight that applying the tools does not result in GDPR compliance by itself, though they can be used to support the process.
- **Create an action plan and form your project team(s)**. With multiple teams divided in different tasks, each team can focus on specified topics, for instance make one team identify issues, and another team address the various identified issues found. Alternatively, it is recommended to hire a project manager to control the teams, as GDPR can for some companies become a large task.
- **Review what data your suppliers hold**; it is crucial to know what data the company hold as well as data passed on to a supplier. Document the sensitivity of the data, volume, security as well as how long the supplier will keep it. Confirm that the suppliers are protecting the data correctly - it is still the company that is responsible for the personal data, even if the supplier are the ones that are processing the data.
- **Audit your suppliers** to confirm the suppliers are storing and processing the data in a secure manner. Alternatively, the supplier can be asked to do a questionnaire that records their compliance to ensure it follows the company's standards. The authors of the book made a questionnaire for companies to use and modify to support this process.
- **Create a data privacy governance structure**. The privacy practices of the company should be reviewed, and should follow the "*security-by-design*" and "*security-by-default*".
- **Review your right to process** and document the legal basis for processing data in the company. The right to process are divided in two categories: The right to process "normal data" and "special categories", where the data processed must be handled differently based on which category it is placed in.

- **Check your incident response plan** in order to tackle incidents quickly. Indecent response plans are effective as it informs employers of a company how to react to a potential targeted attack or natural disasters. Test the incident response plan by testing the team on realistic scenarios in a range of situations. Optionally, while updating an incident response plan, it can be beneficial to review a *Disaster Recovery* and *Business Continuity Plan*.
- **Transitioning to BAU**, in which the authors elaborate: "*Compliance needs to be integrated into day-to-day activities*". By doing this, the company ensures GDPR compliance maintenance. Employers should be aware of the cost of not being compliant. In this step, it is also recommended to let someone conduct DPIAs, as every data processing update should be checked for compliance within the DPIA.

The guide book does not mention if other companies have made use of this approach, and the guarantee of compliance and maintenance is therefore within their own experience only. However, all three authors are three different perspectives on how to be compliant with GDPR, and may not be biased, compared to approaches made by one person only. Their approach seem to be better, if a company applies BAU, which is mostly used by companies who require a lot of maintenance in general [44].

4.2 Complying with LGPD

When dealing with personal data of Brazilian citizens, an organization must oblige by the data protection laws, LGPD. Therefore, a few examples on how to implement LGPD are given to establish an overview of current solutions and frameworks.

One issue that arises for many companies is how to document the process of handling data according to IT professionals Castro, Silva & Canedo [64]. There are a variety of strategies and approaches towards solving this issue. A proposal on how to implement LGPD through a guide was by Vanzolini Foundation. Their guide consists of programs that has several controls defined as follows [64]:

Table 1: (Modified) Implementation of LGPD Guide by [64]

Program	**Controls**
1. Cybersecurity and Information Security Management System (CISMS)	1.1 Structuring of the CISMS 1.2 Implementation of the CISMS 1.3 Maintenance of the CISMS 1.4 Execution of the CISMS
2. Information Protection	2.1 Manage requirements 2.2 Information capture 2.3 Information evaluation 2.4 Information access 2.5 Information removal 2.6 Ethical treatment 2.7 Access to storage media 2.8 Security and privacy audit 2.9 Fulfilling requests 2.10 Incident reporting
3. Business Continuity	3.1 Data backup
4. Safe Attitudes	4.1 Training

This program guides Information and Communication Technologies (ICT) professionals who are managing and working with user data. The guide requires that people in this field are aware and up to date with the current legislations. Table 1 showcases the four programs and its corresponding controls in which

the intention are to cover the ten data processing principles of LGPD. The first program, The Cybersecurity and Information Security Management (CISMS) is working as the foundation of the entire program. The Information Protection program covers data storage, processing and how to collect data. Next, there is the Business Continuity program, where its purpose is to make sure that in case of data loss there will be recovery or have backup of the data. By performing data backup on a daily basis, recovery after any potential attack or risk will be helpful for the business to continue functioning. The last one, called Safe Attitudes makes sure that everyone involved with data handling are informed on what to do regarding issues with data leak or any other cyber related risks.

One approach on how to achieve compliance and implementation with LGPD is provided by [64] which is an implementation guide for LGPD as shown in Figure 2. This framework is a modified framework of the one showcased in Table 1. The additions are in the second program where the ISO 27001:2013 standard and the new program called *Improving Privacy* with the concept of Privacy-by-Design being a major part of it. In order to meet the CIA goals, it is beneficial with a ISO 27001:2013 certificate [64]. It is worth mentioning that this standard has been revised to the new standard ISO 27001:2022 during the writing of this thesis [61]. This standard is very similar to how LGPD manages access privileges. However, this ISO standard is not sufficient on its own and therefore the new program, that [64] proposes is Privacy-by-Design. The principles of Privacy-by-Design can be linked directly the articles with LGPD which can be seen in Table 2.

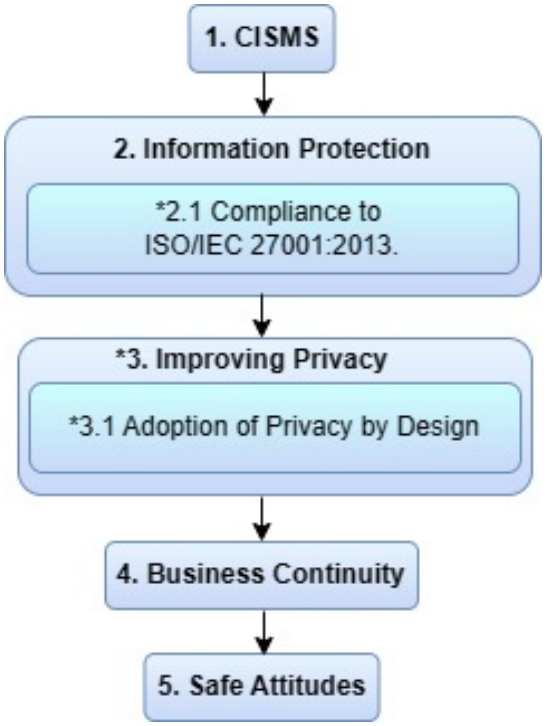

Figure 2: Framework for LGPD implementation[64]

Table 2: (Modified) Association of LGPD paragraphs and Privacy-by-Design principles by [64]

Principle	**LGPD**
Proactive not Reactive: Preventative not Remedial: Predict and prevent privacy incidents before they occur.	Art. 6. item VIII – prevention
Privacy as the Default: Privacy should always be the default setting in any system or even business practice, requiring no user interaction or configuration.	Art. 46. Processing agents shall adopt security, technical and administrative measures able to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing.
Privacy Embedded into Design: Privacy must be incorporated into the design and architecture of systems and business practices.	Art. 49. The systems used for processing personal data shall be structured in order to meet the security requirements, standards of good practices and governance, general principles provided in this Law and other regulatory rules.
Full Functionality - Positive-Sum, not Zero-Sum: Accommodate all the interests of the organization alongside privacy measures to allow the full functionality of the system while bringing benefits for all.	Direct relation not found since it is not in the interests of the law but of the organization.
End-to-End Security – Lifecycle Protection: Adoption of robust end-to-end security measures, protecting data collected throughout its lifecycle.	Art. 46. §2 The measures mentioned in the lead sentence of this article shall be complied with as from the conception phase of the product or service until its execution.
Visibility and Transparency: Documentation and availability of information on privacy policies and practices used by the organization.	Art. 6. item VI – transparency.
Respect for User Privacy: Keep the user's interests above all else by offering strong privacy settings; providing access to their personal information; and explicitly gather user consent before processing personal information.	Art. 6. item IV – free access, Art. 7. Processing of personal data shall only be carried out under the following circumstances: I – with the consent of the data subject.

By adding this new program, it improves the privacy protection by having the mindset throughout the entire process and the lifetime of the system/product. GDPR addresses data protection by design and by default in Article 25, however LGPD does not have it integrated [14][55].

This framework shown in Figure 2 has been evaluated by creating a survey for ICT professionals, where 57 responded. Based on the questionnaire, it was concluded that many companies are adapting to LGPD. However, not many of them are applying the ISO 27001 standard, making business continuity plans, training their employees or making a data protection impact assessment. Even though this framework would be a good approach towards ensuring data privacy in a company, it could be improved more. This has also been highlighted by the creators of this framework, that having some automated tools that could support this compliance with LGPD would be beneficial for the employees [64].

Another framework that helps implementation of LGPD from an IT point of view is proposed by [65]. It has been observed through other related works, that there companies or organizations who implement LGPD in their own way. Hence, there does not exist any standard or practical guidelines on how to actually do it through actions in an organization. There are studies that provides a more theoretical approach towards implementation of LGPD and others have focused more on the process to become complaint

but whereas they target SMEs. What this framework offers is considerations of all aspects, not only governance and privacy but also how to approach any data processing, development and infrastructure. *The LGPD Framework* is created by considering DevOps, Information Technology Infrastructure Library, Control Objectives for Information and Related Technologies (COBIT), ISO 27001, ISO 38500, ISO 20000 and some standards for Information Security Management Systems. The choice of selection for these frameworks were that implementing LGPD by these methodologies would fulfil the requirements of the law [65].

The framework is made in a way that it is flexible and open, meaning that it is allowed to add new content in it. The option of adding new properties does not make the framework lose its consistency and integrity. Furthermore, it adopts the principles and essence of the leading IT standards. As mentioned previously the framework is based amongst others on the COBIT and consists of six main principles [65]:

- Add value.
- Be componentizable.
- Be clear.
- Be versatile.
- Have dynamism.
- Reach the entire organization.

The framework is a conceptualized model and it helps interpret the law in a practical manner, meaning how to make decisions based on these in order to meet the requirements of LGPD. Integration of the requirements within an organization and at the same time providing practical guidelines by each component it comprises of. These components are the practical perspective and the framework consists of four domains [65]:

1. **LGPD Governance & People**
    - 1.1 Strategic Guidelines
    - 1.2 Roles and Responsibilities
    - 1.3 Culture & Communication
    - 1.4 Training & Awareness
2. **Methods & Processes**
    - 2.1 Policies and Standards
    - 2.2 Data Inventory
    - 2.3 Data Classification
    - 2.4 Data Risk Analysis
    - 2.5 Data Protection Architecture Model
    - 2.6 Prevention Model and Incident Response
    - 2.7 Indicators & Monitoring
    - 2.8 Audits and Sanctions
3. **Data Controls**
    - 3.1 Data in Use
    - 3.2 Data in Motion
    - 3.3 Data at Rest
    - 3.4 Data Loss and Remediation

4. **Infrastructure Architecture**

The reason for having this framework based on the practices of DevOps is that it relates to LGPD. Seen from a technical point of view, these practices ensures data protection with its security standards and privacy during the entire process of the software development [65]. The purpose is to incorporate the DevOps methodology in the framework because it makes adaption to new regulations easier as to check whether compliance with the law is there or not, can be difficult due to new changes and therefore more hard to identify them.

Figure 3: The LGPD Framework with four domains [65].

As it can be seen in Figure 3 above with the four dimensions of this framework, it provides an overview of data protection according to the regulations. The first domain, *LGPD Governance and People*, is about guidelines, roles, responsibilities and training. The second domain, *Methods & Processes* revolves around the laws. *Data Controls* handles all personal data or if the data can be assessed as personal data. Also, it is about data insertion, use, storage, saving and deletion at the same time considering what state these data are in. The last category is *Infrastructure Architecture* which covers the physical aspect such as security, reliability, modularity and so on [65]. This framework can be directly linked with the articles from the LGPD laws. Each of these four domains are based on other well known frameworks, standards and laws as it shows in Figure 3.

Each of these dimension contains a number of components that are useful for LGPD compliance. As it was mentioned, the first domain with LGPD Governance and People, one must determine all the roles, responsibilities and others by LGPD. At the same time, all the established frameworks and standards used this information to find the requirements for the governance. Next, the Methods and Processes domain ensured that all the necessary terms and definitions are covered in LGPD. Incident responses, audits, monitoring, and data protection architecture are done here too. Data Controls is about the lifecycle of data and its states. The last one covers the IT infrastructure such has the network, servers, data centers and applications and adapts it to the law.

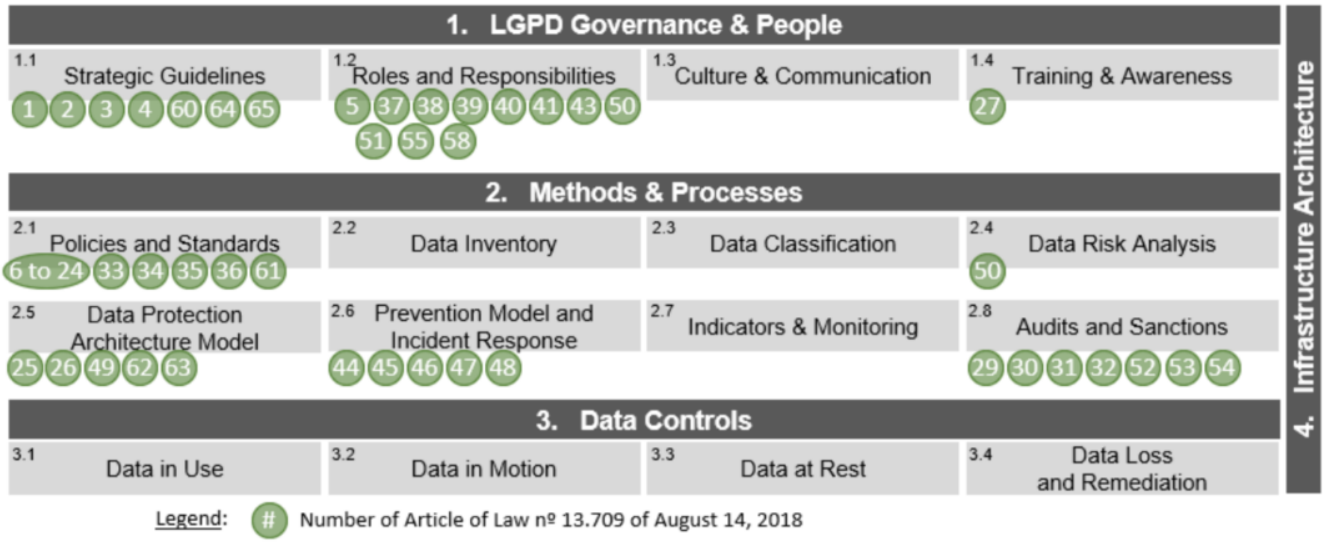

Figure 4: The LGPD Framework and linkage to the laws in GDPR by [65]

4.3 Complying with CCPA

As mentioned, the GDPR was enforced within the countries of EU and LGPD was enforced in Brazil, however in the US, each state has their own laws and regulations, which applies for data protection laws as well. The CCPA is similar to GDPR, with slightly different conditions that makes CCPA considered less strict than GDPR [66]. As implied in the name, the CCPA applies to data subjects in California, which is according to the CCPA defined as Californian *consumers*. The consumers have a list of rights and the businesses are required to comply with the requirements provided in CCPA whenever collecting personal data, which is better known as *personal information* in this context [67]. Compared to GDPR, the consumers do have many of the same rights and principles, including *the right to be informed*, *the right to be deleted*, etc. The differences are shown in, for instance, *the right to opt-in*; data subjects under the GDPR are usually consenting to processing of personal data, whereas consumers under the CCPA can have their information processed and sold without consent. Only children, at the age of 16 years old and below, has the right to opt-in, though done by a parent or guardian if the consumer is below 13 years old [67]. If a Californian consumer would not consent to having their personal information sold, they must make a request to a business in order to opt-out. The business must therefore explicitly communicate to their consumers how they are able to opt-out, since they did not have the option to opt-in [67][68].

Another right that appears differently from the Californian law is the *Right not to be subject to discrimination*, also known as *The right to not be discriminated against* [67][68]. GDPR does not have an equivalent right, though CCPA has a list of categories where businesses cannot discriminate a consumer. For instance selling of goods; a business must not change the price, level or quality of goods. Besides, a business cannot deny goods to a consumer, based on discrimination.

Even though the CCPA has rights such as *The right to not be discriminated against* which is not covered in the GDPR, the California Law seem to learn from the requirements mentioned in the GDPR, and uses some of the terms to enforce new laws with improved data protection. With CCPA's enforcement in 2020, it is the current valid law as of writing this report, however the California Privacy Rights Act (CPRA) wwill be enforced July 2023 and will work as an addendum to the CCPA [67][69]. The new requirements that have been introduced with CPRA are three of the data processing principles within GDPR: Data minimization, purpose limitation and storage limitation [69]. The Californian laws are thereby closer to the GDPR now that the CPRA will be enforced, and having similar requirements internationally might also make it easier to transfer data across borders.

CCPA Being the first data protection law in the US that was in effect the 1st of January 2020, multiple

states are gradually implementing their own data protection laws as well. Virginia's data protection law's effective date was the 1st of January 2023, with more to come within the same year; Colorado and Connecticut's data protection laws' are effective from 1st of July 2023, and Utah's data protection law's effective date is from 31st of December 2023 [70]. With data protection being more widespread in the US, more states will implement more data protection laws. However, based on the European standards, the laws within the US is not sufficiently to keep the personal data protected [66].

If Europeans are applying any services from the US, they might require transferring their personal data to the US, which has been a concern for Europeans for years. Concerns have been caused as it has been revealed that the US government might have access to personal data, including Europeans' personal data through international services [66]. Before GDPR's effective date, EU and the US decided to implement the *Safe Harbor Agreement* or *Safe Harbor Framework* in 2000 which should protect data that is transferred internationally. This was in 2015 invalidated by the European Court of Justice (ECJ), known as the *Schrems I* case, which became relevant when Max Schrems along with ECJ requested an investigation on the data transfers from Facebook's headquarters in EU to the US after Edward Snowden revealed how the US government secretly applied surveillance programs [71][72]. Without an agreement to secure data between EU and the US, the trading business and economy was endangered, until the EU-US Privacy Shield was introduced in 2016. The EU-US privacy shield was invalided by the ECJ in 2020, which is known as the *Schrems II* case. ECJ raised the concern that when data has been successfully and securely transferred to the US, there was no laws within the US that ensured the data was as protected when processed, as required in EU [71]. As the Safe Harbor Agreement and EU-US Privacy Shield both being invalidated, trading internationally was relied on SCCs and TIAs. It was then announced in 2022 a political agreement on a new Trans-Atlantic Data Privacy (TADP) Framework was to replace the EU-US Privacy Shield. This time, measures has to be reconsidered to manage EU concerns about US surveillance practices. Joe Biden, the president of the US, has signed the Executive Order on the matter, and the European Commission's court are still, as of writing this report, working on translating this arrangement into law [72]. Max Schrems' opinion on the new agreement is to reconsider the framework, as he expect another invalidation immediately, as he is 90 percent sure to win if another case, *Schrems III*, should be necessary [73]. If the TADP Framework is enforced, it will require data to be protected by the enforcement date, however the US has data of Europeans from 20 years back, that remains unprotected. Schrems suggests a global agreement should define to which extend surveillance is allowed, and even if multiple laws has transparency as a fundamental data processing law, he still acknowledges this agreement is not feasible in the current time [73].

4.4 Consequences of Noncompliance with Data Protection Laws

Many companies have shown that by not protecting personal data, a data leak can result in consequences for both the company and its users. It can be costly for companies, including receiving fines and getting a bad reputation [74][75][76][77]. As GDPR was enforced in 2018, many companies throughout Europe had to change their structure and protection of personal data, to start complying with the new data protection law. The scenarios listed below are examples from an article by Beckett [74] that was written as a warning before GDPR was enforced, which highlights the results of data protection being ignored:

- A spy tool developed by CIA recorded conversations through televisions in peoples' homes. In addition, the information that was obtained was not protected which got leaked.
- Users of the online dating service Ashley Madison were revealed in a leak, resulting in users being publicly shamed online, as users' affairs were exposed.
- Emails and memos were leaked from the Trump Administration, resulting in "*embarrassment on a daily basis*", people internationally following their every mistake.
- An employee saved their personal iTunes library on a shared drive within the company. Little did he know that the company's IT department was backing up, duplicating, replicating and copying the

shared drive to a tier one storage system. This situation cost the company thousands of pounds.

