AALBORG UNIVERSITY
DENMARK

Semester:
8th Semester

Title:
Cloud and personal data: The study of the Chromebook case

Project Period:
Spring Semester 2022

Semester Theme:
IT Security Governance

Supervisors:

- Henning Olesen
- Morten Falch

Members of Group 6.13:

- A S M Farhan Al Haque
  Student No. 20210768
- David Holm Audran,
  Student No. 20210462
- Charity Uche Orji,
  Student No. 20210771
- Hac Duvarci,
  Student No. 20176600

Page Number:
118 pages

Date of Completion:
December 21th, 2022

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

Secretary: Charlotte Høeg

Abstract

In this project, we explore EU legislation and also foreign laws to identify the different impacts on the cloud computing ecosystem. This was accomplished by carrying out a thorough systematic literature review on the following topics: cloud architecture, legislation like GDPR, Standard Contractual Clause (SCC), EU-US Privacy Shield, CLOUD Act and relevant protection techniques for cloud. We also look through many discrete recent cases where cloud solutions had challenges to comply with legislation. We decided to select the Chromebook-gate case where privacy of a Danish school children was compromised. Along with this case, we also selected four relevant cases of big tech companies like Microsoft, Facebook, TikTok, and Google Analytics. We have performed an analytical case study of all these cases and examined the core issues that led these cases to contradict with EU legislation. We have also performed two interviews with current experts of the field to have a better understanding of the whole scenario. Then, we propose a model named Data Confinement Framework and validate if the framework is able to address all those issues of the cases providing solutions. With our analysis, we have showed that our framework is effective and functional to solve all the mentioned cases.

Cloud and personal data: The study of the Chromebook case

Charity, David, Farhan, and Hac

Aalborg University Copenhagen

Contents

Chapter 1

Introduction

Cloud computing refers to the ability to access and manipulate information stored on remote servers, from simple data storage to e-mail and other applications. Increased availability, reduced costs, unlimited computational resources and no need for maintenance are the main forces driving this change.

A statistic from Eurostat shows that the percentage of enterprises using cloud computing services has increased in almost every EU country between 2020 and 2021 [1]. Moreover, in the second quarter of 2022, the most significant cloud service providers, Amazon, Microsoft and Google combined, had a 65% share of the worldwide cloud market and up to 72% in the public cloud [2].

Moreover, the big-tech cloud providers provide a convenient and qualitative solution for school children, especially in Denmark, where many schools use a combination of Chromebook and Google Workspace for Education. However, the solutions, being a part of a broad portfolio of services, are not well confined, and user data can spread to other parts of their "ecosystem". Furthermore, user data are stored and processed along with other data in a system that is not restricted to Denmark or the European Union. This leads to conflicting legislation and disputes on the jurisdiction, as cloud providers are operating on a global scale.

Cloud computing providers typically collect a variety of data about their users in order to provide and improve their services. This data may include usage data, performance data or even location data, among others. For example, in their privacy policy [3], Google specifies that any information shared by a user can be used and processed, with the aim of improving or promoting their services, but also to conduct targeted advertising. With the right tools and methodology, data can be more valuable than oil [4]. It is especially true for Google, which has an enormous user base and practically unlimited computational power.

GDPR addresses the problems related to the illegal sharing of personal data. According to the regulation, which includes restrictions on sharing data with third parties and processing personal data, companies situated outside the EU and processing data from EU citizens should comply with GDPR.

Digitalization, data, and cloud technology have been heavily integrated into the primary schools of Denmark to the point that they are dependent on US-based services[5]. Since Schrems ll, it has become difficult to establish a legal basis for data transfer to third-countries, which, with these services, may be inevitable.

Such conflict is the use of Google's Chromebook and Workspace for Education software in elementary schools in Denmark. If and when data is transferred outside EU borders, under default circumstances, the rules of GDPR apply. Complying with the GDPR was the case until 2019 when a parent in Elsinore municipality caught their third-grade child on YouTube. More specifically, the use of Workspace requires having a Google account with personal information such as name and photo, among others. Subsequently, a YouTube account was made by the child through the Google account, leading to the data copying between the two.