The scenarios mentioned above, each received huge fines as a consequence. Every single of them were not compliant with GDPR in different ways; some did not categorize user data as personal or sensitive data, meaning storing and protection of data has not been prioritized. Beckett mention how some examples of companies distributed their data to multiple hosts and servers, whereas footprints were left behind. When companies ran out of storage, they simply bought more storage and kept stacking up "*often useless data*". Most of the data appearing in the mentioned leaks above were old data, that should have been deleted, since it was no longer in use. Article 5 of GDPR, *the Principles relating to processing of personal data*, should have been considered, especially the *Purpose limitation* and *Storage limitation* principles, ensuring better protection of sensitive data and removal of unused personal data [41][74]. However, this is only a case specifically focused on GDPR compliance, as LGPD would not require unused data to be removed, with the exception of a user requesting their data to be removed [14]. Beckett's advice is to comply with GDPR. Even if data can give companies "*power and deep insight*" as he explains it, "*it can also come back to bite you*" as companies risk fines for not complying. However, the companies will not have "*power*" over data as they used to, since GDPR and LGPD allows individuals to have stronger rights over their data. With GDPR and LGPD, users can for instance choose if their data should be deleted instead of processed [74].

It was revealed that Ashley Madison's parent company Avid Life Media (ALM) offered users to have a "*permanent deletion*" of their profile, whereas the user is charged $19. In 2014 when the hacker group The Impact Team hacked Ashley Madison, it was revealed that ALM was netting a total of $1.7 million in revenue for this service [75]. However, the leak revealed that the data ALM promised to delete was recoverable, including credit card information, names and addresses. The motivation of this hack was to shut down Ashley Madison, as they threaten to publish all the sensitive data they found of users and employers: "*Shutting down AM and EM will cost you, but non-compliance will cost you more*" [74][75]. And the reason for shutting the website down was that the Impact Team wanted to show that it was a mistake to charge users and lie about ALM's promise of permanently deleting user accounts from their system. After 30 days, The Impact Team posted "*Time's up!*" along with 60 gigabytes of Ashley Madison user data, given that ALM did not shut down the site [76]. Among this data dump, tens of millions of hashed passwords were discovered, and about 4000 of them cracked within five days. The passwords were hashed using the `bcrypt` algorithm, and by utilizing the tool Hashcat, weak passwords were revealed by comparing the hashes with commonly used passwords in the `rockyou.txt` wordlist. The algorithm by itself can therefore be cracked and does not guarantee confidentiality of user passwords, resulting in discovering some of the top used weak passwords on the Ashley Madison website, such as "*123456*", "*password*" and "*qwerty*" [78][79]. In August of 2015, ALM payed $11.2 million to make a settlement, on behalf of the 37 million users included in the data breach [80].

Lessons learned from the Ashley Madison case comes down to the technical security, in which GDPR's *Integrity and confidentiality* principle from Article 5 [41] as well as LGPD's *Security* principle from Article 6 [42] would require the system to apply appropriate mechanisms and utilize algorithms that ensures confidentiality. The data storage must also be improved, as Beckett highlighted in his warning for companies that are noncompliant [74]. Unnecessary and unused data must be removed, according to the data protection laws, especially if the user requests that their data must be erased [49][81]. With the Ashley Madison case, it is shown how the user should have the right to know what user data is stored and processed, showcasing the importance of the *Transparency* principle, which is another data processing principle mentioned in the aforementioned GDPR and LGPD articles. Furthermore, as the user has the right to know what data is processed, they also have the right to be forgotten. In Article 17 of GDPR, *Right to erasure ('right to be forgotten')*, and Article 16 of LGPD, *Deletion of Personal Data*, this right can be exercised *free of charge* [14][49][81].

Ashley Madison is a case that happened before the GDPR and LGPD existed, however, there are still issues with compliance years after their enforcement. An example of a more recent case is the Austrian medical news company, NetDoktor, which collected *unique online identifiers* along with IP addresses,

browser information and hardware information of all visitors, all transferred to the US as NetDoktor utilized Google Analytics. It was discovered that all visitors were assigned an identification number, and with a visitor connected to a Google account, it was possible to link this visitor to other saved data. Transferring Europeans' data to the US raised multiple complaints, one of the complaints stating data transfer using Google Analytics was violating Article 44 of GDPR, *General principle for transfers* [58][82][83]. Secondly, it was not known if the Europeans' data were as protected in the US, as required by law in Europe. Max Schrems raises his concern, as he encourage the US' legislator to utilize better protection, as he mentions "*In the long run we either need proper protections in the US, or we will end up with separate products for the US and the EU*" [82]. It was later announced by the Dutch data protection authority that "*The use of Google Analytics may soon no longer be permitted*", and as of writing this report, Google Analytics is still considered as noncompliant with the GDPR and banned in multiple European countries [77][83].

4.5 Summary

Based on the SOTA, we learned how compliance is achieved, and noncompliance is prevented. All of the mentioned laws are relevant to understand that each law has their own requirements and strategies depending on the scope and context in order to protect data. Specifically for our case with Educado, we need GDPR and LGPD in order to be compliant, which are very similar. With these laws, processing of personal data can be done in many different ways, where we discovered some approaches in the academic field. Learning from these approaches, we learn how other have successfully complied with GDPR and LGPD, which is our goal as well.

The different approaches used to be GDPR compliant that we discovered in Section 4.1 are compared to assess which one is best fit for this project. The parameters are based on the focus of the different material, such as target group to know which type of company is best fit for the approach. The experience of approach are compared, to see if the approaches are applied and tested within companies in EU, and that they provide GDPR compliance as they state. Tools are mentioned as they are recommended for better maintenance. The structure is compared as well, to highlight how a company's structure would fit the approaches. Lastly, who is the one(s) responsible of applying the approach onto the company.

The two different approaches are in some ways similar, based on Table 3. Method 1 is mostly targeted SMEs that collects the whole team in order to create a structure of data use, where each member are part of a step-by-step process in order to comply with GDPR. As part of the process, the company must also conduct a DPIA, and a privacy notice (documented as personal data policy in the paper), which is required by GDPR.

Method 2 on the other hand did not include privacy notice as part of the process, meaning more steps are required for this approach to be fully compliant with GDPR. Method 2 is more of a checklist that recommends following as many of their points as possible, in no specific order. The whole team does not need to be involved in the approach, as a separate project manager can do the job. Their point of transitioning to BAU is where all employees of a company can be included, as the GDPR compliance can be included in the company's day-to-day activities to ensure maintenance.

Table 3: Comparison of GDPR Compliance

Focus	Method 1	Method 2
Target	SMEs.	General companies, Companies applying BAU.
Experience	Approach is made by one person, tested on three SMEs.	Testing of approach is not documented, however, approach is based on methods used by three different authors who each had 30+ years of experience in IT and Technology.
Use of tools	DPIA and Personal data policy.	BAU, DPIA and "GDPR Tools": Microsoft, SNOW, Nymity, Totalprogramme.
Structure	Step-by-step approach, with three steps.	A list of recommendations, with eight points to consider.
Responsibility	Everyone in the organization.	A project team, or a project manager.

Both approaches can be used at the same time, making it one joint method to achieve compliance. The step-by-step approach from Method 1 can be used, along side the optional list of recommendations from Method 2. The responsibility could rely on a project manager, though with input from everyone in the organization. All the mentioned tools can be applied, including the DPIA, privacy notice, and the GDPR tools mentioned from Method 2. Combining these approaches may be a challenge, though hopefully ensure compliance.

GDPR compliance is not enough for Educado, however, as the data subjects are located in Brazil, Educado must also be compliant with LGPD. As we discovered in Section 4.2, approaches for LGPD compliance appeared differently than the approaches for complying with GDPR. To compare our findings of GDPR and LGPD compliance, we apply the same parameter of Table 3 to Table 4 with the two different LGPD approaches.

Table 4: Comparison of LGPD Compliance

Focus	Method 1	Method 2
Target	Brazilian ICT professionals.	Everyone in the organization.
Experience	This method was tested on 53 ICT professionals in the field.	Not documented.
Use of tools	ISO 27001:2013, Privacy by Design.	COBIT, ITIL, DevOps, ISO 38500, ISO 27001, ISO 20000.
Structure	A guideline of five steps.	A guideline consisting of four dimensions.
Responsibility	ICT professionals.	Everyone in the organization.

As it can be seen in Table 4, there are major differences between the two methods. Method 1 is targeted ICT professionals whereas Method 2 is targeted towards the entire organization. This is important, as with Method 2, everyone in the organization has a role to play and that is why *Training and Awareness* is an important factor within this framework. Since, not everyone is tech savvy, there must be clear roles and responsibilities and all should have a good grasp of protecting any data within the company. Whereas, with the first method, it is only the ICT practitioners who are responsible for the data handling, privacy and security. This parameter is similar to the GDPR compliance, where it seems like compliance can be achieved no matter if one person or the whole team is involved in the process. As long if that one person is a professional, an expert within the field.

Furthermore, the Method 1 has been tested out through a questionnaire to the right audience, by 53

professionals which gives this approach a good evaluation. Contrary, the Method 2 has been documented or mentioned whether any evaluation or validation has been performed and therefore it makes it more difficult to picture if this would work in a real life scenario. One parameter that both approaches share is the ISO 27001 standard. This standard is an important part of both methods, as it is a major international standard and the certificates obtained from this ensure more protection of data and credibility.

Considering both GDPR and LGPD compliance, it seems that professionals should be responsible for compliance, where the rest of the organization is included to evaluate all team members' input. The approach can be structured by a pre-defined guide, with support from list of recommendations. Though DPIA, ISO 27001, and other tools must be included to gain compliance successfully, as these are recurring within multiple approaches.

5 Case Study: Educado

As mentioned in Section 2.1, we chose to apply case studies as a method to apply our knowledge on data protection and compliance in a specific and realistic case. To do that, we need to understand Educado, as we have not worked on the project until our academic journey to Brazil, which is further elaborated in Section 5.1. Educado is owned by SomethingNew and was introduced to us by the co-founders. The current status of the Educado ecosystem consist of a web application for content creators, where new courses are created and a mobile application for waste pickers where courses are shown as presented in Section 5.2.

The technologies that are used in Educado can be categorized in *Data Storage* where MongoDB and AWS are the selected and applied technologies, *Data Transfer* using NodeJS and *Data Exchange* using OAuth. Each technology mentioned is further elaborated in Section 5.3. Exploring these technologies are useful for understanding how the data is shared among systems, and interpret how privacy implementations can be integrated in the ecosystem.

This section is an attempt to study the needs within Educado to recommend best practices and achieve compliance with both the GDPR and the LGPD. The LGPD will therefore be compared to the GDPR to understand the similarities and differences in Section 5.4.

5.1 Global Students SDG Challenge

The Global Students SDG Challenge's goal is to develop sustainable solutions and products by allowing students from different countries collaborate to find sustainable solutions. Specifically students of engineering and computer science have been participating in the project since 2018, including AAU and UnB [10][12][84].

Multiple projects started by the Global Students SDG Challenge are still in progress, including *River Plastic Waste Recovery*, *IoT in Selective Collection*, and *Mobile Financial Education* [10]. The latter is Educado, and it is an ongoing project where multiple project groups contributed by either working on the infrastructure, features or design. We started on this project to focus on the privacy of users in the app, as no privacy has been considered in the previous projects of Educado [12][13][84]. We started out by travelling to Brasília, Brazil to participate in the 7th Global Student SDG Challenge, where Educado was one of the projects in focus. Along with students of UnB we established a cross-disciplinary team to study privacy and cyber security objectives of Educado. Throughout the challenge we researched on the Brazilian data protection law, LGPD, and discussed with the students how it differs from GDPR. Furthermore, we visited a recycling complex founded by one of UnB's professors, which can be seen in Figure 5. This is where we learned about the issues of waste picking, and how the poor Brazilians worked illegally in unsafe, hazardous environments. The recycling complex was a solution to establish official jobs for waste pickers, and ensure a more stable but low-paid job situation.

As seen in Figure 6, the recycling complex is filled with huge piles of waste to manage, and in Figure 7 that the employees at the recycling complex are hard-working. This is where Educado comes in, to potentially help these people to make the transition to a more better paid jobs with good conditions. Waste pickers collected garbage that was more valuable and earned money that way. However, since waste picking has become illegal, the waste pickers then work in the recycling complexes and earn four times less.

Figure 5: Recycling Complex in Brasília.

Figure 6: Working environment in the recycling complex.

Figure 7: Employees working in the recycling complex.

One of the employees at the recycling complex agreed to do an interview, where we introduced Educado and asked if data protection and security would be an important factor when utilizing such app. It was revealed that the Brazilian data protection law is not commonly known among some Brazilians, however the employee expressed that privacy in general was important to him. Figure 8 showcases the interview we conducted, with us, Brazilian students, and the waste picker.

Figure 8: Interview at the recycling complex.

Finally, we presented our findings at the Global Students SDG Challenge event along with the other students who each worked on their own projects [85]. As our journey ended, we planned to keep in touch, in order to be able to ask our Brazilian contacts for advice on legal documents. This was indeed the case, as we hoped to have Brazilian feedback to confirm our LGPD understanding, which is further elaborated in Section 7.4.

5.2 Current State of Educado's Functionality

The current status of the Educado ecosystem as of February 2023, consist of a mobile application for waste pickers and a web application for content creators. These were last updated in 2021, dated back when the co-founders started this project as their bachelor thesis [12]. Many of the features that were originally considered are not implemented in the current system.

The current web app, has the option of creating new courses, where these courses have sections, and sections have components [12]. The web app is usable, but only usable for the administrators, as those who access the system are pre-defined and whitelisted in the system. If a user is authorized to create a course, they enter the home page as seen in Figure 9.

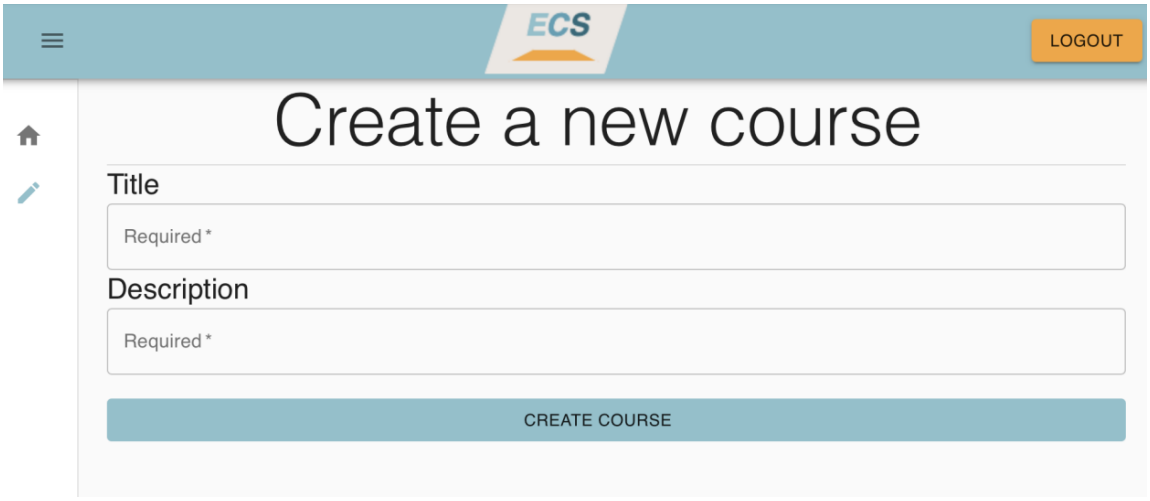

Figure 9: Homepage of Educado web app [12].

The objective is that the professors are responsible of creating courses, and add any number of sections in that course, along with any number of self-selected components. The components are text, images, videos or sound files uploaded by the professor. These components are stored in the file storage, and Figure 10 showcases how the components are displayed in the system if the files are uploaded successfully.

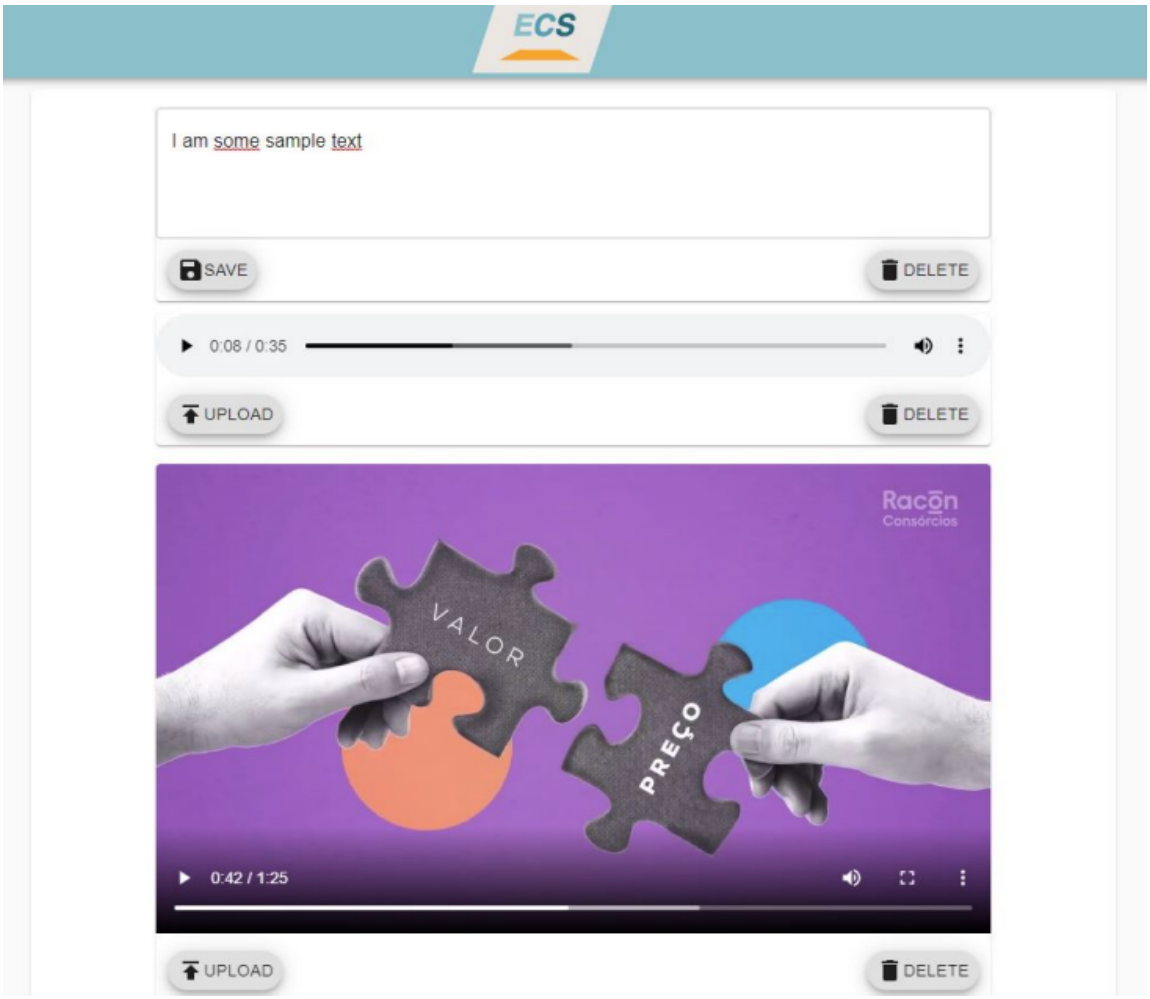

Figure 10: Uploading components for a course [12].