Consequently, the child later got a disturbing comment from another YouTube user, which scared the child and then worried the parent, as the child's YouTube account displayed their full name, school name and even class grade. The addition of the add-on service (YouTube) was allowed through the Google Workspace account for teaching purposes. The parent reached out to the school, which resulted in the

Danish Data Protection Agency (Datatilsynet) investigating the use of Google's Chromebook and the Workspace for Education software in the schools of Elsinore municipality.
In the recent development of the Chromebook-gate, which is still ongoing, it is now known that data personal data is transferred out of the EU. This means that these personal data are under the laws of the jurisdiction where they are located and GDPR simultaneously. Moreover, the US has surveillance laws that can be concerning to some people because they may be seen as infringing on individuals' privacy rights. For example, FISA 702 allows the surveillance of non-US persons located outside the US without a warrant.

1.1 Problem Formulation

From this leads us to the following question:

- *What are the impacts of EU legislation on the Cloud computing ecosystem?*

More specifically, we want to look into different impacts and related questions:

- How can big tech companies process data of EU subjects while being complaint to GDPR?
- How can Google provide a solution with Chromebooks for elementary schools in Denmark without sharing data across their entire ecosystem?

1.2 Report Structure

In this report, we aim to illustrate our research questions through the analysis of the Chromebook case. We will provide recommendations for the Elsinore Municipality, in its role as both a cloud consumer and a data controller; and Google, in its role as both a cloud service provider and a data processor. We start by looking at the methodology we choose and different tools we use, described in chapter 2. In order to totally understand the Chromebook case, and provide thorough analysis and recommendations, we first have to understand different fields and what they imply for it. The first relevant field is cloud computing, which is described in chapter 3, as Google is in this case a cloud service provider. As cloud computing involves data processing, it is also relevant to understand the legislation in place, such as GDPR, which is described in chapter 4. Chapter 5 describes state of the art data and privacy protection techniques. Chapter 6 investigates relevant cases and what they implied for the users, the CSPs and the legislation. The next chapter, chapter 7, is the case study in itself, where we describe the Chromebook case in an intelligible and comprehensive manner. Chapter 8 provides a throughout analysis and aforementioned recommendations. Chapter 9 discusses and concludes the report.

Chapter 2

Methodology

This chapter describes the methodologies we use to solve our problems. The first methodology is a classic literature review, which aims to gain knowledge of the existing research in different relevant fields. It is followed by the interviews we conducted, with the explanation of our a qualitative study based on those. Following that is the description of our case study approach. Next, we outline the methodology used to develop a framework of our own and conclude the chapter by explaining our work tracking and distribution using a tool called Trello.

2.1 Literature review

In order to find relevant literature for our project, we searched for different articles with the keywords described in the following subsections. We entered those keywords in Google Scholar, Researchgate, Aalborg University Library and other relevant search engines for scientific papers. As the subject is relatively new and the case we chose to study is still ongoing, and without any published academic or scientific articles, we searched for information through non-scientific sources such as Max Schrems, field experts, newspapers, videos, blogs and official reports.

Cloud computing related

It is relevant to look at this field of knowledge as the main case we analyze uses cloud computing. With this field review, we want to understand the following concepts:

- Cloud computing
  - definition
  - architecture
  - privacy
  - and GDPR
  - and personal data

Legislation related

As personal data breaches have raised many concerns in recent years, legislation has been developed to address these. Since the architecture of cloud computing and its use involves cross-border data transfers, it is crucial to understand what legislation applies and how it works. As our case study involves a European school and a US company, we examine European and American legislation.

- EU data protection laws

- Privacy Shield
- GDPR
- SCCs
- US surveillance laws
- FISA 702
- Cloud Act

Data protection related

As this project aims to provide possible recommendations for the different actors involved in the Chromebook case, it is important to understand and refer to state-of-the-art data protection and privacy techniques. To do so, we searched for the keywords:

- data protection cloud
- privacy-preserving techniques
- personal data protection

Chromebook case related

The Elsinore Chromebook case is our main case and the focus of our study. As mentioned earlier, this case is still ongoing. Hence, finding precise and authoritative information takes time and effort. We also investigate recent similar and relevant cases.