When a course is created on the web app, this course can then be seen in the mobile app. The mobile app is simple, but multiple projects have worked on how the design should be [12][84]. A course will be shown in the mobile app, where all sections within that course must be completed in order to successfully finalize that course. However, finishing the course does not result in any certifications for now, as that feature is not yet implemented.

The web app is almost fully developed, while in contrast the mobile app is not functioning as of writing this report. Figure 11 is the only illustration of the app for now, as there are no documentations of a newer version of the mobile app [12].

Visualized in Figure 11a, is a sketch of the home page, where each item has a clear indication of categories using icons. The reasoning for applying these icons is to represent the context without the use of written language, making it understandable without reading. Figure 11b showcases a specified course, where the finance icon is occupying a large space on the screen. It is noticeable that the course material is written in Brazilian Portuguese, as the waste pickers most likely cannot understand English.

(a) Home page in Mobile app. (b) Showcasing a course.

Figure 11: (Modified) Mobile App Screenshot [12].

5.3 Technologies

This section covers the technical measures of the Educado Ecosystem in order to create an overview of the communication between both data storage, APIs and apps.

Figure 12 is a diagram taken from SomethingNew's report from 2021, which gives an overview of the individual microservices, that allows different parts of the system to be created separately and apply different technologies without having issues when communicating with each other [12][86]. Each component is further elaborated in this section. Section 5.3.1 further explains the flow of the data that runs between the system using HTTP, where the data flow is based on whether the user utilizes the mobile or web app.

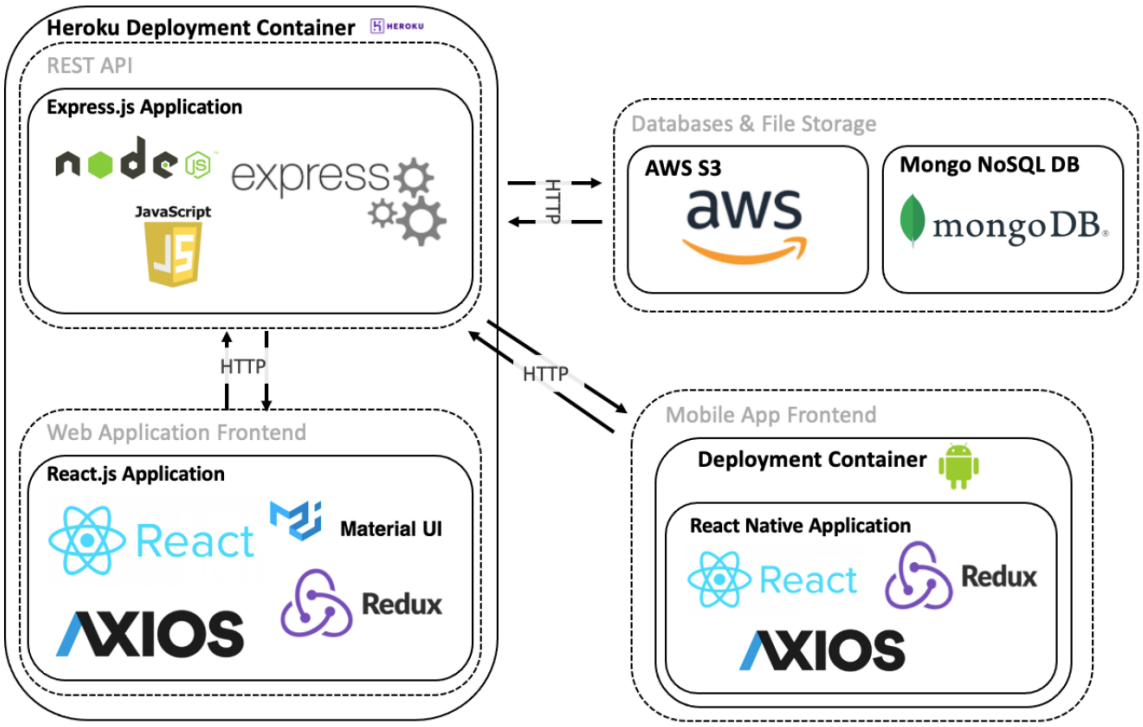

Figure 12: Architecture drawn by SomethingNew [12]

5.3.1 Data Flow

Figure 13 showcases the communication of Educado as developed by SomethingNew [12]. The figure starting from the bottom left corner illustrates how the flow moves throughout the system, beginning with a user interacting on either web or mobile app as a client. Communication consists of HTTP requests and responses between the components, where any user interaction is sent to the API using HTTP requests. As the API processes the received data, the database may be involved based on which request types are utilized. With completion of processing, the HTTP response is sent back to the user's client. If needed to re-render the client's interface, the user may have to update their client in order to visibly see the changes they made [12].

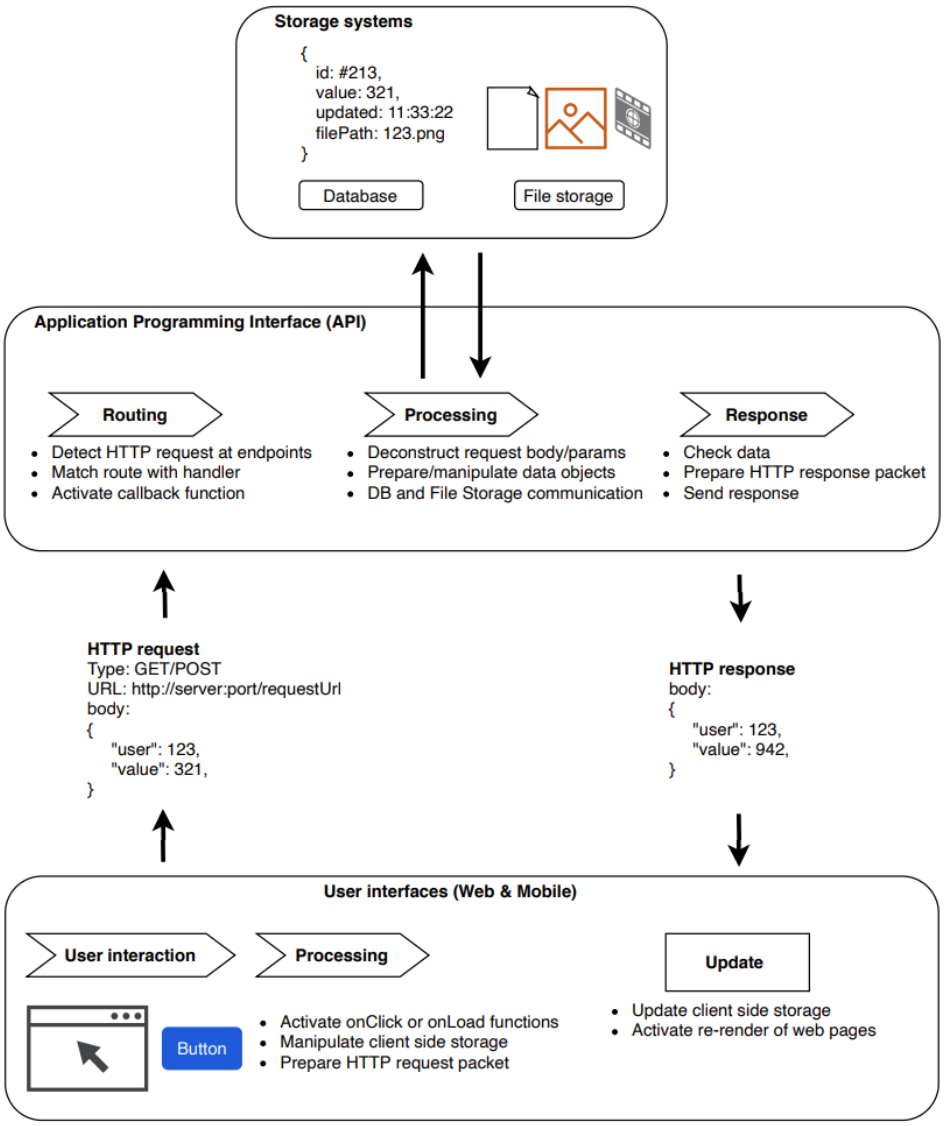

Figure 13: (Modified) Interface Model by SomethingNew [12]

5.3.2 Data Storage

There exists many data storage services where it is possible to retain the data on-premise or using cloud storage options. There are many aspects of data storage that are important to consider such as reliable data transfer, fast and efficient processing and file sharing. A systematic and organized way of storing data is by using a database and then it is possible to manage and access the information. Databases differ in the way they are built, some can be categorized as relational and others non-relational. In the former, the data is saved in tables consisting of columns and rows [87]. With relational database, the Structured Query Language (SQL) is applied whereas non-relational database with the Not Only SQL (NoSQL) the data is stored as JavaScript Object Notation (JSON) documents instead of in tabular form. Both have its advantages and disadvantages, when processing a large amount of data relational database management systems are suitable than the alternatives [88].

MongoDB is an open-source database and ranked as the 5th most popular Database Management System[89][90]. It is a cross-platform, document-oriented database known to be of NoSQL type. As explained above, NoSQL is a way to store and retrieve data from a database by not using tabular relations as seen in a relational database. MongoDB saves data in in JSON format-looking documents where it has dynamic schemas instead of fixed tables, using the query language SQL. Data are stored in documents and

organized in collections where each document can have different values and fields. These collections can be queried.

Educado uses MongoDB as the database containing the logic. The emails of the users are being stored inside the MongoDB user database where it is also here that Google authentication is being checked. The course are being saved in the database as well.

AWS is a cloud computing platform and IT Infrastructure founded in 2006 [91]. AWS is a subsidiary company of *Amazon.com, Inc.* based in Seattle, Washington. Their services can be divided into seven main categories such as 1) *Compute*, 2) *Storage*, 3) *Database*, 4) *Networking & Content Delivery*, 5) *Analytics*, 6) *Machine Learning* and 7) *Security, Identity, & Compliance* [92]. These services are available for all, private persons, companies or governments on a pay-as-you-go basis [93]. Users can access a large variety of services on the same platform without having to manage any infrastructure. The wide range of services makes this company the leading cloud infrastructure provider in the market by offering computer power, storage options, networking and database which is designed to make web-scale computing easier for their customers[94]. The users can scale up or down the services according to their needs and requirements quickly and without the hurdle of setting up and managing complex systems. Therefore, the AWS users can spin up machines, without the required configuration for their applications, in minutes.

AWS offers virtual servers named Elastic Compute Cloud (*EC2*), object storing called Simple Storage Service (*S3*) and database hosting with Relational Database Service (*RDS*) [95]. With EC2, the user can have multiple instances to spin up so they can run their systems (websites, applications, etc.). S3 provides the users access to their data through objects in which storing and retrieving data can be accomplished from anywhere on the web. The way storing works with S3 is that data is stored as objects and consists of object data and its metadata. Each of these object contain metadata, a key, value and version ID. These objects are being saved and organized into buckets (folders/directories) which can be any type of file (videos, images, text files) where they get their own unique identifier. This unique identifier is also called the key of the object or the name of the object within its bucket. The data within the object is the value. The version ID helps differentiate between all the versions of the object inside a bucket. Metadata is just additional information such as last modified date or size of the object. It is possible to create as many buckets as needed for different purposes. The moment the object is saved in S3 it is accessible from anywhere in the world with an internet connection [91][95][96].

5.3.3 Data Transfer

When working with any kind of data, they need to be transferred from one point to another. In other words, we are talking about moving data between devices/locations in which the objective is to get data flowing through either some channels, bandwidth or protocols. This transfer can either be done once (file upload) or as an ongoing process (streaming of media). There are some criteria to be met when transferring data and these are accuracy, timeliness and jitters. The data that is being transferred can be represented in a variety of ways: as text, numbers, images, audio or video. There can be several approaches to data transfer and different technologies and methods can be applied depending on the situation and context of the data, the transmission medium, infrastructure, performance and security factors, with many more [97].

NodeJS is an open source, server-side developer tool that makes it possible to write JavaScript code for a web application. In other words, it helps building network applications. It is also platform independent and asynchronous capabilities and is well suited for network requests, database handling/accessing and it is rather event-driven. The NodeJS libraries have been applied for the backend of Educado when working with HTTP REST API framework. As NodeJS has its strengths for microservices, Educado has used this lightweight approach to implement the backend [98][12].

5.3.4 Data Exchange

In contrast to data transfer, date exchange is a broader concept. Besides the transferring, a focus brought on the collaboration between the entities as well. This means that factors such as synchronization, in-

tegration, standards and protocols are being considered. There exists many technologies that facilitates data exchange, among others, the most well-known are XML, JSON and RESTful APIs. Educado applies REST API and React for the frontend where both are in JavaScript. Educado uses the framework NodeJS as described above to manage the authentication by implementing Google OAuth. With integration of Express.js REST API, authentication is managed with Google OAuth. Express.js is a web application framework within NodeJS and for the Educado backend, there is the package called "passport" which is necessary for the Google OAuth strategy [12].

5.3.5 Our Idea of Improving Educado

As shown in Figure 14 below, we made a diagram to showcase how we would improve the architecture compared to the original Educado architecture diagram. It can be observed that the security is missing in web protocol HTTP in Figure 12. Therefore, in order to make this data exchange and communication secure, we highly recommend to add this layer of security by applying HTTPS as communication protocol. The components that make up the entire ecosystem is still remaining the same such as the file storage, database and interfaces. The only difference is the addition of HTTPS between each entity.

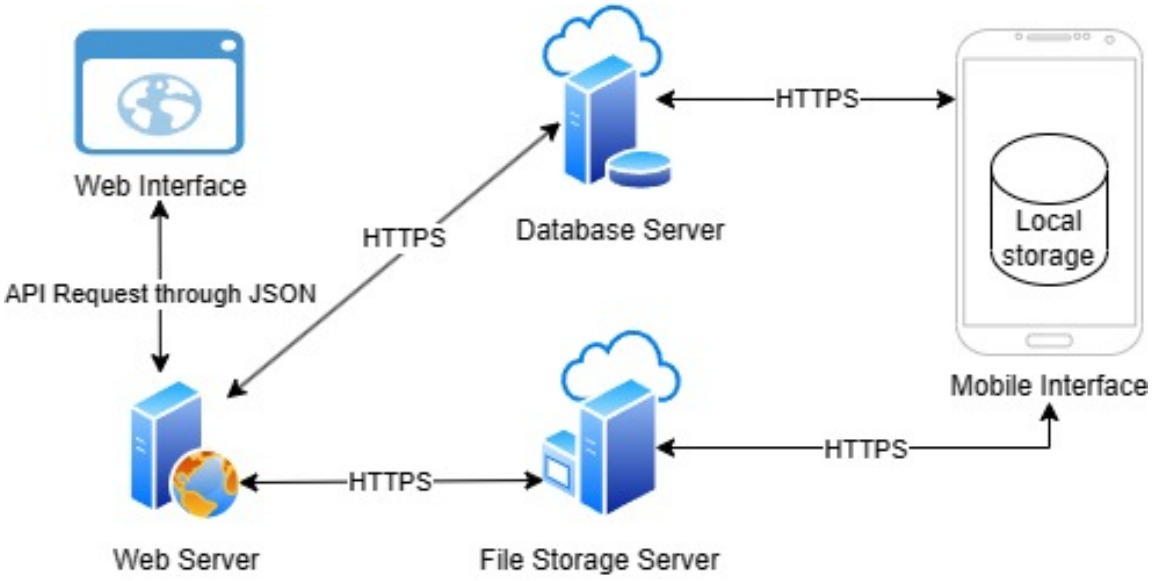

Figure 14: Architecture diagram of Educado Ecosystem

5.4 Data Protection Law in Brazil: LGPD

The Brazilian federal law, LGPD is comprised of 65 articles that is a comprehensive data protection regulations and is very similar to the European GDPR. This compilation of documents describes how to manage and handle personal data. The LGPD was enforced in August 2021, and Autoridade Nacional de Proteção de Dados (ANPD) is the National Data Protection Authority of Brazil who are responsible for evaluating if companies and organizations are being compliant [14].

It is mandatory by law, that Brazilian companies comply with LGPD, and failure to comply with these can result in heavy fines and legal consequences [14]. The compliance are being implemented by applying various measures such as ensuring that data collection consent is obtained, assigning a data protection officer, implement security mechanisms to protect personal data, making sure that access to personal data are available when requested, report of data breach(es) to the authorities and all affected individuals. Therefore, LGPD, as GDPR, is holding Brazilian companies accountable in such a way that they must protect personal data and collect/process the information responsibly [14][42][99].

5.4.1 Principles of LGPD

The core fundamentals of this law is protection of personal data, where as Article 6, *Principles That Govern Processing Activities*, can be used for properly processing personal data [42]. This protection means anything related to processing of data that includes all types of operation with it. These operations could be, how the personal data is collected, stored, distributed, deleted, transferred and many more. Furthermore, the law specifies the rights of the data subjects, where it is clarified which rights the data subjects have, where the most important are their rights to know the specific purpose of processing and its duration of processing activity [14][99]. Similarly to GDPR compliance, all principles of data protection must be applied whenever personal data is processed. Each principle are mentioned in Article 6 and listed below [42][100]:

1. *Purpose*: The collection and processing of personal data must be justified, legally and specifically as to what the purpose is. Further usage or processing that are not compatible with its purpose is not allowed.
2. *Adequacy*: The processing of personal data must be according to the purpose that was given to the user.
3. *Need*: There should only be collected an amount of data that is necessary in such way that it matches the purpose.
4. *Free access*: The data subject should be able to access their personal data and its form or duration without paying anything for it. This works as an assurance for the data holders.
5. *Data quality*: A guarantee for the holder that the data is of good quality.
6. *Transparency*: The data and how it is processed, compatible with the purpose, is given to the users.
7. *Security*: This ensures that the personal data is being kept secure and protected from unauthorized access. Furthermore, its data integrity is kept intact.
8. *Prevention*: The personal data is not being transferred or shared between others who are not allowed to process it.
9. *Non-discrimination*: The processing of data cannot be done for any other purposes that involves illegal and discriminatory intentions.
10. *Responsibility and accountability*: Proving compliance with LGPD, and the effectiveness of the applied measures.

5.4.2 Data Subject Rights

Similarly to the GDPR, the data subjects has a list of rights that are guarantees for protection of users in a service. Some of them are similar to the data subject rights mentioned in GDPR, however each right is not as thoroughly defined in the law as the GDPR. Article 18 mentions the data subject has the right to [101][102]:

1. *Confirmation of the existence of processing*: The data subject should know if and how their personal data is handled.
2. *Access own personal data*: The data subject can access their personal data by request, allowing them to know what data is held within a service.
3. *Correction of incomplete, inaccurate, or outdated data*: The data subject can update or correct inaccurate data.
4. *Anonymization, blocking, or deleting data*: Personal data categorized as unnecessary or non-compliant can be anonymized or deleted if requested by the data subject.

5. *Data portability*: The data subject can request that their personal data is forwarded to a third party.

6. *Erasure of data (the right to be forgotten)*: The data subject can request their personal data to be erased, free of charge. The data controller must respond as soon as they can, to assess if erasure of data is possible. Exceptions are listed in Article 16 [81].

7. *Information about data sharing with other companies*: The data subject shall know which stakeholders and third parties the data controller has shared their personal data with.

8. *Information about the possibility of not providing data*: If the data subject does not wish to provide personal data, then they shall be aware of the consequences.

9. *Withdraw consent*: The data subject is allowed to revoke their consent at any time. Their personal data cannot be processed when consent has been withdrawn.

5.4.3 Transfer of Personal Data

Based on Article 33: "*Cases of Permission for the International Transfer of Personal Data*" transfer of personal data outside of Brazil is allowed in nine cases, where our case includes transfers to EU, a country that must be compliant with GDPR. This falls under the first case in Article 33, where transfer of personal data outside of Brazil is allowed "*for countries or international organizations that provide a degree of protection of personal data appropriate to the provisions of this Law*" [103]. With GDPR and LGPD having similar degrees of protection of personal data, it is expected that the criteria are met.

Compared to transfer of personal data in the GDPR, no TIA is required according to LGPD. As mentioned in Section 4.3, EU did not trust that personal data would be securely transferred out of EU, which is why they require documentation to ensure compliance can be achieved. With Educado transferring data between EU and Brazil, a TIA must then be applied.

5.4.4 DPIA

In the LGPD, the DPIA mentioned has similarities to the GDPR, however after further research it is discovered that in Brazil, the DPIA is also known as a *Relatório de Impacto à Proteção de Dados Pessoais* (RIPD) [104][105].

In LGPD, it is not mandatory to perform a RIPD, however, if ANPD requests for one then it must be delivered [14]. In addition, upon the request from ANPD, further documentations might be demanded as well [14][104]. Companies who are processing sensitive personal data such as anything related to ethnicity, race, religious/political views, sexual orientation or biometric data are obligated to make a DPIA [14].

The RIPD contains guidelines and explanations such as recommendations, preparations and law references for every category listed in the assessment. One of the first points to be emphasized in the RIPD is the fact that they let it up to the data controller to determine whether there are any risks that violates the principle of responsibility and accountability as stated in page 9 of 27, *"It should be noted that, for the purpose of preparing the RIPD, these criteria should not be considered exhaustive, so that the controller can verify the existence of high risk in situations other than those indicated. Thus, in accordance with the principle of responsibility and accountability, it is up to the controller to assess the relevant circumstances of the specific case, in order to identify the risks involved and the appropriate prevention and security measures, considering the possible impacts on freedoms and fundamental rights holders and the probability of their occurrence"* [105]. It is important to note that the statement mentioned is not in its native language, Brazilian Portuguese, but an auto-generated translation to English made by Google.

In order to explain the similarities and differences between DPIA and RIPD, a comparison table has been made in Table 5. Here it shows, that in most parts they are covering most aspects accordingly with a few exceptions. In overall, the third row with "Identify the need for the a DPIA" and its equivalent in RIPD, "Need to prepare the report" and "Description of the treatment", we can see that there are

some subtleties in RIPD that are required to answer. This is under the section "3. Description of the treatment" called "3.3 Treatment context" in the RIPD. Here, it is asked of the data controller to provide any information related to experience with personal data prior to this RIPD.

Another angle that is missing in the European DPIA which is in the RIPD, is "Consulted Stakeholders". This section is about identifying and documenting all parties that have been seeking advice at, which could be anyone from information security specialists, management or legal advisors. This correspondence and consulting must be recorded as it is a communication outside of SomethingNew.

Table 5: Actions in DPIA and RIPD

	DPIA	**RIPD**	**Accordance**
1	DPIA Team	Identification of treatment agents and person in charge	✓
2	Information	Identification of treatment agents and person in charge	✓
3	Identify the need for a DPIA	Need to prepare the report + Description of the treatment	✓
4	Describe the data flows	Consulted stakeholders	✗
5	Assess the activity against the key Data Protection Principles	Need and Proportionality	✓
6	Privacy Risks	Risk Identification and Assessment + Measures to Deal with Risks	✓
7	Evaluation	N/A	✗
8	Integrate	N/A	✗
9	Approval	Approval	✓

5.4.5 Privacy Notice

Based on the LGPD, conducting a privacy notice is not a requirement, however the data subjects has a list of rights and must have freely access to be informed on the data processing within a service [99][106]. Presenting these information can be displayed in any forms, as long it "*is available to the data subject in a clear, adequate and ostensive manner*" [14].

The information that must be included according to Article 9 is as listed below: [14][99][106]:

1. The *purpose* of processing data.
2. The *duration* in which the data will be processed.
3. *Contact details* of the data controller.
4. Information regarding *shared use* of personal data.
5. Which *responsibilities* the agents have, as they carry out the processing.
6. An explanation of rights defined within the LGPD, along with how to *exercise the user rights*.

As these information are similar to the privacy notice in the GDPR, it makes sense to structure it as a privacy notice.

5.4.6 Comparison and Similarities of GDPR and LGPD

As the relevant parts to our case study of the GDPR and the LGPD has been studied, Educado can then be evaluated on which parameters must be considered to achieve compliance. The differences between the laws have already been mentioned throughout this section, where Table 6 summarizes the laws' most important parts for Educado.

Table 6: Comparing selected topics of GDPR and LGPD.

	GDPR	**LGPD**
Demography	Europeans [14]	Brazilians [14]
Processing Data Principles	Article 5: "*Principles relating to processing of personal data*", listing 7 principles [41]: 1. *Lawfulness, fairness and transparency.* 2. *Purpose limitation.* 3. *Data minimisation.* 4. *Accuracy.* 5. *Storage limitation.* 6. *Integrity and confidentiality.* 7. *Accountability.*	Article 6: "*Principles That Govern Processing Activities*", listing 10 principles [42][100]: 1. *Purpose.* 2. *Adequacy.* 3. *Need.* 4. *Free access.* 5. *Data quality.* 6. *Transparency.* 7. *Security.* 8. *Prevention.* 9. *Non-discrimination.* 10. *Responsibility and accountability.*
Data subject rights	Chapter 3 includes a list of articles defining the data subject rights [46][47][48][49][50][51][52][53]: 1. *Right to be informed.* 2. *The right of access.* 3. *The right of rectification.* 4. *The right to erasure.* 5. *The right restrict processing.* 6. *The right to data portability.* 7. *The right to object.* 8. *Rights in relation to automated decision making and profiling.*	Article 18 defines the data subjects right to [101]: 1. *Confirmation of the existence of processing.* 2. *Access own personal data.* 3. *Correction of incomplete, inaccurate, or outdated data.* 4. *Anonymization, blocking, or deleting data.* 5. *Data portability.* 6. *Erasure of data (the right to be forgotten).* 7. *Information about data sharing with other companies.* 8. *Information about the possibility of not providing data.* 9. *Withdraw consent.*
Transfer of personal data	Article 44: "*General principle for transfers*", allows transfer within EEA. TIA must be conducted if personal data is transferred outside EEA, to assess and mitigate risks [58].	Article 33: "*Cases of Permission for the International Transfer of Personal Data*", a list of cases define if international transfer is allowed, TIAs are not applied for international transfers [103].

DPIA	Article 35: "*Data protection impact assessment*". Required if personal data that can be related to the data subject is processed [28].	Article 38: "*DPIA or Data Protection Impact Report*", also known as RIPD. May be required to draw up a report if asked by the National Authority [104].
Privacy Notice	A mandatory document targeted data subjects used to specify how Article 5: *Processing Data Principles* is compliant [41][44]. Must include a list of points stated in Article 13: *Information to be provided where personal data are collected from the data subject* [46][44].	A document used to specify how Article 6: *Principles That Govern Processing Activities* is compliant [42][106]. Specifically privacy notices are not required, however some sort of clear representation must include a list of points stated in Article 9: *Personal Data Subject's Right of Access* [14][99].

As seen in Table 6, the laws have a lot of similarities, with minor differences. For instance, both of their processing data principles essentially cover the same topics, where biggest difference at glance is the data minimization and storage limitation principles in the GDPR that are missing in the LGPD. Without these principles, LGPD does not restrict services, allowing them to store old, unused data, unless the data subject requests it to be removed. We personally experienced and observed these first-hand in Brazil, that more data than necessary was collected, compared to European standards, when utilizing a service, which we further elaborate in Section 7.6.

The data subject rights of the two data protection laws look different, however many points are essentially the same, and allows that the data subject are more in control of how their personal data is processed.

International transfers both require that appropriate data protection is in place before transfer is allowed. For the GDPR, this includes conducting a TIA if that country is outside EEA, meaning a TIA must be conducted to allow transfers from Denmark to Brazil.

Another assessment to conduct is the DPIA, as it is required according to the GDPR. In Brazil, it is not required to conduct an RIPD, unless it is requested by ANPD. A DPIA should be conducted in our case, as it is required by GDPR, which regarding LGPD can then be delivered to ANPD if requested.

Privacy notice will also be needed, as the GDPR utilizes this as the approach to inform users about their user rights and the processes of personal data within a service. This is suitable in the case of LGPD, as it is required to showcase the aforementioned information for the data subjects, and a privacy notice is categorized as an accepted approach.

6 Privacy and Data Protection in Educado

As the current state of Educado has been evaluated in Section 5, we know which features are already implemented, and which features we need to add to the system. Currently, only emails are collected that will be categorized as personal data. Based on the GDPR definitions in Section 3.2 and LGPD definitions in Section 5.4, we know the system must follow a plethora of requirements. To meet these requirements before conducting impact assessments will prevent some potential privacy risks, since we are already aware they may cause an issue in the system as we learned from our research of noncompliance in Section 4.4:

- Companies must be transparent about how and why they process personal data. If preferred, the data subject can at any point request what data a company has stored about them, and how it is processed [41][42].
- We learned that user consent must be implemented in Educado, as consent must be given before processing personal data, Furthermore, if the data subject wish to withdraw their consent, they should be allowed to at all times. Data subjects has the right to be forgotten, meaning they can disallow their data to be processed, or simply removed [49][81].
- Personal data in the system should be stored if it has a purpose, and only for a necessary period of time. The data is thereby minimized, the storage and purpose will then be limited. Unused data should be removed from the system [41][42].
- The confidentiality, integrity, and security in general must be ensured by applying appropriate technical measures, to ensure, for instance, personal data is not readable for unauthorized users. This may include cryptography, hashing, anonymization, monitoring, etc. [41][42].

Understanding the use for Educado, we also made some decisions, in which Educado should implement to realize a usable product for their users, and to achieve compliance.

- The personal data collected by Educado are: Email, full name and age (group).
- The personal data will be encrypted using AES-256 as the encryption algorithm for the data in rest and HTTPS/TLS is used as encryption method for data in transit where the RSA algorithm is used with it.
- Transferring of data will be monitored 24/7, a staff member will assess potential threats that appears based on the monitoring.
- The PETs applied in the app are Differential Privacy, for anonymization of user activity and statistics, and Federated learning for applying personalized measures in the mobile app without transferring personal data to SomethingNew.
- SomethingNew will implement role-based access control, and the staff will only have limited access to personal data, or none at all if it is not necessary.
- The data subject will regularly insert a (self-chosen) verification PIN to confirm their data is up to date and they are still utilizing the service.
- If the data subject does not perform the verification step, they will have their personal data removed from the system after 3 years of inactivity.

Currently, we have not implemented these features in the app and these assessment impacts are usually conducted on systems to assess their current state. Functionalities that was part of the initial idea, such as generation of certificates, are assumed to be implemented in the future, and thereby included in the assessments. These implementation of features and functionalities are further discussed in Section 7.5. The DPIA, TIA and Privacy Notice are documented in the following sections.

6.1 DPIA

This DPIA template has been obtained through University College London [24]. It must be noted that this DPIA is a sample, and we have filled in all the necessary and relevant sections for our case study, Educado Ecosystem on behalf of SomethingNew.

When the template was conducted, a guideline was followed as well to understand what was required in each category of the template. As mentioned in Section 2 prior to carry out a DPIA it was necessary to perform a screener to check whether it was required to conduct the DPIA or not, in which we found out was required of us as we process personal data.

The entire DPIA has been filled out with the exception of the section "Privacy Risks" in which the last column requiring "Deadline for implementing solution" has been removed from Table 10. This is removed because we do not have information on the future plans of SomethingNew, and their plans of handing over the Educado Ecosystem to others as discussed in Section 7.5.

Two more sections which have been left out in our DPIA is "Integration" and "Approval". These are expected to be handled by lawyers and DPOs, which has not been feasible for our project. As mentioned in Section 7.5, it was planned to request a Brazilian lawyer for an approval.

DPIA Team

The DPIA team is defined in Table 7, to evaluate who is responsible for conducting the DPIA.

Table 7: DPIA Team

Information Owner	SomethingNew I/S
Job Title	Co-Founder
Email	contact@somethingnew.dk

Information

With the ones responsible for the conducting the DPIA defined in Table 7, Table 8 is used to define the category of the service and its stakeholders.

Table 8: Information

Activity name	Educado
Department / entity	Educational System
Parties involved	SomethingNew I/S, Aalborg University, University of Brasília

Identify the need for a DPIA

Conducting the DPIA screener confirmed that the processing of personal data in Educado must be considered and assessed using a DPIA. The need for a DPIA is identified through the following points.

Purpose/aims of the activity

The purpose of Educado is to function as an educational platform for the Brazilian waste pickers/natural persons in which they will have easy access to the mobile application. This application requires connection to the Internet, as new content and course material will be made available. The users must sign up with their email for the app to function. The more the user is completing courses, the more information (certifications) is being gathered and stored from that specific user.

Why was the need for a DPIA identified? Explain the role of personal data in the activity

As personal data is being collected such as an email from the user, confirmation that the user is of legal age, full name, course activities, SomethingNew is obligated by law to be in compliance with the data protection laws. No sensitive data is being collected or used, however personal data is required for the usage of the system. The personal data is used to improve functionality of the app, as well as verification and user authentication. Whenever a user receives a certificate, it has to be associated with an identifiable user to confirm they completed a course in the app. Contact information is thereby used to authenticate users, where identifiable information is used to assign certificates.

Describe the data flows

The diagram on Figure 15 is made with the expectation that the users already created an account and is logged into the system as either a web user or a mobile user. The processing steps of the data flow diagrams are further elaborated:

- **1.0**: The web user gets all the courses created by that specific user displayed which are handled by HTTPS GET requests being processed in the backend. The user then gets access rights by CRUD operations. These operations are handled by HTTPS POST requests to the file storage, depending on whether content is being uploaded/downloaded. The file storage sends information back based on creation/deletion of the course and the user gets updated their user interface and can see the new changes made.
- **2.0**: The user can access the content on the mobile application. A course or courses can be selected in the app by making HTTPS GET requests to the file storage, in which the requested material is being made. The file storage sends the course material back to the user and the user can download the content (video, sound, text, images) down to their local device.
- **3.0**: As the mobile user has courses downloaded on their device, they can then select and start a course. The progress of the course is stored locally on the mobile device, meaning when a user selects a course, Educado will check the local storage to see if the user has any records stored from previous use before entering a course. The user makes new progress and completes courses in that course, their progress will be stored on their local device, within their specific choice of physical storage. The user can access the progress offline at any point in time, until the course is completed as there are no more courses to do. The device is thereby updated whenever a course is completed.
- **4.0**: When the mobile user has completed their course, the certificate can then be downloaded from the app. The app needs the user's information as well as their completed progress of a course in order to autogenerate a certificate, which is done in processing step 5.0. The database authorizes the user by receiving the user's identifiable information through HTTPS GET requests, and confirms the identity of the user with a HTTPS response to ensure the user did complete the course and is eligible to receive the certificate. The database fetches user data from generation of certificates in 5.0 and checks if a specific user has completed the course and sees if there is a match.
- **5.0**: The certificate will be generated by first authorizing the user with processing step 4.0 to then fetch information about the certificate through the file storage. In file storage the details will be collected, assembled and returned. This is further used to connect the certificate data to the specific user and forwarded to the database. Then, the user and the certificate are linked and the certificate is granted by being displayed on the app screen.

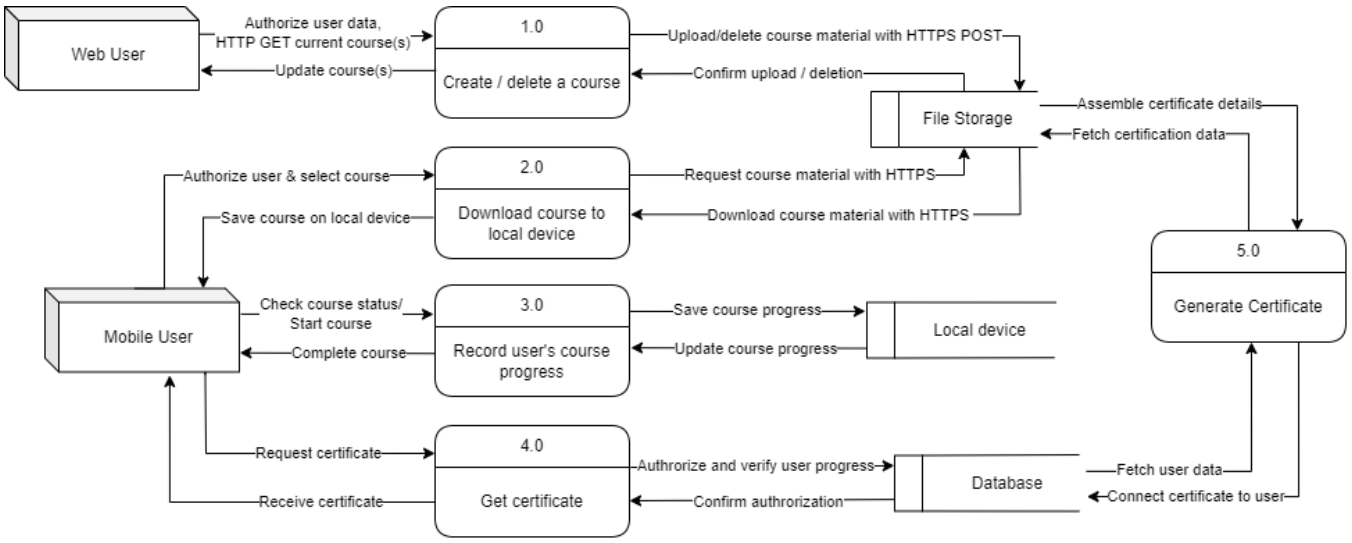

Figure 15: Data Flow Diagram of Educado.

Assess the activity against the key Data Protection Principles

The data processing principles of GDPR are applied to assess if all principles are covered in Educado.

Lawfulness, fairness and transparency

The data collected are identifiable information such as **full name**, **email**, along with data revealing personal data such as **age group(s)**.

The data is obtained via user registration, whereas the data is obtained directly from the user themselves. The information that is provided for the user about the processing is found in a privacy notice, which is a separate document, see Section 6.3.

Purpose limitation

The personal data collected is used to manage the user's course progress and certificates for the mobile app users, whereas the web app users personal data is used to highlight the creators of courses. The names are displayed in certificates in the mobile app and the course responsible name(s) on a selected course is shown too. The age group is confirming the users of the app are above 18 years old, and furthermore, the emails are used to contact the users and authenticate their accounts.

The users will be able to access the Privacy Notice within the mobile application. In this, the purpose of the collection of personal data will be detailed as to why we need the age group and contact information.

We will ensure that the data are not processed for any other purposes than we have claimed in the Privacy Notice. The data will be kept within a secure and safe storage service and there is no intention of using the data for marketing or sharing with third parties. As the purpose of Educado is to give a platform for education for waste pickers, there is no financial gain.

Data minimization

It is necessary for Educado to collect the personal data, including name, email and age, in order to run the functionalities in the app as intended. Without the email, the users cannot be authenticated in the system. The names are identifiable and associated with the assigned certificate, without the names, the certificate would not verify and confirm the user has personally completed the courses. The waste pickers

who work at the cooperative recycling centers are above 18 years old, which must be confirmed in the system, meaning the age is not necessary, however confirming the user is above the legal age is necessary.

The processing of personal data is proportional to the purposes of the data as only necessary data is being gathered to make the mobile application functional.

The steps we are taking to ensure that we collect as little personal data as possible for the purpose of Educado is by reviewing the amount and type of data we are gathering regularly and make sure that we do not collect unnecessary data. And at the same time make periodic checks on whether the data is still relevant for the purpose of the app to function fully. Furthermore, we will not collect data that we might think will be useful later on and justify every collection.

Accuracy

New software will not deviate or affect the data, however data will stay up to date and keep its accuracy in the system.