- Denmark Chromebook case
- Elsinore Chromebook case
- Microsoft EU Data Boundary
- Google Analytics Ban in Europe

2.2 Interviews and qualitative analysis

In order to gain knowledge, insight and to support our case study, we decided to interview two experts in the area:

- Allan Frank, IT Security specialist and jurist at the Danish Data Protection Agency.
- Ole Kjeldsen, CISO at Microsoft Denmark.

The type of interview we conducted is a semi-structured interview, which is a data collection method that relies on asking questions within a predetermined thematic framework. We chose this type of interview because it is more open than a structured interview, allowing new ideas that the interviewers may not have thought about to be brought up as a result of what the interviewee says, and more formal than an unstructured interview.

In order to qualitatively analyze the interviews, we decided to take the deductive approach, which is a method of reasoning that involves making logical conclusions based on known facts. It allows us to point out answers essential to our research, which will be reused as part of our analysis.

Interview questions

Our interviews were conducted with the same themes in mind. However, each had some specifics, as both our interviewees have different roles within their respective organizations, and the organizations themselves are also different (Microsoft being a private company and the DPA being a public institution). The exact questions can be found in Appendix A and D. However, due to the semi-structured nature of the interviews, some questions asked may not appear among the prepared ones.

The interviews had common themes. Although asking about the same themes, we got different and interesting answers, which will be discussed in section 8.1. The common themes we questioned the two interviewees about were the Chromebook case, as they are both security experts and Allan Frank was the case handler inside the Danish Data Protection Agency; foreign legislation, in order to understand what Microsoft does about it, and to get the opinion of a qualified lawyer; and alternative solutions, in order to know if our proposed solutions are relevant, as well as maybe hear about solutions we ourselves have not thought about.

We asked Ole Kjeldsen specifically about Microsoft's data processing in order to get a better understanding of how it occurs at big providers. We also questioned him about Microsoft's upcoming EU Data Boundary project, as they promise that customer data will be stored and processed in the EU. Finally, the trustee model with Deutsche Telecom to understand why it did not work.

Allan Frank was asked specific questions about the Danish Data Protection Agency, its role and different processes, such as decision-making, within it.

2.3 Developing a Privacy Enhancing Framework

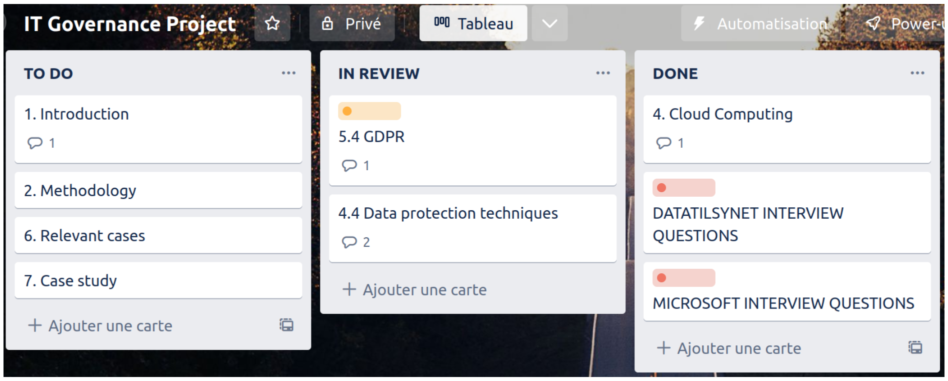
We investigate the privacy issues of EU users using cloud services. We investigate the significant concerns bringing out specific issues that cause privacy breaches. One of the main contributions of this project is that we strive to develop a framework or model that might address the core issues. We examine how befitting the framework will be to resolve the issues. We also recommend some solutions where we can implement the framework to scrutinize its feasibility. We do not just intend to prepare a checklist of different tasks for different organizations but a complete guideline to achieve the desired privacy of users in the cloud. The organizations that provide cloud services and the companies built on those services can consider the framework as a collective approach to different aspects of legal and technical liabilities on both sides. The framework neither lands all the responsibilities on the CSP nor the companies alone. Our aim is to prepare the framework in such a manner that balances the responsibilities evenly on both sides.

2.4 Case Study Approach

We decided to do a case study of the Elsinore Chromebook case as it helps us explore this phenomenon within its real-life context, as suggested by Robert K. Yin in his book *Case Study Research - Design and methods* [6]. Our case study is illustrative in the sense that it will help us highlight problems, decisions and implications related to our research questions. It is also exploratory in the sense that it will help us answer questions such as what happened and how in the concrete case, but also on a higher level in the sense of how the legislation is implemented and applied. By describing the specific Elsinore case, we dig deeper into the processes at play. The case study is built through the use of multiple sources of information, including our literature search on the Elsinore case, interviews with key actors, official decisions and newspaper articles. There is also an element of comparative study in our report as we explore similar cases and try to understand how alike and different they are from the main one.

2.5 Work tracking and distribution

To ensure a smooth workflow and efficient collaboration, Trello is used to label, assign and track tasks. We create tasks and assign them to team members, as can be seen in figure 2.1.



TO DO

1. Introduction 1

2. Methodology

6. Relevant cases

7. Case study

+ Ajouter une carte

IN REVIEW

5.4 GDPR 1

4.4 Data protection techniques 2

+ Ajouter une carte

DONE

4. Cloud Computing 1

DATATILSYNET INTERVIEW QUESTIONS

MICROSOFT INTERVIEW QUESTIONS

+ Ajouter une carte

Figure 2.1: Tasks distribution and tracking via Trello

These measures allow us to add tasks for future completion and monitor existing ones, which provides an overview of the completed and ongoing ones. When one member completes a task, he asks the others to review it. The group members will review the work and can either ask for changes or approve the completion of the task. It gives a better collective work examination and space for suggestions if needed. This also gives the group members the opportunity to get familiar with a part of the project they have not directly worked with.

Chapter 3

Cloud Computing

In this chapter, we start by giving a definition of Cloud computing, covering the essential characteristics. The second section looks at the cloud architecture, encompassing the major actors, their interactions and the distribution of control between the cloud providers and cloud consumers. The third section talks about the activities of cloud providers. The forth section focuses on personal data in the cloud. The last section looks at the cloud market. This chapter is based on NIST Cloud Computing definition [7] and NIST Cloud Reference Architecture [8].

3.1 Cloud computing definition

NIST defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [7].

Essential characteristics A cloud infrastructure refers to a collection of hardware and software that enables the following five essential characteristics of cloud computing:

- *On-demand self-service* - The principle that the consumer can setup, monitor and manage computing resources himself, as needed, and without requiring human interaction with cloud providers.
- *Broad network access* - The principle that the computational resources are provided over standard networks and can be accessed by different devices.
- *Resource pooling* - The principle that the provided computational resources are shared between multiple consumers and are dynamically scalable according to demand. This is known as the multi-tenant model. The consumer has, most of the time, no control or knowledge over the location of the resources but can sometimes chose a location at a high level, such as country, datacenter, etc.
- *Rapid elasticity* - The principle that the computational resources are "elastic" meaning that they can be upgraded and downgraded on an as needed basis.
- *Measured service* - The principle that the service is measured, typically a pay-per-use basis, meaning the use of the service is controlled, monitored and reported depending on the type of service, such as storage, processing, etc. Both the provider and the consumer gain transparency.

3.2 Cloud architecture

This section is based on NIST's Cloud Computing Reference Architecture [8]. In this paper, they present the Conceptual Reference Model which identifies the major actors, their activities and functions in cloud computing. An overview of this is presented in figure 3.1. It is important to overview the roles of the different actors in order to understand their different responsibilities. It is especially important for the cloud provider and the cloud consumer which are the two major actors involved in the Chromebook case.