The personal data collected will be verified by the user, where the accuracy of data is ensured as the user is authenticated. If the authentication is confirmed through e.g. a Google account, then Google is considered a reliable source which handles data accurately. The user shall have the possibility to edit and update their personal data (for instance by legal name change) to keep the data accurate. To confirm the accuracy of the data, the user is prompted to verify their personal data e.g. a PIN selected by the user will be prompted which is being used for verification once every three months. This verification also provides evidence that they are still actively using the app.

Storage Limitation

The personal data should only be kept while the user is actively using the app. We would keep the data as long as the user wants to use the app or until they request for deletion, and in case of inactivity for three years, their data will be deleted by the system.

PETs are applied by implementing differential privacy on the user data, which ensures the users are anonymized and not identifiable when managing user activity. Furthermore, federated learning will be implemented to collect user data locally while ensuring the data is not identifiable in the ecosystem.

Rights of individuals

Educado allows data to be added, edited, and deleted, if requested by a data subject. If the data subject asks for restriction on the processing of their data, it will be provided by Educado, and the data subject will receive a confirmation notification as a response to their request.

Withdrawal of consent must be as easily accessible as giving consent to the processing of personal data in Educado. The decision making in the system (for instance deciding if a user is eligible to request a certificate) is solely on the basis of processing by automatic means, without any human factor involved.

Educado is not a marketing project, it is a non-profit initiative made for educational purposes. The data subject's personal information is thereby not used for targeted advertising and data subjects will not experience any type of advertising in general.

Integrity and confidentiality (security)

Technical measures that will be used within Educado are:

- Encryption
  - Data encryption in transit/at rest for database and file storage.
  - Creating role based access controls for the database.
  - Encryption keys.

- Logical Access Control
  - The access control is set whenever the users are registered in the system, the roles of users cannot be modified, and each user has a specified set of limited privileges.
- Monitoring
  - The S3 Bucket requires monitoring to be in place. By monitoring the system and traffic, the communication is audited.
- Anonymization
  - PETs ensures user data activity cannot be traced and linked to specific users. The PETs used are differential privacy and federated learning.
- Integrity checks
  - User's Gmails and Google tokens must be compared in order to check the email is legit and authenticated in the system. Amazon S3 uses checksum, meaning the data is verified and thereby used for integrity check, by comparing the data to corresponding hash values in the database.
- Backups
  - AWS Backup ensure automatic backup in a centralized system.
  - Regular backups ensure the data is not lost within courses, analytics and user activity.
  - Courses have offline backup to ensure the user's progress can be saved whenever Wi-Fi is not available.
- Malware detection
  - The monitoring is able to audit and detect if the data is suspicious. If anything suspicious appears, a staff of Educado will assess the risk.
- Secure communications
  - The monitoring is able to audit and detect if the communication has suspicious activity. Therefore, communication can be assessed and the team can act to ensure the communication is kept secure. Policies are adjusted to ensure the communication only accepts secure protocols (such as HTTPS), and thereby have encrypted communication.

Only the server is physical, which is provided by AWS and located in Germany. The server is not physically accessible by SomethingNew or other partners, as it is solely handled by AWS. If any risks were to affect servers, then it is risks regarding human interaction within AWS or natural physical measures relevant in Germany.

Educado will follow policies and rules provided in a privacy notice. The management regarding the project, incidents, staff, maintenance is handled by SomethingNew. Monitoring is used to provide audits and logs that can be used to support the management process. Furthermore, documentation and more security mechanisms will be handled by AWS.

International transfer

The data is processed in Denmark and the data subjects are located in Brazil, meaning the personal data collected from the users are transferred between Brazil and Denmark. Denmark is within the EU, however, Brazil is not part of the EU and has their own data protection laws to follow.

There will be a "Transfer Impact Assessment" (see Section 6.2) which is mandatory by European laws, and important for this case, as the data is transferred outside of the EU. Furthermore, a transfer agreement is required, in order for data transfer to be compliant with LGPD.

The security and transferring of personal data is protected by being compliant with data protection laws of Denmark and Brazil, including secure communications and storage. The considerations of international transfers are shown in Table 9.

Table 9: International Transfer

Consideration	**Answer**
Is the data being transferred outside the EEA?	Yes. The personal data is transferred between SomethingNew in Denmark (data processors) and users in Brazil (data subjects).
Will SCCs be put in place to cover the data transfer in questions?	Clause 14, a TIA, will be put in place to cover the data transfer in question.
Does the data transfer require a new contract?	In case of change in the system, a new TIA will be conducted to be kept up to date.
What awareness will the data subject have of the specific data transfer?	The data subject has access to the privacy notice at any time, in which awareness of transfer will be documented.
What benefits does the data subject get from the processing that involves the data transfer?	No benefits will be provided for the data subject involving the data transfer.
What personal data is included in the transfer?	The personal data included in the transfer are identifiable information such as Full name, Email. Along with Data revealing personal data such as Age group(s).
Is the processing/transfer in an area that has seen ICO enforcement?	The DPA associated with Denmark is Datatilsynet. This is where threats and issues are reported to, in case of data breach due to bad implementation or noncompliance. Datatilsynet would publicly share requirements, regarding the context of transferring personal data.
Does the processing / data transfer help adherence to other data protection requirements?	The data transfer does help adherence to other data protection requirements, such as data minimization and purpose limitation; only the necessary information is transferred between Denmark and Brazil.
Does the third party demonstrate a decent level of GDPR compliance?	Third parties such as UnB, located in Brazil must comply with LGPD, and by cooperating with SomethingNew and AAU they must also comply with GDPR.
Conclusion: Based on the above risk assessment, please explain why you believe any risks of international transfer have been mitigated for this research study.	The risks are mitigated by applying secure communication as well as transferring only the necessary limited amount of data. By following the respective data protection laws at the origin of data and destination of data countries, any risks are being assessed.

Local laws and regulations

Being compliant with LGPD in Brazil is not sufficient, as third parties should at least be compliant with the GDPR because the management is located in Denmark. Therefore, they must follow the stricter data protection requirements which are required by law within the EU. All communication must be protected using encryption mechanisms, and data must be accurate and up to date. The mobile users are prompted to verify their data is accurate by confirming a 4-digit PIN of their choice, which is required every three months. An audit of keeping logs of all activities, including data collected from third parties, and documenting it to keep track of any suspicious interaction or activities. An employee responsible for auditing will review the documentation regularly and act on the logging to ensure the suspicious activity is inspected and assessed.

Data Processors

SomethingNew are in contact with local lawyers and Brazilian student(s) who are working and studying about LGPD compliance. Their experience with LGPD can be used to evaluate and approve the DPIA in a legal sense, as their expertise and judgment are more reliable then the DPIA team's, since they consist of engineers only.

Privacy Risks

The privacy risks has been identified based on the data processing principles and international transfers. These risks are assessed in Table 10 below.

Table 10: Privacy Risks

	What is the privacy risk?	**How likely is the harm?**	**Solution/Action to be taken**	**Result**
Lawfulness, fairness and transparency	Low	Remote	The Privacy Notice is freely available, documenting how data is processed in the system.	Eliminated
Purpose limitation	Low	Possible	Only necessary (non-sensitive) data that contributes to the functionality of the app is collected.	Reduced
Data minimisation	Low	Possible	Only necessary (non-sensitive) data is collected, and will be deleted after a period of time being inactive.	Reduced
Accuracy	Low	Possible	User data is kept up to date by verifying with the user every three months that their data is still valid and accurate.	Reduced
Storage limitation	Low	Possible	If the user is inactive after three years, then their data is deleted from the system. Storage is managed by SomethingNew only.	Reduced
Rights of individuals	Low	Remote	The rights of individuals within GDPR and LGPD protects and ensures the privacy rights of all data subjects.	Eliminated
Confidentiality, integrity, availability	Medium	Possible	The user data is encrypted and security mechanisms are implemented to protect data (use of PET, hashing of passwords, etc).	Reduced

International transfer	Medium	Possible	Transfer of data is being handled by secure communications such as HTTPS and reliable APIs. The data transfer is being documented with its purpose and how it is being transferred through transatlantic borders. This is done by completing a TIA (See Section 6.2).	Reduced
Local laws and regulations	Medium	Possible	SomethingNew documents their rules that they follow according to GDPR, along with a set of rules and requirements that third parties must consider, when the data is transferred to Denmark.	Reduced
Data processors	Medium	Possible	Third parties and all involved stakeholders are being transparent and following rules and regulations that are being reviewed by local lawyers.	Reduced

Evaluation

Educado is a non-profit educational platform for waste pickers and in this case SomethingNew does not benefit by any financial means and the entire purpose of the Ecosystem is to help the transition of being a waste picker to employment. This means that individuals such as professors who are the content makers are necessary for both the mobile application and web application for achieving the goal of the project.

6.2 TIA

In order to determine whether a TIA is required or not, we had to evaluate the data protection laws and based on this we did draw the conclusion of carrying one since we are transferring data from Brazil to Europe, where the collected and transferred data is being processed in Denmark.

Hence, we have applied the TIA template provided by Health Service Executive [27]. One important modification that we have been making is that we replaced all the mentioning of "HSE" in the template with Data Exporter, since this is proper for our case study, SomethingNew.

Since SometingNew does not transfer data to and from a Brazilian stakeholder, we must keep in mind, that the TIA appears different than normal, as SomethingNew in this case appears as both the data importer and data exporter.

We deselected some parts of the original TIA template that we did not find fitting to our case study. For instance, in Table 16 the template required both the data protection laws to be documented with separated columns, which in our cases became a merged column. Since the data importer and data exporter is the same, and SomethingNew primarily follows the GDPR, we choose to merge those.

Overview of Data Transfer

To initiate the TIA, the definitions of roles and responsibilities are being defined as well as identification of the receiving country for the data transfer which can be seen in Table 11 and Table 12.

Table 11: Parties to the Data Transfer & TIA

Data Exporter:	SomethingNew
Status of the Data Exporter in relation to the data transfer:	Controller, Processor
Data Importer:	SomethingNew
Country of Data Importer:	Brazil
Status of the Data Importer in relation to the data transfer:	Controller, Processor
Nature of Data Importer's business/operations:	Private Sector Organisation
Starting date of the data transfer:	2nd of June 2023
How often will the TIA be reviewed? (next date of review to be specified and recorded for follow up purposes):	The TIA will be reviewed every three years, meaning the next TIA review will be on 2nd of June 2026.

Table 12: Receiving Jurisdiction / Third Country

What country is the personal data being transferred to/accessed from?:	The personal data is being transferred to Denmark from Brazil through Germany. However, we are sending data back to Brazil.
What GDPR Article 46 transfer mechanism is used to facilitate the data transfer to the Data Importer?:	The mechanism chosen are binding corporate rules.
Nature of Data Transfer:	Personal data is hosted by the data exporter within the EEA, the users can request access to their own personal data and get a copy of it.
Will the Data Importer be transferring the personal data onwards to another party/parties (e.g. sub-contractors, sub-processors, etc.)?:	No, there will not be transferred personal data to other parties.

Information on what, why, when, who and how data are being transferred must be specified in Table 13.

Table 13: Details of the Data Transfer

What is the context and purpose of the data transfer (e.g. IT support, storage, backup, research, analysis, marketing, compliance with legal obligation)?:	The purpose is functionality and usability of the app, as well as contact information to identify and/or update users on the Educado system without accessing the app. The user data is transferred to our database and file storage.
What processing activities will the Data Importer undertake on the personal data once it is transferred?:	The data is processed by categorizing the user's information to contact information and identifying information, anonymizing the identifying information using PETs. Comparing identifying information, whenever a certificate is requested.
What categories of personal data are transferred (e.g. HR data, financial data, survey data, training data, audit data etc.)?:	Identifying information, and data revealing personal data.
Will special categories of personal data be transferred?:	No.

Will personal data relating to criminal convictions and offences be transferred?:	No.
Who are the data subjects or classes of data subjects?:	Services users.
Will the personal data of children and/or vulnerable data subjects be transferred?:	No.
Have the data subjects been notified of the nature of the transfer (e.g. privacy statement, etc.)?:	Yes, the privacy notice is available for data subjects at any time, in which notifies the nature of the transfer.
What is the expected volume of personal data being transferred?:	Full name, email and age group is being transferred per user, the volume is therefore expected to be small.
What is the the data exporter's lawful basis for processing the personal data (by transferring it) under Article 6 of the GDPR?:	Consent of the data subject(s).

Table 14 describes which safeguards are being ensured for the data transfer together with the security measures.

Table 14: Existing safeguards in place

In what format will the personal data be transferred?:	Encrypted.
How will personal data be transferred to the Data Importer?:	Using secure protocols such as HTTPS, and traffic is monitored by Data Importer.
What security measures does the Data Importer have in place to mitigate any risks associated with data transfers to countries outside the EEA which are not covered by an European Commission 'adequacy decision':	Data encryption in transit, data encryption at rest, role based access, 24/7 access monitoring.

Next, in Table 15 the possible alternatives are identified, if any.

Table 15: Possible Alternatives

Can the data exporter's purposes be achieved without transferring the personal data to a country outside the EEA not covered by an European Commission 'adequacy decision (e.g. using a supplier based within the EEA or a country outside the EEA covered by an European Commission 'adequacy decision)?:	No.
Can the data exporter's purposes be achieved with the transfer of anonymised data to the Data Importer, in place of personal data?:	No.

The enforceability of appropriate safeguards

Here, in Table 16 the relevant data protection laws with their respective safeguards are provided together with how they would be enforced. Any associations or involvement with the relevant data protection laws in the origin of data collection to the destination of the data transfer are being described.

Table 16: Data protection law or practice in recipient third country.

Does the country have a dedicated data protection law?:	Yes.	Educado must follow Brazil's LGPD, as well as GDPR.
Is that data protection law based on any international instruments on privacy or data protection?:	Yes.	LGPD is based on GDPR.
Is the Data Importer subject to the data protection law(s) described above?:	Yes.	Educado is compliant with both LGPD and GDPR.
Do individuals have substantive data protection or privacy rights, e.g. right to access their personal data, right to remedy for breach of their rights?:	Yes.	LGPD and GDPR mentions transparency as a fundamental principle.
Are there any specific restrictions on the disclosure of personal data by the data importer to third parties?:	N/A	There are no transfers to third parties.
Is there a distinction under data protection or privacy law between citizens or residents and non-citizens or non-residents?:	No.	All residents in Brazil are protected by LGPD, and all residents in Europe are protected by GDPR
Is there an independent data protection regulator with powers of oversight and enforcement?:	Yes.	ANPD, the data protection authority in Brazil, and Datatilsynet, the data protection authority in Denmark.
Can individuals exercise their data protection rights through the judicial system or data protection regulator?:	Yes.	The data subject rights are defined in the Privacy Notice (Section 6.3) which is required by the GDPR.
Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties?:	Yes.	LGPD and GDPR might impose fines.
Is there a legal requirement that any restrictions to fundamental rights and freedoms be necessary and proportionate (e.g. that restrictions are for justified and limited in purpose such as for law enforcement, national security or safeguarding public health)?:	No.	There are no legal requirements that restricts the fundamental rights or freedom of the users.
Is there evidence that the law(s) identified above are applied in practice?:	Yes.	ANPD ensured LGPD was enforced in 2021, EU ensured GDPR was enforced in 2018.
Is the Data Importer aware of any applicable laws or practices (e.g. criminal law enforcement, national security intelligence and surveillance, regulatory compliance etc.) within the recipient third country that could constitute an obstacle to its ability to comply with appropriate safeguards (i.e. SCC's) pursuant to the GDPR? If so, please explain in the detail what these laws or practices are and how these could impact the Data Importer's ability to comply:	Yes.	The Data Importer are collaborating with Brazilians on having a mutual understanding of the local laws and all necessary regulations to be compliant with.
Do national intelligence or security services within the recipient third country, operate surveillance programmes?:	No.	It is not expected that national intelligence, etc. Are operating surveillance on the recipients.

Can public authorities (e.g. intelligence, law enforcement, defence services, regulatory agencies or other government agencies) within the recipient third country, access or compel disclosure of personal data from the Data Importer?:	No.	Public authorities can in Brazil access personal data without consent, however GDPR would not allow access of personal data for anyone that is not necessary for the purpose.
What limitations in law and/or practice are imposed on such requests by public authorities?:	Yes.	LGPD allows public authorities to request data, however GDPR limits the access for public authorities.
Is there evidence of surveillance authorities in the third country accessing large volumes of personal data?:	No.	There are no known cases of surveillance authorities in Brazil, and GDPR disapproves surveillance authorities.
Are surveillance operations / operators in the third country subject to audit or oversight for compliance?:	No.	No surveillance operations are shown in the LGPD, and surveillance operations are not allowed with GDPR.
Can individuals challenge, before a judicial or other independent tribunal, access to their personal data by public authorities, including for surveillance measures?:	No.	The public authorities will have to access the personal data from Educado to include surveillance. However, Educado will not share their data with anyone, as it is against the Purpose limitation principle.
Has the Data Importer ever been subject to a request (including by request, court order or other form of access) from public authorities within the recipient third country for access to EEA personal data? If so, how often and by whom?:	No.	Personal data can be requested, howbeit not accessed by public authorities.
Could the Data Importer be subject to a request from public authorities within the recipient third country, for access to data held within the EEA by the Data Importer?:	No.	GDPR would not allow access to data within EEA from outside.
Does the Data Importer have a documented public authority access policy? If so, provide a copy of the policy:	No.	The data importer will provide policies, though public authority access policy might not be included.
Does the Data Importer refuse access requests from public authorities within the recipient third country, unless the request is a mandatory compulsion order or where the Data Exporter has provided their written consent?:	Yes.	SomethingNew will not provide written consent for access to requests from public authorities.
Will the Data Importer notify the Data Exporter about any requests from Public authorities within the recipient third country for access to data which they received from the Data Exporter, unless legally prohibited to do so?:	Yes.	The data importer and data exporter are the same, information requested by public authorities in Brazil and Denmark is handled/granted by SomethingNew
Does the Data Importer publish any transparency reports that set out the number of access requests or demands for data disclosure it has received from public authorities?:	Yes.	Transparency is one of the data processing principles in both the LGPD and the GDPR

Is there evidence of other operators in the Data Importer's sector in the recipient third country receiving requests for access or disclosure from public authorities?:	No.	Requests from public authorities for access or disclosure are declined by SomethingNew

Table 18 below mentions if any supplementary safeguards has been taken into account.

Table 17: Supplementary measures to appropriate safeguards.

Taking account of the circumstances of the transfer detailed in Table 13 and the responses at Table 16, is the data exporter satisfied that the law or practice of the recipient third country will not impinge on the effectiveness of the safeguards provided by the SCCs, i.e. that the level of protection in the recipient third country is essentially equivalent to that guaranteed in the EU (by the GDPR read in light of the Charter of Fundamental Rights)?:	Yes, LGPD is based on GDPR and therefore has equivalent guarantee like EU.

This last category, Table 18, lists all the supplementary measures to safeguards and the relevant measures are being given as seen below.

Table 18: Supplementary measures to appropriate safeguards.

Pseudonymisation	No
Encryption:	Yes. The data is encrypted both before and after it is transferred. The data is encrypted at rest and in transit. The encryption algorithms and protocols used are HTTPS, AES-256. The encryption product used is AWS. SomethingNew manages the encryption keys and where are the encryption keys are stored.
Protected recipient(s):	Yes, both data subjects and stakeholders are protected using the technical measures mentioned.
Other technical measure(s):	PET: Differential Privacy, Federated Learning.
Further binding contractual clauses to the SCCs:	No, no supplementary measure is required.
Organisational measures:	No, no supplementary measure is required.

6.3 Privacy Notice

We made our privacy notice based on the template obtained from ICO [31], where we ended up applying everything that was in the original template.

The template is provided by an European service, meaning the structure of the privacy notice is targeted GDPR compliance. The data subjects being Brazilians, we compared the information needed for privacy notices in both the GDPR and the LGPD, to ensure our privacy notice is compliant with both. For instance, description about the responsibilities of the data controller is needed, based on the LGPD.