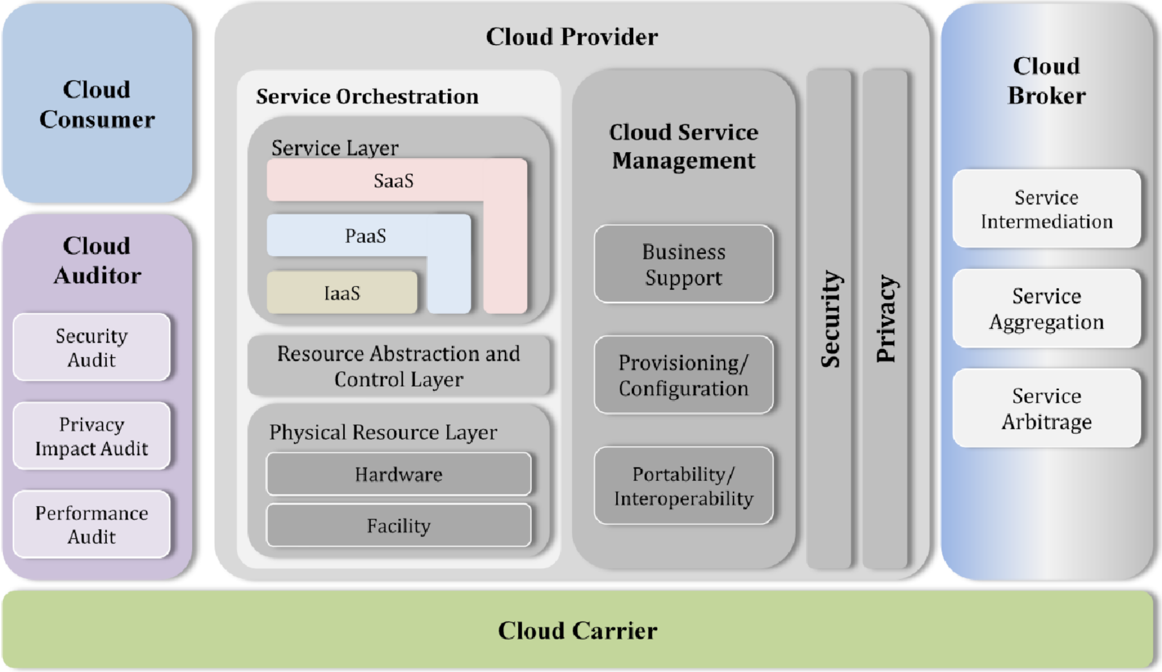


Figure 3.1: Conceptual Reference Model

Actors

The NIST Cloud Computing Reference Architecture [8] defines five major actors with their roles and responsibilities. Those five actors are:

- *Cloud Consumer* - An entity, a person or an organization that uses services from Cloud Providers. Cloud consumers have access to different types of services based on which type of consumer they are.
- *Cloud Provider* - An organization, a person or an entity responsible for making a service available to interested parties. There are five major areas concerning the activities of a cloud provider, later described in section 3.3.
- *Cloud Auditor* - An entity that conducts independent assessments of cloud services. This may include auditing the cloud system's performance, security and more recently data protection and privacy, among other things.
- *Cloud Broker* - Manages the use, performance and delivery of cloud services and negotiates the relationships between cloud providers and consumers.
- *Cloud Carrier* - This actor acts as intermediary and provides connectivity and transport of cloud services from providers to consumers.

Figure 3.2 shows the interactions between the different actors.

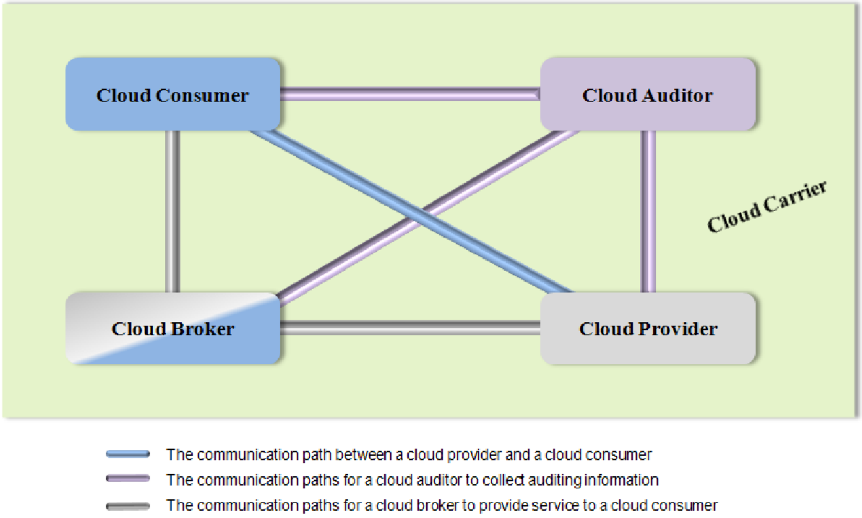

Cloud Consumer
Cloud Auditor
Cloud Carrier
Cloud Broker
Cloud Provider
The communication path between a cloud provider and a cloud consumer
The communication paths for a cloud auditor to collect auditing information
The communication paths for a cloud broker to provide service to a cloud consumer