Furthermore, the privacy notice template only recommends providing one service under the "How to complain" part, where we choose to include both contact information on SomethingNew and ANPD.

Our contact details

Company name: SomethingNew I/S
Website: https://www.somethingnew.dk
Contact persons: Daniel Britze (Co-Founder) or Jacob Vejlin Jensen (Co-Founder)
Phone number: +45 28643117
Address: Falkoner Alle 56 C 3 th, 2000 Frederiksberg
Email address: *contact@somethingnew.dk* or *sysadmin@somethingnew.dk*

What type of information we have

We currently collect and process the following information:

- Personal identifiers and contacts (full name and email)
- Data revealing personal data (age group)

How we get the information and why we have it

The personal information we collect from your Educado registration is transferred to us directly. The reason for collecting the data is:

- We wish to contact you outside Educado, to verify and authenticate your account.
- We wish to identify you and confirm your certificate by inserting your full name in the certificate form.
- We wish to confirm you are of legal age.

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing this information is your consent. You are able to remove your consent at any time. You can do this by contacting SomethingNew I/S at contact@somethingnew.dk.

What we do with the information we have

We use the information that you have given us in order to personalise your experience, and keep track of your progress in courses, which can be finalised in a certificate with your full name highlighted on the certificate as documentation. The data that you will provide is being processed and transferred to the EU for storage and making sure that the functionalities or purpose of the data is realised.
We will not share any information with other organisations or individuals, meaning no data will be shared to other third parties. However, the data will be transferred between Denmark and Brazil for processing.

How we store your information

SomethingNew is responsible for processing your data, including collecting, transferring and deleting your personal data.
Your information is securely stored in our database located in Germany, which is hosted by Amazon Web Services and managed by SomethingNew.
We keep your personal data for three years, in case of inactivity. We will then permanently dispose of your information by deleting all user activity and progress associated with your account, as well as personal data provided by you in our database and storage.

Your data protection rights

Under data protection law, you have rights including:

- Your right of access - You have the right to ask us for copies of your personal information.
- Your right to rectification - You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
- Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.
- Your right to restriction of processing - You have the right to ask us to restrict the processing of your information in certain circumstances.
- Your right to object to processing - You have the right to object to the processing of your personal data in certain circumstances.
- Your right to data portability - You have the right to ask that we transfer the information you gave us to another organisation, or to you, in certain circumstances. You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us at contact@somethingnew.dk if you wish to make a request.

How to complain

If you wish to send a complaint regarding our processing of your data, you can contact the following:

SomethingNew I/S
Falkoner Alle 56 C 3 th, 2000 Frederiksberg
+45 28643117

Autoridade Nacional de Proteção de Dados (ANPD)
Setor Comercial Norte - SCN, Block 6, Conjunto "A", Edifício Venâncio 3000, Block "A", 9th floor, CEP 70.716-900 - Brasília – DF
+61 20258101

6.4 Guidelines for Implementing Data Protection

In order to be compliant with the data protection laws, it is important to understand the current requirements stated in the laws. Data protection laws mentions actions which must be taken into account to be compliant, which depending on location, can involve conducting a plethora of assessments and documentations.

For GDPR, we observed that a DPIA must be conducted whenever personal data is involved, whereas the LGPD only requires a DPIA (or Brazilian RIPD) if requested by ANPD. The DPIA can be used to highlight the management of personal data within a service, including data storage, data transfer, security measures, etc. Furthermore, the DPIA can identify privacy risks, and encourage services to mitigate potential impacts. Therefore, the DPIA is not only a requirement (within the GDPR), it is also a recommendation in which organizations should conduct to prevent privacy risks.

The data processing principles are evaluated, to ensure all aspects has been covered. Using GDPR as an example, the principles of data processing reduces misuse of personal data. With the principles of *purpose limitation*, *storage limitation* and *data minimization*, a service must keep their data collection of personal data to a minimum and only available when necessary, where these limitations must be defined by the data controller. The *transparency* and *accuracy* principles allows users to know what personal data of theirs is processed, and allows the user to remove, update and/or add personal data in a system, according to the user's preference. With the *integrity and confidentiality* principle, the security measures of an organization

must be defined to deduce which cryptography and hashing algorithms should be implemented, where a PET is recommended to include, to apply anonymization or pseudonymization of personal data.

The rights of the individuals must also be presented clearly towards the data subject. For instance within the GDPR, the users have a list of rights in which a service must be compliant with, as mentioned in Section 3.2 such as *The right of access*, *The right to be forgotten*, etc. An organization must follow the data protection law that is relevant for their service, to know what user rights must be ensured.

The potential privacy risks can then be assessed, as the principles are utilized and user rights are implemented in a service. Based on the chosen implementation, each privacy risk will appear as either low, medium or high risk, where high privacy risks are prioritised, and all must be mitigated. This part is where vulnerabilities appear, and the data controller must take action in order to mitigate high risks before the next DPIA is conducted.

International transfers are also introduced in the DPIA, which is to assess if international transfers (if any) are allowed. With third parties included, all stakeholders involved must follow data protection laws enforced at the location of the data subject. With an European data subject for instance, a service must be compliant with the GDPR.

The risks within international transfers are further evaluated in a TIA, which must be conducted if European data is transferred outside EEA (with some exceptions). The DPIA does introduce some of the data transfer risks that might occur, though not as detailed as the TIA. The additional factors in the TIA entail assessing how public authorities potentially affect a service, and if surveillance is a potential impact. Multiple data protection laws might affect the data transferring, depending on where third parties are located, and the TIA will highlight the differences between those laws. For instance if data from Europe is transferred to California, then both GDPR and CCPA must be compliant.

In order to let everyone within a company know how to process and transfer data, a privacy policy must be made. Not to be confused with a privacy notice, which is directed the data subjects. Both privacy policy and privacy notices are required to ensure everyone involved know how a company is compliant with GDPR, and how the data is handled. These documents should be freely available and accessible at any time, meaning data subject can always read the privacy notice, however the employees of the company are the only ones reading the privacy policies. Employees of a company is able to read the privacy notice as well, though it is targeted data subjects.

Data subjects will also encounter the *Terms & Conditions* when applying a system for the first time. This document should let the data subject know about the company's use of personal data, how it is stored, transferred, etc. to ensure transparency between the company and data subject. If the data subject does not wish to apply a service based on the conditions, they are welcome to reject the service. Companies are thereby obliged to ensure the product is for the data subject's best interest, in order to make them want to utilize the service. Though, the *Terms & Conditions* is also mandatory to create, in order to be compliant with specified laws, such as GDPR.

Other recommendations to consider is the standard ISO 27001 which is not directly linked to GDPR, however compliance is ensured if these frameworks and strategies are applied in the industry. Especially the ISO 27001 is a mandatory framework to follow, according to the Brazilian academia, as mentioned in Section 4.2.

Based on the analyzed frameworks, assessments and documentation that we see as best practices in general for any organization, we can now suggest these to be applied within a specific context. These guidelines, recommendations and best practices are highly encouraged to conduct in Educado, as SomethingNew must be compliant with the relevant data protection laws and regulations.

We concluded that there are many standards, procedures and important factors to consider when working with personal data, however, we observed that it is best fit to only carry out a DPIA, TIA and Privacy Notice at the current state of Educado.

Since Educado is an European owned company, it is obliged by law to carry out a DPIA, TIA and Privacy Notice. Educado are obtaining personal data from Brazilians in which these data are being collected, transferred to Europe and stored in European territory, Germany. Since data is being transferred

into Europe and outside of Europe, SomethingNew must document any processing of personal data. Even though, no sensitive data is collected, there are still personal data involved such as the name, age group and email addresses. As personal data are collected, processed and transferred, an assessment of potential risks must be documented. This documentation can be shown as demonstration of compliance with GDPR by SomethingNew.

Furthermore, SomethingNew as Data Controller must provide information on how they collect data, for which purposes, what rights the user have and what are being stored. The user must be given sufficient information on their rights to be deleted from the database or to complain if anything and therefore contact information must be inserted too. This privacy notice must be visible and implemented in Educado mobile app. This is very important to make as it is required by law. In addition, the privacy notice must be translated to Brazilian Portuguese so the users, Brazilian waste pickers, can read and understand the content. This will be discussed further in the Section 7.3.

By ensuring privacy and security of the Educado users, SomethingNew must oblige by the relevant data protection laws, GDPR and LGPD. Since, there is a high probability that Educado will be handed over to Aalborg University in the future and there is an expectancy of potentially many users of Educado, it will be crucial to maintain and update the aforementioned assessments which will be discussed in Section 7.5.

Lastly, it is very important to make a Privacy Policy and Terms & Condition for Educado. A Privacy Policy will make the guidelines on what to be aware of when implementing any features for the developers, within SomethingNew as a company and make sure that the employees are gathering information and operates in accordance to the privacy rules defined. Moreover, it is important to protect Educado as a service too, so a Terms & Condition should be made such that when the user agrees to this, they are accepting the rules defined by SomethingNew and helps preventing abuse and would be legally binding.

Something that was not implemented in this project was the ISO standards, which was defined in Section 3.3. Throughout the SOTA of LGPD in Section 4.2, it was mentioned that the ISO standards are commonly used in order to obtain compliance, and thereby highly recommended for companies to follow. Specifically the ISO 27001:2022 could have been relevant and useful, to keep up to date with the current security measures. Another improvement for Educado would be to follow the principles of privacy-by-design, which were defined in Section 3.2. This is another approach of obtaining compliance, where an example of it being applied is mentioned in Section 4.2.

Now, it can be seen in Table 19 which frameworks and assessments we ended up conducting in this project, compare to the ones we recommended companies to implement for compliance. Further discussion will be made in Section 7.5.

Table 19: Implementation Recommendations

DPIA	TIA	Privacy Notice	Privacy Policy	Terms & Conditions	ISO 27001	Privacy-by-Design
✓	✓	✓	✗	✗	✗	✗

Our project is thereby missing a privacy policy, terms & conditions, ISO 27001 and privacy-by-design. This is further elaborated in Section 7.5.

7 Discussion

After conducting all the relevant assessments and documentation, we discuss in this section what we learned from each part, and how it is usable for SomethingNew and Educado. Based on the GDPR and the LGPD, we evaluate if our results can highlight compliance, and what is necessary to prioritize, if it is not achieved yet. With the DPIA, TIA and privacy notice, we only covered some requirements and recommendations, and have many other tools to learn from. All in all, we discuss how the future of Educado looks, based on our work, and if the users has their personal data protected. As mentioned, the target group is waste pickers, though it is possible for everyone to utilize Educado as a service. Any user has equal rights in the app, and will be able to find the privacy notice in the app, while their data processing and transferring is documented in the DPIA and TIA.

Other than evaluating the results of our assessments, we look back at the challenges that we encountered, as the outcome was affected by the these challenges. We were already aware that as engineers we are not as knowledgeable on the legal perspectives of data protection, and our attempt on conducting these documentations was challenging, but significant task.

Lastly, we discuss our personal experience with the data protection laws in both Denmark and Brazil, and mention how field observation was applied during our academic journey.

7.1 DPIA Result

As it can be seen in Section 6.1, the DPIA was carried out after a screener was made. Prior to conducting a DPIA, we had to answer a questionnaire and got four *Yes* out of eleven, as shown in Appendix A. This meant that a DPIA was required and set the foundation for the assessment.

There were many challenges associated with constructing the DPIA. One of the major one was understanding and creating a data flow diagram. Depending on how the user would receive the certification when completing a course, the data would flow differently. The issue arises due to the fact that there are two scenarios:

1. The user completes a course and will see a screen on their mobile app that shows the user on their progress and course completed successfully.
2. The user receives an email from Educado with a PDF that contains their full name, completion of course, and approval from Educado authority.

In both cases, an evaluation or validation is required. Since, the user completes a course, the data is being sent to the backend. From there on, the generation of some sort of documentation can either be sent directly to the user by email, to their home address or simply displayed on their mobile app. Where the latter has been decided to follow in our DPIA based on assumptions. However, as the mobile app aims at helping waste pickers transition to an actual employment and gives them certification that they can show to potential employees, it would be more reasonable to generate a certification that actually looks legitimate and they can use it to support their case.

Another major challenge was the evaluation on international transfer of personal data. As the data being collected comes from the Brazilian waste pickers, it makes the origin of data gathering Brazil and destination for processing Copenhagen, Denmark. The data in transfer is being sent to Germany and stored by the American cloud storage service AWS. Furthermore, the data processor and data controller is the same, SomethingNew, which is located physically in Denmark. This changes the view and angle on the laws and regulations too because European data is not being transferred outside of EEA, but rather opposite.

Hence, the DPIA was made from GDPR point of view, since the data controller and data processor are both the Danish company, and SomethingNew is obligated to follow the European data protection laws. When that being established, it also means that LGPD has been enforced too, with small variations. LGPD is very similar to GDPR and the latter being more strict, makes the compliance more similar as well. As

mentioned in Section 5.4, the Brazilian equivalence to the European DPIA is a RIPD. The Personal Data Protection Impact Report contains, in most parts, the same subjects as the European DPIA. However, there are some differences between both. The Brazilian RIPD template is publicly available, but it is in Brazilian Portuguese. The template is published through the Brazilian official governmental website and was updated with version 2.0 on 5th of May 2023 [105]. The responsible for conducting an RIPD is the data controller, in this case SomethingNew. The RIPD is based on ISO/IEC 29134:2017 standard and the template is composed with inspiration of the DPIA, conducted for SomethingNew that has been provided by University College London [24].

In LGPD, it is not mandatory to perform an RIPD, however, if ANPD requests for one then it must be delivered [14]. In addition, upon the request from ANPD, further documentation might be demanded as well.

We have conducted a DPIA with the point of view from SomethingNew and European data protection laws, GDPR. It is important to note that there are differences between GDPR and LGPD, also from the point of view with data protection assessments. One major observation was regarding the lack of coverage on the data processing principles *data minimization* and *storage limitation* in LGPD. In no place in the Brazilian data protection law does it mention that organizations are not allowed to retain old and/or unused data of the data subjects. Whereas in GDPR it is clearly stated that it is not permissible to keep that type of data. These fundamental GDPR principles, data minimization and storage limitation exists with the purpose of protecting personal data of users by making sure that their data is only processed and retained if necessary as explained in Section 3.2.1. However, it is mentioned in the LGPD that unused/old data must be deleted only by request of the data subjects. This can be a problem as many Brazilian citizens are not aware of their rights and therefore do not know that they can request for deletion of their data. This was confirmed by the interview we conducted with the anonymous employee at the recycling complex who expressed his concern on privacy but was not aware of the data protection laws ensuring and protecting his rights.

RIPD is recommended to conduct in the future when more stakeholders are involved. When processing a DPIA and aiming for approving it, a lot of legal work is required. We have been in contact with our Brazilian collaborators in regards of gaining approval and seeking advice for our DPIA. We did not get our DPIA approved and we have been trying to get feedback from our Brazilian contacts on their local laws and regulations too. This is being elaborated further in Section 7.5.

7.2 TIA Results

Since data transfer are being made between Brazil and Denmark, a TIA is required which has been conducted in Section 6.2. The TIA has been carried out from the perspective of SomethingNew, which is a Danish owned company and therefore European based.

Before conducting the TIA, we discussed whether it was required to make one or not. When researching about the necessity of a TIA, we mostly found European sources whom advised that a TIA is required if European data is transferred out of EEA [26]. Our case specifically collects data of Brazilian data subjects, where no European data is collected and transferred. As data is processed in Europe by SomethingNew, the data is then stored in Europe, and sent to Brazil when applied in the mobile app. This situation where the processed data is sent to Brazil, is the reason why we conducted the TIA. With GDPR, a TIA becomes mandatory, as the European data protection law is known to be the strictest. As mentioned in Section 4.3 and Section 4.4, Europe has had some issues with transfer of European data, and after the Schrems cases, data controllers must assess if the data can be securely processed when transferred outside EEA. Brazil, the US and other countries outside Europe would not require data controllers to conduct TIAs.

Another consideration that came up was that the data exporter and data importer is the same company. While conducting the TIA, it was clear that the data transferring between countries and companies would make more sense, if data is shared among multiple stakeholders. If SomethingNew were to collaborate with a Brazilian organization, then the Brazilian company would be the one collecting personal data with LGPD

compliance. However, SomethingNew is solely responsible for the data in Denmark, and data protection will therefore mostly be based on the GDPR.

The TIA template we chose focused on specific areas, whereas one of these areas included how surveillance and national intelligence are part of the data transferring. Some of the point within the TIA asked if it was proven that national authorities operate surveillance programmes, however this information is not commonly known. With both EU and Brazil having similar data protection laws, we expect no surveillance, and we simply disallow national authorities to access the transferring of data controlled by SomethingNew. Based on Section 4.3, this issue is more relevant when transferring personal data to, for instance, the US.

The TIA we made is not how a fully TIA appears, and it would have been beneficial to have guidance from professionals and exports in order to simulate a real TIA. Our contact persons were mostly based in Brazil, and we did not expect them to have experiences in TIAs as they already did not know much about DPIAs. The Danish experts we tried to contact did not respond, though we believe their knowledge from an European/GDPR point of view would have been valuable feedback for the project. However, we did gather an understanding of compliance on our own throughout the making of our TIA. The transfer of European data and Brazilian data made us consider exactly what data is transferred across the countries, along with which data protection laws to consider depending on process. It was clear that stored data in the database and file storage is compliant with the GDPR as it is located in Europe, however data in transit applies security measures as well which must be defined in order to conduct the TIA. This assessment gave an perspective of the differences between the GDPR and the LGPD, and when compliance between both changes accordingly.

Similarly to our case with the DPIA, we mentioned in Section 7.1 that we were not able to have our assessment approved. Though, even without approval, it was mandatory for us to conduct the TIA according to the GDPR in order to archive compliance. In the end, we now have a TIA that we can present to ANPD if requested.

7.3 Privacy Notice Results

For this project, we conducted a privacy notice in Section 6.3, which is a document targeted data subjects to let them know how their data is used and what rights they have according to the law. We used a template that is meant for GDPR compliance, but we added a more detailed description about the responsibilities of the data controller, to make sure LGPD is complied with too.

The privacy notice we made is in English, however with the target group being Brazilian residents, we would have to translate the document to Brazilian Portuguese before implementing the privacy notice in the app, specially since waste pickers most likely have not learned English. As we went to Brazil, we discovered that some also can not read in Portuguese, which would make it difficult for the them to read the privacy notice. Based on our interview with a waste picker, we also discovered that the data protection law is not commonly known among waste pickers in general. With waste pickers not being aware of the law, they may not be aware that this privacy notice exists. Though, the privacy notice should still be available in the app at any time, even if they choose to not read it. Other than it is required by law, it should also present that the developers of Educado are prioritizing the security of its users.

A potential solution to this issue could be that the privacy notice has a text-to-speech feature implemented, which can read aloud while the text is highlighted accordingly. Then, the waste pickers has the option to learn about their user rights by clicking on a speaker logo.

From the industry's point of view, we should have a privacy policy alongside the privacy notice, then both the data subjects and staff of Educado has separate documents to go back to, whenever they wish to recall how the data is processed in Educado. Completing a privacy policy would also result in compliance of GDPR, as it is required, like the privacy notice. Our experience on international websites were that privacy notices are not available, however the privacy policy is found. Many different sources defined privacy notice and privacy policies differently, and some sources only had data on privacy policies. That means, depending on location of the world though most likely outside EEA, our documentation may be interpreted as a privacy policy instead of a privacy notice. However, with Educado being compliant

with GDPR and LGPD, both privacy notice and privacy policy must be implemented within the system. Furthermore, we should also make a terms & conditions document, in which the data subjects should read as they register in the system. The idea of making a privacy policy and terms & conditions is further elaborated in Section 7.5.