Figure 3.2: Interactions between the different actors of cloud computing

Distribution of control

The control of the resources in Cloud is distributed between the Provider and the Consumer. As illustrated in figure 3.3, different service models, explained in 3.3, affect the control a person or an organization has over the computational resources in the system. The following figure shows these differences, which includes different layers.

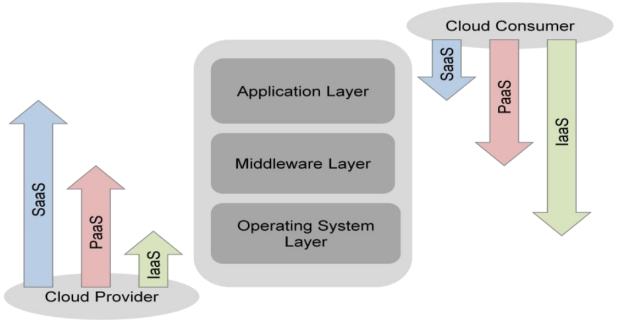


Figure 3.3: Distribution of control between Provider and Consumer in the Cloud

Depending on the distribution of control to consumers, their responsibilities in securing data and assuring data privacy greatly increases.

Service models

There are three main types of service models of cloud computing. Each type of cloud computing provides different levels of control, flexibility and management. Those three types are:

- *SaaS (Software as a Service)* - Enables the consumer is to use the provider's applications running on a cloud infrastructure.

- *Paas (Platform as a Service)* - Enables the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

- *Iaas (Infrastructure as a Service)* - Enables the consumer to provision processing, storage, networks, the used operating system and other fundamental computing resources.

The interesting service model in our case study is the software as a service, as this is what Google provides to the schools of Elsinore municipality.

3.3 Cloud Provider activities

The activities of cloud providers can be distinguished in five areas, which are described in the following subsections.

Service deployment

As NIST defines it in their Cloud Computing Definition [7], a cloud infrastructure can be operated in one of the following deployment models:

- *Private cloud* - This is a cloud system that only one organization can use and it can exist on or off premises. It can be managed by the organization itself or a third-party.

- *Public cloud* - In this type of deployment, the cloud infrastructure is provisioned for open use by the general public. Different types of organizations (business, academic, government, etc.) may own/operate/manage/maintain the cloud infrastructure. The fundamental characteristics of public clouds are multi-tenancy, as they are meant to serve multiple users who each require an isolated computing environment.

- *Community cloud* - This deployment model is used by a community of consumers that decided to come together for different reasons such as shared concerns, cost reduction and compliance considerations. One or more of the organizations in the community, a third-party, or some combination of them may own/manage/operate/maintain the cloud service.

- *Hybrid cloud* - The deployment model is a composition of two or more distinct cloud deployment models (private, community, or public) that remain unique entities but are bound together by software or technology.

The differences of those deployment models are how exclusive the computational resources are to a consumer. The one interesting us for the Chromebook case is the public cloud.

Service orchestration

Service orchestration refers to the composition of system components to support the Cloud Providers activities to provide cloud services. It includes different layers, one example is the physical layer which includes the monitoring of all physical resources in data centers.

Cloud service management

Cloud Service Management includes all the functions that are required for the management and operation of cloud services. As illustrated in figure 3.4, cloud service management can be described from the different perspectives.

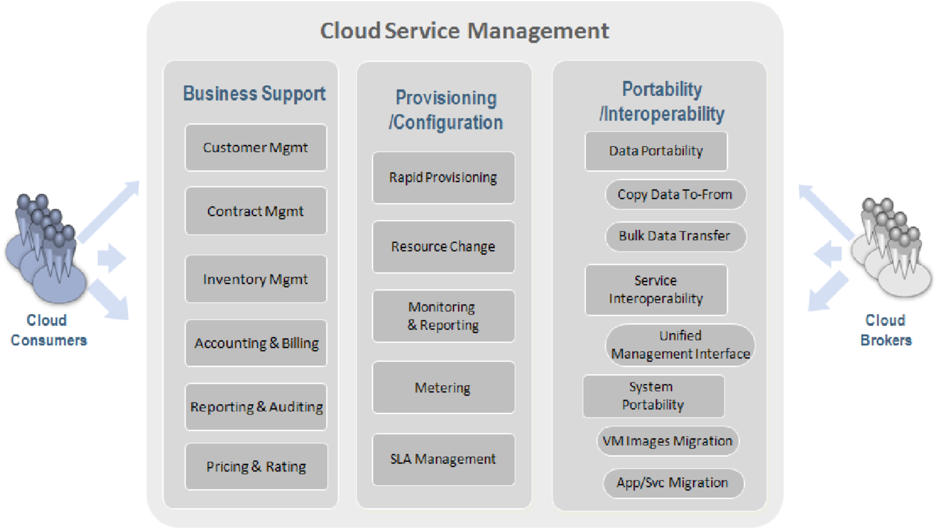


Figure 3.4: Cloud Provider - Service Management

Security

Security is a cross-cutting function that spans all layers of the reference architecture, involving end-to-end security that ranges from physical security to application security [8]. Hence, security in cloud computing concerns all the actors. The system has to address basic security controls such as authentication and identity management, among others, but also specifics about cloud computing, such as user isolation or container security.

The three service models, described in 3.2, expose different entry points into cloud systems. This means that adversaries have different attacking surfaces, making the chosen model a relevant factor to consider.

The deployment model perspective, which is described in 3.3, is another way to consider the security implications. Tenants have differing level of exclusivity depending on the deployment model.

Cloud computing does not have one specific architecture or deployment model, it is therefore really important to know what is used, who are the actors, what control do they have over the resources and what are there responsibilities regarding data protection and privacy.

Privacy

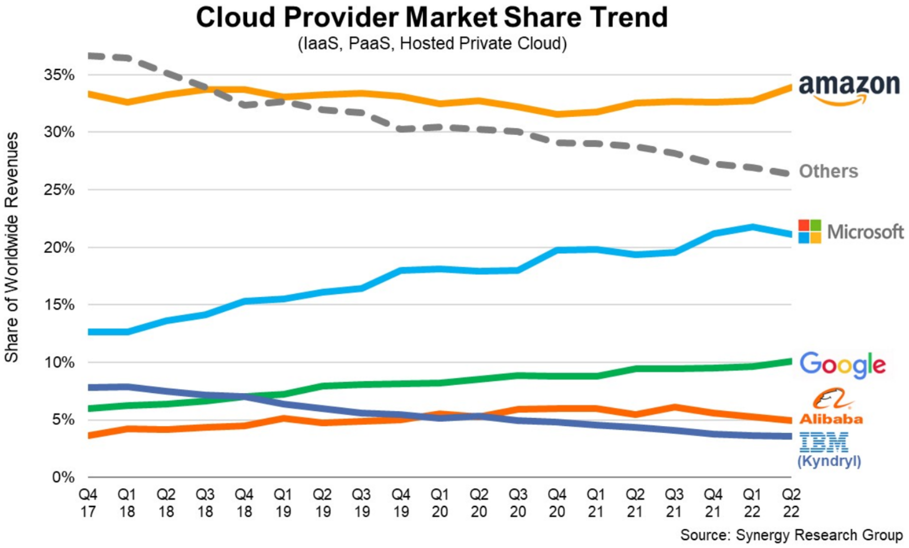
Cloud providers are required to assure the privacy of personal information when processed. This is usually ensured through different mechanisms such as data isolation, access control and data retention and deletion policies, among others. Those controls defend the users' privacy against malicious actors. However, data monitoring done by the cloud providers themselves, such as to ensure service quality or to detect and prevent abuse, could potentially compromise the privacy of users. It is hence important for cloud consumers to carefully review the privacy policies of cloud computing providers to understand what data is being collected and how it is being used.