7.4 Challenges

We have been making several choices to understand how we can document best practices and recommendations to ensure privacy and data protection for applications. These choices encompasses conducting a DPIA and not a RIPD since Educado is owned by a Danish/European company and therefore under European jurisdiction. We could have been making a RIPD as well since this is the Brazilian equivalent to the European DPIA. However, we chose not to conduct one as the data controller and data processor is the same, SomethingNew.

Furthermore, we chose not to conduct a RIPD as we did not have the proper time frame to conduct one, it is written in the original language Brazilian Portuguese and needed translation to English, require a legal team with a good understanding on local, federal laws in Brazil and most importantly we did not have a Brazilian data importer or data processor/data controller. This would become relevant in the future when for example Brazilian endpoints would be installed and configured there for storage and data processing.

The DPIA was not approved due to many reasons. In consequence, a Brazilian LGPD lawyer that we have been in contact with, have declined assistance to offer his unofficial opinion or feedback as we asked of. When we were visiting Brazil, we had a meeting with him about the Brazilian data protection law as he is an expert in LGPD and this is his field. Therefore we asked about his thoughts on whether our LGPD understanding reflects in our GDPR focused DPIA. His response was that a DPIA requires substantial amount of information and insight into the project and what has led this to the DPIA and all the choices of technical nature that has been considered. Hence, he expressed very clearly that he cannot approve our DPIA unless he overtakes the case himself as he is not familiar with the Educado Ecosystem as we are. His reasons were that he needed many hours for his team to document all the necessary statements and only then provide an official approval, as elaborated in Section 7.5.

When conducting the assessments, especially the DPIA and TIA it has been very challenging due to many factors. One of the major issues has been the unavailability of SomethingNew to clarify and provide us the necessary information to continue and make the DPIA as accurate as possible. This has been especially problematic when making the data flow diagram as we did not know how a certification was being generated for the user when completed a course successfully. Furthermore, we needed clarification on where the data storage would happen. As we were briefed in semester start that Educado uses AWS EC2 instance that is located in Europe and perhaps Germany (Frankfurt) we were not sure on this information. Since, AWS is an American cloud service company and if the storage was being on American soil, American data protection law would apply.

Another obstacle was the legal aspect of the project which has been heavily focused on due to the interpretation and understanding of the different data protection laws. Since we are engineers and not lawyers, it has been challenging to understand and interpreting the problem from a legal point of view. Therefore, we seeked advice and legal aid from our Brazilian contacts to get us in the right direction. The time difference between Copenhagen and Brasília has played a role too, as we have been writing to our contacts through WhatsApp and email.

Communication with SomethingNew has not been the best, as we have been compelled to make decisions based on our assumptions in order to continue with our research and work. Access to the necessary resources and demonstration of these have been limited. Since the project is depended on proper functionality for the mobile app and the web app, it has been difficult to visualise how, for instance, the terms and conditions should be added, how the certifications are being generated. Since, other collaborators (study programmes) have been involved within the project it has been chaotic to understand and get an overview of the Educado Ecosystem in general.

Our reflections are that we could have been taken decisions earlier in the project to avoid time being wasted and getting postponed. Getting all the right access to resources and documentation of those would have been useful.

7.5 Future Improvements

Throughout the project, we figured that we did what we could to achieve our goals, however a lot could have been improved and many factors could increase the quality of our results. Working within a limited time frame and among unexpected challenges mentioned in Section 7.4, we chose to deselect some ideas, and instead listing them within this section to mention how we considered these.

7.5.1 Frameworks, Assessments, Documentation

As seen throughout Section 6, only the DPIA, TIA and privacy notice was conducted, in which we highlight that we could have considered privacy policy, terms & conditions and ISO 27001 as well. Out of the aforementioned frameworks and assessments, we believed the assessments to be most important to highlight. Conducting these are crucial to understand the risks and parameters of a system, and of course, an important part of being compliant.

Something that we hoped would improve the results of our assessments, was feedback from a Brazilian perspective. As mentioned in Section 7.1 and Section 7.4, we did receive a Brazilian equivalent to a DPIA, however we did not get the time to conduct it. Receiving the RIPD was a step forward, though conducting the Brazilian Portuguese documented assessment would have been time consuming for us, in which we knew we were not capable of doing in the short period of time left we had as we received the template. If we had both a completed DPIA and a completed RIPD, then we ensured compliance for both data protection laws. However, without input from Brazilian experts, or any approval on the assessments, the documentation for compliance can not be confirmed.

We did reach out to a Brazilian lawyer, who were knowledgeable in both the GDPR and LGPD, and he was capable of approving our DPIA with his team. What we learned from our conversation, was that approving a DPIA requires a lot of legal work. He assessed our DPIA on its own was not enough to get an approval, and he evaluated that a team must go through the case first, since they are not familiar with Educado. As our DPIA is based on how we imagine Educado will be developed, we knew that we could not provide his team enough documentation on the data flow, data processing, etc. However, he did estimate that if his team were to complete this task, it would require work from both of our sides:

- A team from his company will be responsible, including two tech/data protection lawyers, and one data protection intern.
- The team and SomethingNew would need a couple of hours on a video call, to discuss the project.
- Depending on if the team is ready to start reviewing the DPIA, they may “do some homework”.
- The DPIA document will be reviewed.
- The team will document our answers into statements, comparing them to the information on the DPIA to ensure these are correct.
- The team will invest €1,200 in attorney fees, considering all relevant fields are included: DPIA reviewing, GDPR, LGPD, international transfers.
- Only then, the approval of the DPIA can be obtained.

Even though we were not able to accept these conditions, we learned how assessments are conducted from a legal point of view. At the time, we only asked for approval on the DPIA, where we assumed that the TIA would require a lot of legal work as well in order to be approved. We did hope to ask for more advice and guidance from the Brazilian lawyer, however we respect that as a lawyer without any knowledge on the Educado project, he can not provide that.

Other than the assessments, we conducted the privacy notice. The privacy notice is not as important for SomethingNew in the current state, as the app is not ready to be released anytime soon, however we found it as an opportunity to make something that can show the users, that their data is protected.

What we are missing on the other hand, is a privacy policy that can be shown to SomethingNew's employees. Making a privacy policy is similar to the privacy notice, though there are just some other factors to consider, as the target groups are different. With the similarities of privacy notice and privacy policy, it would be an evident next step to add to Educado's compliance completion. However, if we were to conduct another framework, then the privacy policy would not be the prioritized option. Based on the privacy notice, we already know how the structure and content of the privacy policy, where only minor changes appears.

The ISO 27001 is seen as a more prioritized solution to go for as a next step, since new considerations and valuable discussion points must be conducted in order to successfully apply the standard. While many of the applied assessments are based on GDPR compliance, this ISO 27001 is commonly used internationally and shed light on another perspective than from an EU point of view, which might be beneficial to secure Educado. As it is described in Section 3.3, ISO 27001 contains a table with references to information security controls. All these controls are covering different categories of controls such as organizational control that can be applied in Educado to ensure authentication information, access rights, access control, information transfer and many more controls. The second category is the people controls which ensures security awareness and training for the employees of Educado or the developers working on the Educado Ecosystem. Then, we have the physical controls where SomethingNew for instance secure the physical storage, equipment used in the future such as endpoints physically installed in Brasília. Lastly, we have technological controls that must make sure that access to the Educado source code (backend and frontend) are being kept intact and only few authorized developers can read/write, keeping backup as well as monitoring and logging. As these controls are ensured in Educado, the potential risks are being prevented or mitigated as well. These mitigation strategies are being executed if the ISO 27001 is obtained [62].

The ISO standards were used as an approach to achieve LGPD compliance, whereas the principles of privacy-by-design was another applied approach as described in Section 4.2. Privacy-by-design, being part of Article 25 in the GDPR, provides relevance on technical measures in an app, as the principles highlight data protection implementation options [55]. This term is not mentioned in the LGPD, however with privacy-by-design being utilized in the cases mentioned in SOTA in order to be compliant, is implying that it is well suited for both GDPR and LGPD compliance. Even though it has not been the intention to follow this approach, we did cover some of its principles in the end. The DPIA for instance supports the first principle, *Proactive not Reactive*, where the potential privacy risks are identified and considered to prevent impacts before they occur. As well as the last principle, *Respect for User Privacy*, where it is mentioned to empower user-friendly options by for instance highlighting appropriate privacy notices. Principles we did not cover, are for instance the fifth principle, *End-to-End Security*, as it has not been decided how to handle physical devices, and safely dispose of them. If we did plan to follow the privacy-be-design, it would make sense to learn from the findings in Section 4.2, and ensure all eight principles are considered in Educado.

Lastly, we did not complete terms & conditions for the users of Educado. As mentioned, the privacy notice did not contribute with the biggest impact on Educado, since it is not released yet, hence why the terms & conditions is not seen as a highly prioritized feature for now. When the waste pickers were to use the app, then this feature should be implemented before release, as this is the approach that ensures consent from data subjects. With the current system, we would not have any idea if the data subjects agree with the data processing, or even if they are aware that the data processing is documented somewhere. The benefit of implementing terms & conditions is that the user must encounter this document before confirming the registration on the app. Even if the user does not read the terms & conditions, we will receive consent and know that the data subject is aware that their personal data will be processed. Both the privacy notice and the terms & conditions should possibly implement an option to read aloud from the

document, as the waste pickers may have a better understanding of the data processing, if it is explained to them. These should, naturally, be in Brazilian Portuguese.

All of the aforementioned frameworks, standards and assessments should be included and implemented to achieve GDPR and LGPD compliance, as we found out throughout the project these will improve the data protection and security of a service. However, some of the documents might be invalidated, depending on the future of Educado. Throughout the project, the data controller has always been SomethingNew, though there has been discussion with SomethingNew on potentially passing Educado on the AAU. AAU has always been a stakeholder, as Educado started out as a student project, though the co-founders, who are also students at AAU, will potentially not work further on Educado. Furthermore, multiple groups has already worked on Educado via AAU, with guidance from SomethingNew. Handing over Educado will require a longer process, and it is not known if it will happen in the near future, though it is likely AAU will be responsible for data processing and transferring in the future. With AAU as new data controllers, all of the mentioned documents may be invalidated, however the content remains the same.

7.5.2 Implementation

As mentioned in Section 1.2 and Section 7.4 this project was meant to include implementation of data protection, which we found out throughout the process was not feasible in the end. Though, we came across some possibilities of implementation, that we wanted to consider in case we were to implement them in the system.

Based on the DPIA, we discussed how data is protected when personal data is transferred and within the storage. In our case, we are not operating with any sensitive data, as we only process emails, full names and age group. The data minimization principle in GDPR ensures that only necessary personal data is collected, and based on the purpose of Educado, we only wanted these three factors to make it functional for the data subjects. There could have been features in the app that requires more personal data. An example we discussed was that certificates could be sent as a physical copy to the waste picker to their home address, though this address would be categorized a sensitive data. If we were to process and store sensitive data, we should remember to make it very clear for the data subject, to ensure their consent.

Other than considering how the data is structured, we also discussed how the implementation of Educado is structured. With the possibility of handing over Educado from SomethingNew to AAU, there might be a change in architecture. As mentioned in Section 5.3 a plethora of technologies are applied in order to run Educado, though some solutions might be replaced as SomethingNew originally planned a more organized solution, without implementing it. They mentioned for us, that they implemented the architecture using micro services, where they later described this architecture as outdated and discovered that they prefer a monolith structure where everything is managed with AWS. AWS already provide many features that benefits the services, such as backup and encryption, and if AWS were to be replaced, then many of the security measures should be reconsidered as well, especially when conducting the DPIA. They already removed some technologies that was mentioned in their report, such as Heruko.

Another discussion point regarding technologies was that the current login feature is managed by OAuth, which they wish to continue using, though with a focus on Gmail, WhatsApp or Facebook, as the waste pickers are likely to utilize these services.

It is not clear how many waste pickers would register and use Educado, however after conducting the DPIA, it was discussed if data partitioning should be considered. The current architecture may be capable of ensuring availability of the users, however if the app ended up with a large amount of mobile users, then it could be a possibility to distribute the server to both Europe and Brazil, to improve the performance and scalability. This could be managed by installing and configuring endpoints in Brazil as well.

7.6 Field Observations

This section finalizes the discussion of the report by having us share our personal experience in Brazil in regards of data protection.

As mentioned in Section 2.1, we conducted field observation, which helped us throughout the project as we established a better understanding of waste pickers and their working environment. While working on the Global Students SDG Challenge, our goal was to visit the recycling complex and study the data protection law of Brazil with the Brazilian students of UnB. However, even without the SDG Challenge programme, we still learned about how the data protection is handled in Brazil, just by flying to the country.

At the airport we experienced, as we were on our way to board to Brazil, that we had to face a camera and wait for authentication and validation of our identity through this biometric verification, in order to enter the plane. Biometrics are well known and well used as a way to authenticate users, however it was an unexpected experience for us. Being in Brazil, we discussed with Brazilians about the use of face recognition to be authenticated, in which they expressed is a common approach that they do not question.

One of the Brazilians even mentioned he was responsible for keeping track of who had physical access to a youth community club using face recognition techniques, where he explained how he now remembers the faces of everyone involved, and that the authentication system stores all those faces.

Applying biometrics as a technology in this case is for convenience, as they do not need to remember any passwords to enter, however we were wondering how the airport require our identifiable biometrical personal data in order to board the flight. The airport already identified us by confirming our passports.

Without the data minimization and storage limitation principles in Brazil, many systems like these exists, where personal and identifiable data is kept. The airport collects a large amount of personal data. Since it is not required for a service to erase personal data, unless requested by the data subject, the airport could store identifiable personal data of a large amount of both Brazilians and visitors.

Another observation was the use of social security number, which in Brazil is known as Cadastro de Pessoa Físicas (CPF). This identifiable CPF was used for almost everything that required a registration. Visiting for instance the office of Grupo Gestão, the junior enterprise of Production Engineering (one of the partners for Global Students SDG Challenge), we had to register ourselves with a CPF. As Danish citizens, we did not have CPFs and were not permitted into the building. Instead they found a solution to have us write down our full names and passport numbers. Some of the Danes jokingly mentioned to add random numbers, as these numbers where not used for anything other than registering. No one verified our identities, or confirmed our passports. We discussed how this number did not add any value, however it was common for Brazilians to always register themselves with this data that we in Denmark would categorize as sensitive data.

As the programme came to an end, we chose to go clubbing with the Brazilian students of UnB, however even at the club we were not able to utilize their system without a CPF. Their reasoning was that their payment system was registered to someone's CPF, and everything they purchase throughout the night, will add up in a total cost that is payed as they leave the club. We were therefore not able to buy our own drinks as foreigners in a club in Brazil, because it requires a social security number to store someone's purchase history in. Something we wonder about, is if these purchase histories are kept in the system after they leave the club. Is their personal data and activities in the club, the university, the airport stored even 10 years later utilizing a service?

The Brazilians were asked if they had any thoughts or opinions on this, where they responded that the CPF was simply used as a way to identify people. As Europeans under the GDPR, we mentioned how the social security number is considered sensitive data, and we would be concerned if services required this data, unless it has something to do with health, finance or other sectors managed by the state. These scenarios thereby gave us a first-hand experience of how the differences between privacy and data protection appears in daily life situations.

8 Conclusion

Personal data and protection of its nature, scope and context has become a very important factor in many fields and organizations. Due to the rise of internet connected services, being healthcare, educational institutions, e-commerce or finance, large amounts of data are being collected, stored, transferred and processed through transatlantic territories. Therefore, privacy and security are highly prioritised in many industries. In this thesis, a state of the art of privacy and data protection has been conducted in order to establish a baseline of the current technologies, frameworks, standards, and the relevant data protection laws.

With GDPR being enforced in 2018, LGPD being enforced in 2021, and many new data protection laws internationally, we expect the protection of data to be a high priority at the present time. Each data protection law defines their own requirements, which might affect the possibility of approving transferring data across regions and countries. The privacy risks that may occur must be considered whenever we utilize applications and systems, where the relevant standards and frameworks are applied, and appropriate technical measures are implemented to prevent the risks.

Through these observations, study and analysis we followed the problem formulation in which we defined in Section 1.1:

How can we document best practices and recommendations to ensure privacy and data protection for applications?

In this project we have selected a number of the most well-known frameworks, internationally acclaimed standards, best practices supported by researchers and specialists that we have evaluated to be the best guidelines, approaches and techniques to consider and follow when working with privacy and security for applications.

However, recommending security and data protection in general can be a challenge, as the requirements highly depends on where a service is located, and thereby which data protection laws to consider. Another consideration is the type of personal data, as some categories of personal data can appear more sensitive. All of the considerations must be established in order to understand and assess what is needed to protect the users of a service.

We specifically chose to focus on a case study to showcase that our selected app require studying the data protection laws within EU and Brazil, and include all the relevant documents that is mandatory to conduct for each data protection law.

Therefore, we also defined our sub-questions, to set our direction: The first sub-question refers back to the methodology in Section 2.1 where we mentioned how the case study is involved as our approach:

How can a case study approach be used to emphasize the importance of implementation on privacy and security measures in a real-life context?

Throughout our academic journey, we started with travelling to Brasília, Brazil in collaboration with the Global Students SDG Challenge, to discover the issues on illegal waste picking. These issues have, with support from UnB, been a focus for UN to realize a developing industry where these waste pickers are encouraged to get jobs in recycling complexes. Educado has been one of the proposed solutions, as this app gives waste pickers a chance to study different subjects provided by professors, and obtain a certificate as documentation of completion.

Educado had no security implemented as we started the project, however both we and SomethingNew knew that the data protection and security must be assessed and improved in order to achieve compliance with both GDPR and LGPD, to release the app and make it usable for waste pickers.

To obtain compliance, we followed the next sub-question, which made us define our strategy and structure to ensure Educado is compliant with the relevant data protection laws:

What strategies, rules, principles, privacy and security mechanisms are required in order to be compliant with GDPR?

There are several strategies and rules that an organization must implement in order to be compliant with GDPR. According to GDPR, an organization is obligated to conduct a DPIA, if necessary when working with personal data, and document it. We have been examining whether a Brazilian equivalence of the European DPIA is necessary and how to conduct one. RIPD is not compulsory as DPIA, however, if ANPD requests one, the organization must be able to deliver documentation and all relevant evidence along with it. We have assessed that Educado is an European owned system and has both the role as data controller and data processor, data importer and data exporter, which makes SomethingNew obligated to follow GDPR.

Furthermore, when processing data that are being transferred outside of EEA, the so called TIA must be documented in which all the security measurements such as CIA goals are being met. The TIA is required by EU, though not required from a Brazilian point of view. Additionally, we chose to make a privacy notice, as this document is required by the GDPR, but also defines the processing of personal data in the service. Applying this document highlights how data protection has been thoroughly considered and that the users has a list of rights as a user of our service. The intention of this document is therefore that the target group has access to read this privacy notice at any time, to have them evaluate if they feel protected as they utilize the service.

As it was decided which assessments and documents to conduct for us to obtain compliance, we finally define our last sub-question:

What is necessary for Educado as a case study to create a DPIA, a TIA and a privacy notice?

Studying the GDPR and the LGPD lead to reviewing what is required to achieve compliance for both data protection laws.

LGPD is very similar to GDPR and by following the GDPR, we cover the majority of the same content. It is important to note, that depending on the situation and context of Educado Ecosystem in the future, the conveyance of the ownership to Aalborg University and/or other parties, a RIPD might become relevant.

In this relation, we have been consulting a lawyer with LGPD expertise and good insight into local and federal laws of Brasília, to whom we have sent our DPIA to for evaluation or potential approval. His professional input on this matter was that a DPIA requires in-depth insight of the system, a legal team who can go through all aspects and technical knowledge. Therefore, he provided an estimate of the cost and expenses of performing one.

The TIA requires assessing the security of a country or region, to evaluate if personal data can be securely transferred out of EU, by studying the use of surveillance and inclusion of public authorities. A privacy notice must include all the rights the data subject has, as well as the explanation of how the data is processed in the service.

The outcome was that in the future, it must be considered that a DPIA, RIPD and TIA can be time consuming, needs legal team from all involved parties and requires a financial budget.

Furthermore, it is also good practice to have created a Privacy Policy and Terms & Conditions. By having these in the organization, it ensures clear rules and statements that specifies what, when, how and why to handle personal data. The Privacy Policy is internal documentation for the organization, so everyone has the same terminology and understanding of managing personal data. The Terms & Conditions will protect SomethingNew and eventually the party that will officially own the Educado Ecosystem.

Lastly, ISO 27001 and Privacy-by-Design are recommended tools to achieve compliance with both data protection laws, as they are preventing potential privacy risks, and used internationally.

9 References

[1] Ani Petrosyan. *Number of internet and social media users worldwide as of January 2023*. 2023. URL: https://www.statista.com/statistics/617136/digital-population-worldwide/.

[2] Lionel Sujay Vailshery. *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030*. 2022. URL: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

[3] Tiago Bianchi. *Most popular websites worldwide as of November 2022, by total visits*. 2023. URL: https://www.statista.com/statistics/1201880/most-visited-websites-worldwide/.

[4] Ani Petrosyan. *Number of data records exposed worldwide from 1st quarter 2020 to 3rd quarter 2022*. 2022. URL: https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/.

[5] European Parliament and Council of the European Union. *Complete guide to GDPR compliance*. URL: https://gdpr.eu/.

[6] Ben Wolford. *What is GDPR, the EU's new data protection law?* URL: https://gdpr.eu/what-is-gdpr/.

[7] United Nations. *THE 17 GOALS*. 2023. URL: https://sdgs.un.org/goals.

[8] United Nations. *Transforming our world: the 2030 Agenda for Sustainable Development*. URL: https://sdgs.un.org/2030agenda.

[9] United Nations. *Why the SDGs Matter*. 2022. URL: https://www.un.org/sustainabledevelopment/why-the-sdgs-matter/.

[10] Mateus Halbe Torres. *Global Students SDG Challenge*. 2023. URL: https://www.sdgchallenge.com.br/.

[11] Deutsche Welle. *Brazil: Reforming the garbage economy*. 2020. URL: https://www.dw.com/en/brazil-reforming-the-garbage-economy/video-51154608.

[12] Daniel Britze and Jacob Vejlin Jensen. "Digital learning platform for waste-pickers in Brazil: Building a microservices based distributed web system for creating and presenting digital learning material". Bachelor's Thesis. Aalborg University, 2021.

[13] Daniel Britze and Robert Nedergaard Nielsen. "Mobile Education Platform". Student Report. Aalborg University, 2019.

[14] DataGuidance by OneTrust and Baptista Luz Advogados. *Comparing privacy laws: GDPR v. LGPD*. OneTrust DataGuidance, 2022.

[15] Richie Koch. *What is the LGPD? Brazil's version of the GDPR*. URL: https://gdpr.eu/gdpr-vs-lgpd/.

[16] Amazon Web Services Inc. *GDPR compliance when using AWS services*. URL: https://aws.amazon.com/compliance/gdpr-center/.

[17] Robert K. Yin. *Case Study Research: Design and Methods (Applied Social Research Methods)*. Fourth Edition. Sage Publications, 2008. ISBN: 1412960991. URL: http://www.amazon.de/Case-Study-Research-Methods-Applied/dp/1412960991%3FSubscriptionId%3D13CT5CVB80YFWJEPWS02%26tag%3Dws%26linkCode%3Dxm2%26camp%3D2025%26creative%3D165953%26creativeASIN%3D1412960991.

[18] B.L. Berg. *Qualitative Research Methods for the Social Sciences, Pearson International Edition*. Pearson International Edition, 2017. ISBN: 9780205668106.

[19] Babak. *Why and how to write the state-of-the-art*. 2007. URL: https://blog.babak.no/2007/05/22/why-and-how-to-write-the-state-of-the-art.

[20] sikkerdigital.dk. *Skabeloner og værktøjer*. URL: https://sikkerdigital.dk/virksomhed/test-og-vaerktoejer.

[21] Virksomhedsguiden. *IT-risikovurderingsværktøj*. URL: https://virksomhedsguiden.dk/content/ydelser/it-risikovurderingsvaerktoej/fce38da7-025d-4326-98fe-c198f3ad8316/.

[22] ENISA. *Threat Taxonomy*. URL: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view.

[23] University College London. *Data Protection Impact Assessment (DPIA) Screener*. URL: https://www.ucl.ac.uk/data-protection/data-protection-impact-assessment-dpia-screener.

[24] University College London. *Data Protection Impact Assessment (DPIA)*. URL: https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/data-protection.

[25] ICO. *Data protection impact assessments*. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

[26] Datatilsynet. *Vejledning - Overførsel af personoplysninger til tredjelande*. Datatilsynet, 2022. URL: https://www.datatilsynet.dk/Media/637902777513932912/Vejledning%5C%20om%5C%20overf%5C%c3%5C%b8rsel%5C%20til%5C%20tredjelande.pdf.

[27] Health Service Executive. *Transfer Impact Assessment (TIA) Template*. URL: https://assets.hse.ie/media/documents/hse-transfer-impact-assessment-form.docx.

[28] Proton AG. *Data protection impact assessment*. URL: https://gdpr.eu/article-35-impact-assessment/.

[29] The International Association of Privacy Professionals. *Privacy Policy*. URL: https://iapp.org/resources/article/privacy-policy/.

[30] The International Association of Privacy Professionals. *Privacy Notice*. URL: https://iapp.org/resources/article/privacy-notice/.

[31] Information Commissioner's Office. *Make your own privacy notice*. URL: https://ico.org.uk/for-organisations/sme-web-hub/make-your-own-privacy-notice/.

[32] A.F. Westin and D.J. Solove. *Privacy and Freedom*. Ig Publishing, 2015. ISBN: 9781935439974. URL: https://books.google.dk/books?id=1RXqoAEACAAJ.

[33] João Mello da Silva and Paulo Celso dos Reis Gomes. *INSTRUÇÕES TRABALHO EM EQUIPE: EPR0071-PROJETO DE SISTEMAS DE PRODUÇÃO 1 (PSP1/2022P)*. University of Brasília. Brasília, Brazil, 2022.

[34] Derek Scally Berlin. "Time to tell tech firms that private data is 'none of your business' – Max Schrems". In: *The Irish Times* (2017). URL: https://www.irishtimes.com/business/technology/time-to-tell-tech-firms-that-private-data-is-none-of-your-business-max-schrems-1.3309734.

[35] Fortinet. *CIA Triad*. URL: https://www.fortinet.com/resources/cyberglossary/cia-triad.

[36] William Stallings. *Network Security Essentials: Applications and Standards, 6th edition*. Pearson, 2017. ISBN: 978-1-292-15485-5.

[37] European Union Agency For Network and Information Security. *Privacy Enhancing Technologies: Evolution and State of the Art*. European Union Agency for Cybersecurity, 2017. URL: https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art.

[38] Justin Hsu et al. "Differential privacy: an economic method for choosing epsilon". English. In: *Proceedings of the 2014 IEEE 27th Computer Security Foundations Symposium, CSF 2014*. 27th IEEE Computer Security Foundations Symposium, CSF 2014 ; Conference date: 19-07-2014 Through 22-07-2014. IEEE Computer Society, 2014, pp. 398–410. ISBN: 9781479942909. DOI: 10.1109/CSF.2014.35. URL: http://csf2014.di.univr.it/.

[39] Ágnes Fekete. *What are privacy enhancing technologies? The five best PETs for the modern tech stack*. 2022. URL: https://mostly.ai/blog/what-are-privacy-enhancing-technologies.

[40] Cynthia Dwork. "Differential Privacy: A Survey of Results". In: *Theory and Applications of Models of Computation*. Ed. by Manindra Agrawal et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 1–19. ISBN: 978-3-540-79228-4.

[41] Proton AG. *Principles relating to processing of personal data*. URL: https://gdpr.eu/article-5-how-to-process-personal-data/.

[42] ECOMPLY.io. *Article 6: Principles That Govern Processing Activities*. URL: https://lgpd-brazil.info/chapter_01/article_06.

[43] Ben Wolford. *Writing a GDPR-compliant privacy notice (template included)*. URL: https://gdpr.eu/privacy-notice/.

[44] Mark Foulsham, Brian Hitchen, and Andrew Denley. *GDPR: How To Achieve and Maintain Compliance*. 1st ed. 2019. ISBN: 9780429449970. DOI: https://doi.org/10.4324/9780429449970.

[45] Civil Nuclear Constabulary. *Data subject rights*. 2022. URL: https://www.gov.uk/government/publications/data-subject-rights/data-subject-rights.

[46] Proton AG. *Information to be provided where personal data are collected from the data subject*. URL: https://gdpr.eu/article-13-personal-data-collected/.

[47] Proton AG. *Right of access by the data subject*. URL: https://gdpr.eu/article-15-right-of-access/.

[48] Proton AG. *Right to rectification*. URL: https://gdpr.eu/article-16-right-to-rectification.

[49] Proton AG. *Right to erasure ('right to be forgotten')*. URL: https://gdpr.eu/article-17-right-to-be-forgotten/.

[50] Proton AG. *Right to restriction of processing*. URL: https://gdpr.eu/article-18-right-to-restriction-of-processing/.

[51] Proton AG. *Right to data portability*. URL: https://gdpr.eu/article-20-right-to-data-portability.

[52] Proton AG. *Right to object*. URL: https://gdpr.eu/article-22-right-to-object/.

[53] Proton AG. *Automated individual decision-making, including profiling*. URL: https://gdpr.eu/article-22-automated-individual-decision-making.

[54] Meta. *What Are Privacy-Enhancing Technologies (PETs) and How Will They Apply to Ads?* 2021. URL: https://about.fb.com/news/2021/08/privacy-enhancing-technologies-and-ads/.

[55] THE EUROPEAN PARLIAMENT and THE COUNCIL OF THE EUROPEAN UNION. *Article 25: Data protection by design and by default*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3063-1-1.

[56] Ann Cavoukian. *Privacy by design: The 7 foundational principles – implementation and mapping of fair information practices*. Information and Privacy Commissioner of Ontario, 2022.

[57] GDPR informer. *7 Key Principles of Privacy by Design*. 2018. URL: https://gdprinformer.com/gdpr-articles/7-key-principles-privacy-design.

[58] Proton AG. *General principle for transfers*. URL: https://gdpr.eu/article-44-transfer-of-personal-data/.

[59] EU. *Chapter 5Transfers of personal data to third countries or international organisations*. URL: https://gdpr-info.eu/chapter-5/.

[60] THE EUROPEAN COMMISION. *COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021*. URL: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en.

[61] cybersecurity echnical Committee : ISO/IEC JTC 1/SC 27 Information security and privacy protection. *ISO/IEC 27001 Information security management systems*. URL: https://www.iso.org/standard/27001.

[62] ISO and IEC. *INTERNATIONAL STANDARD ISO/IEC 27001*. URL: https://sd.ds.dk/Home#q=iso.

[63] Martin Brodin. "A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises". In: *European Journal for Security Research* (2019). DOI: https://doi.org/10.1007/s41125-019-00042-z. URL: https://link.springer.com/article/10.1007/s41125-019-00042-z.

[64] Evandro Thalles Vale de Castro, Geovana R. S. Silva, and Edna Dias Canedo. "Ensuring Privacy in the Application of the Brazilian General Data Protection Law (LGPD)". In: *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*. SAC '22. Virtual Event: Association for Computing Machinery, 2022, pp. 1228–1235. ISBN: 9781450387132. DOI: 10.1145/3477314.3507023. URL: https://doi.org/10.1145/3477314.3507023.

[65] Sara Carturan, Beatriz Matsui, and Denise Goya. "LGPD Framework: An Implementation and Compliance Guide for Technology Areas". In: *Anais do XLIX Seminário Integrado de Software e Hardware*. Niterói: SBC, 2022, pp. 176–187. DOI: 10.5753/semish.2022.223289. URL: https://sol.sbc.org.br/index.php/semish/article/view/20807.

[66] Rachel F. Fefer and Kristin Archick. "U.S.-EU Trans-Atlantic Data Privacy Framework". In: *Congressional Research Service* (2022). URL: https://crsreports.congress.gov/product/pdf/IF/IF11613.

[67] iubenda. *California Consumer Privacy Act (CCPA) Compliance Guide*. URL: https://www.iubenda.com/en/help/19133-ccpa-compliance-guide.

[68] OneTrust DataGuidance and Newmeyer & Dillion LLP. *Comparing privacy laws: GDPR v. CCPA & CPRA*. OneTrust DataGuidance, 2022.

[69] Cookiebot. *California Privacy Rights Act (CPRA)*. 2023. URL: https://www.cookiebot.com/en/cpra/.

[70] International Association of Privacy Professionals. *Key Dates from US Comprehensive State Privacy Laws*. 2022. URL: https://iapp.org/media/pdf/resource_center/key_dates_us_comprehensive_state_privacy_laws.pdf.

[71] Nigel Cory, Daniel Castro, and Ellysse Dick. "'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation". In: *Information Technology and Innovation Foundation* (2020). URL: https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic/.

[72] Gunes Haksever. *The new Trans-Atlantic Data Privacy Framework is taking form*. 2022. URL: https://www.jdsupra.com/legalnews/the-new-trans-atlantic-data-privacy-4376808/.

[73] Agnes Rønberg. *Max Schrems forventer EU-cloud: Jeg er 90 procent sikker på at vinde en tredje retssag*. 2023. URL: https://www.version2.dk/artikel/max-schrems-forventer-eu-cloud-jeg-er-90-procent-sikker-paa-vinde-en-tredje-retssag.

[74] Phil Beckett. "GDPR compliance: your tech department's next big opportunity". In: *Computer Fraud Security* 2017.5 (2017), pp. 9–13. ISSN: 1361-3723. DOI: https://doi.org/10.1016/S1361-3723(17)30041-6. URL: https://www.sciencedirect.com/science/article/pii/S1361372317300416.

[75] Simon Thomsen. *Extramarital affair website Ashley Madison has been hacked and attackers are threatening to leak data online*. 2015. URL: https://www.businessinsider.com/cheating-affair-website-ashley-madison-hacked-user-data-leaked-2015-7?r=US&IR=T.

[76] Brian Krebs. *A Retrospective on the 2015 Ashley Madison Breach*. 2022. URL: https://krebsonsecurity.com/2022/07/a-retrospective-on-the-2015-ashley-madison-breach/.

[77] Carlo Cilento. *Is Google Analytics illegal in Europe?* 2022. URL: https://www.simpleanalytics.com/blog/is-google-analytics-illegal-in-europe.

[78] Zack Whittaker. *This is the worst password from the Ashley Madison hack*. 2015. URL: https://www.zdnet.com/article/these-are-the-worst-passwords-from-the-ashley-madison-hack/#ftag=YHFb1d24ec.

[79] Dean Pierce. *What I learned from cracking 4000 Ashley Madison passwords*. 2015. URL: https://www.pxdojo.net/2015/08/what-i-learned-from-cracking-4000.html.

[80] Jonathan Stempel. *Ashley Madison parent in $11.2 million settlement over data breach*. 2017. URL: https://www.reuters.com/article/us-ashleymadison-settlement-idUSKBN19Z2F0.

[81] ECOMPLY.io. *Article 16: Deletion of Personal Data*. URL: https://lgpd-brazil.info/chapter_02/article_16.

[82] Jennifer Bryant. *CNIL is latest authority to rule Google Analytics violates GDPR*. 2022. URL: https://iapp.org/news/a/cnil-is-latest-authority-to-rule-google-analytics-violates-gdpr/.

[83] Stephan Winklbauer and Robert Horner. "Austrian DPA Decides EU-US Data Transfer through the use of Google Analytics to Be Unlawful". In: *Eur. Data Prot. L. Rev.* 8 (2022), p. 78.

[84] Ina Vedige Brøchner Rasmussen, Anja Bang Mejer, and Emma Bredahl Mortensen. "Mobile education Platform: Finance management for waste pickers". Bachelor's Thesis. Aalborg University, 2020.

[85] Auditório FT UnB. *Evento: SDG - CHALLENGE 2023 (de 23 a 27/01/2023)*. 2023. URL: https://www.youtube.com/live/GXjOn7RlVco?feature=share&t=5168.

[86] Stephanie Buga. *Monolithic vs Microservices: The pros, cons, and everything else*. 2023. URL: https://www.contentful.com/blog/monolithic-vs-microservices/.

[87] Abraham Silberschatz, Henry F. Kort, and S. Sudarshan. *Database System Concepts*. 978-0-07-802215-9. McGraw-Hill Education, 2020.

[88] Inc. MongoDB. *Relational vs. Non-Relational Databases*. URL: https://www.mongodb.com/compare/relational-vs-non-relational-databases.

[89] MongoDB Inc. *What is MongoDB?* URL: https://www.mongodb.com/what-is-mongodb.

[90] DB-Engines. *DB-Engines Ranking*. URL: https://db-engines.com/en/ranking.

[91] Amazon Web Services Inc. *About AWS*. URL: https://aws.amazon.com/about-aws/.

[92] Amazon Web Services Inc. *AWS Cloud Products*. URL: https://aws.amazon.com/products/.

[93] Amazon Web Services Inc. *AWS Pricing*. URL: https://aws.amazon.com/pricing/.

[94] Felix Richter. *CLOUD INFRASTRUCTURE MARKET - Amazon, Microsoft Google Dominate Cloud Market*. URL: https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

[95] Inc. Amazon Web Services. *Use Amazon S3 with Amazon EC2*. URL: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonS3.html.

[96] Inc. Amazon Web Services. *What is Amazon S3?* URL: https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#S3Features.

[97] Behrouz A. Forouzan. *Data Communications and Networking*. McGraw-Hill, 2013. ISBN: 978-0-07-337622-6.

[98] The OpenJS Foundation. *About Node.js*. URL: https://nodejs.org/en/about.

[99] ECOMPLY.io. *Article 9: Personal Data Subject's Right of Access*. URL: https://lgpd-brazil.info/chapter_02/article_09.

[100] Ministry of Citizenship. 2021. *Princípios da LGPD*. URL: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/principios-da-lgpd.

[101] ECOMPLY.io. *Article 18: Personal Data Subject's Rights in Relation to the Controller*. URL: https://lgpd-brazil.info/chapter_03/article_18.

[102] Gatefy. *9 rights guaranteed in the LGPD to data subjects*. URL: https://gatefy.com/blog/rights-guaranteed-lgpd-data-subjects/.

[103] ECOMPLY.io. *Article 33: Cases of Permission for the International Transfer of Personal Data*. URL: https://lgpd-brazil.info/chapter_05/article_33.

[104] ECOMPLY.io. *Article 38: DPIA or Data Protection Impact Report*. URL: https://lgpd-brazil.info/chapter_06/article_38.

[105] gov.br. *Guias e modelos*. 2023. URL: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd.

[106] Privacy Research Team. *LGPD Privacy Policy Requirements – The Basics To Know*. 2023. URL: https://securiti.ai/blog/lgpd-privacy-policy/.

Appendix

A DPIA Screener

Table 20: DPIA Screener [23]

DPIA Screening Questions	**Yes/No**
Will the project involve the collection of new information about individuals?	Yes
Will the project require individuals to provide information about themselves?	Yes
Will information about individuals be shared with organisations or people who have not previously had routine access to the information?	Yes
Will the project use information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	No
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	No
Will the project result in you making decisions or treating individuals in ways which can have a significant impact on them?	No
Is the information about individuals likely to raise privacy concerns or expectations, for example, health records or information that people would consider to be particularly private?	No
Will the project require contact with individuals in ways they may find intrusive, for example, unexpected telephone calls?	No
Will the project use personal data, including personal data obtained from live or operational systems for access or transfer outside the UK (e.g. use of Cloud, Hybrid or offshore support purposes)?	Yes
Will the project involve processing special category personal data?	No
Will the project involve the processing of under 18's personal data?	No