3.4 Personal data in the cloud

Personal data is a critical resource in cloud computing as consumers want their data to be protected and private. One of the challenges for cloud providers is to keep the data protected, while still being able to process it and gain new information. The cloud providers collect user data from the users directly, such as email, name or payment details. They also collect a lot of data through their services, which is often called "consumer generated" or service data, in order to improve their services and personalize them. Such data can include usage, performance, device information and location, along with others. All those different data points can be aggregated and processed to make predictions about consumers' future interactions with the proposed service. They can also be used to provide more personalized advertisements as well as statistical analysis. Data can be processed and sold as long as legal conditions for that are fulfilled.

3.5 Cloud market

The cloud computing market is a rapidly growing and evolving industry that encompasses a wide range of products and services. It is dominated by three companies which are Amazon, Microsoft and Google. As can be seen in figure 3.5 from Synergy Research Group, Amazon holds 34% of the market, while Microsoft holds 21% and Google 10%, which adds up to 65% of the total market share.



Cloud Provider Market Share Trend

(IaaS, PaaS, Hosted Private Cloud)

Source: Synergy Research Group

Figure 3.5: Cloud Provider Market share

This market being dominated that much by American organizations can be a concern for European organizations and governments, as USA had and have legislation that conflicts with the European one, as will be described in the next chapter.

Chapter 4

European and US legislation

This chapter describes relevant European and US legislation, given that the focus of this report is to figure out the Chromebook case where European data is transferred to the US. We start by looking at GDPR which is an important legislation that applies to companies all over the world. We then try to understand American legislation and the concerns they have raised among European citizens and organizations. We conclude by investigating the evolution of the legislation, and what impacts cases such as Schrems I and II have had on it.

4.1 General Data Protection Regulation

The existence of data protection legislation dates back to the 1970s with the first ever Data Protection Law in Hessen, Germany. Over the years as the world of Information Technology evolved, there have been several legislation on the protection of personal data in Europe. These regulations include the Data Protection Directive, Safe Harbor, and presently the General Data Protection Regulation, among others. The General Data Protection Regulation(GDPR) is a European legislative act on the protection of natural persons with regard to the processing of personal data and on the free movement of such data[9]. Personal data in this context is any information relating to an identified or identifiable natural person.

The GDPR which went into effect in all EU member states in 2018 aims at unifying data protection laws across Europe, replacing the Data Protection Directive[10]. The Data Protection Directive(DPD) of 1995 was adopted to reconcile the protection of fundamental rights and freedom of natural persons in respect of processing activities and to ensure the free flow of personal data between Member states[11]. European regulations at the time have to be transposed into national law as they were not directly applicable in all Member states. Thus, data processing activities that were seen as lawful in one Member state were regarded as unlawful in another. These differences in implementation of European directives in each Member state made the DPD a failure[10], resulting to the adoption of GDPR.

Since May 25, 2018 the GDPR has been the regulation used in enforcing data protection in all EU member states. It is applicable to any processing of personal data by automation or otherwise. Organizations operating in all EU member states and processing personal data of data subjects in EU are expected to comply with it. Compliance with GDPR has not been an easy ride for many organizations since its inception. There have been about 1397 cases of violation of GDPR with fines up to €746,000,000[12].

4.1.1 Structure of GDPR

The GDPR is organized into 11 chapters with 99 articles, outlining important concepts to personal data protection such as Principles, rights of the data subject, controller and processor, transfer of personal data to third countries or international organisations, etc.

Chapter 3 of the GDPR lays out various rights of data subjects which are very essential to maintaining data privacy. These rights are:

1. Transparency and Communication: According to Article 13, the data controller must provide any information such as the purpose of processing the personal data and how long the data would be kept, upon request by the data subject in a clear manner by writing or other appropriate means.

2. Information: Whenever personal data are collected from a data subject, the data controller should provide certain information to the data subject such as: its identity and contact details as well as that of the data protection officer where necessary, recipients of the personal data and adequate information on if the personal data would be transferred to a third country or international organisation.

   On the other hand, if the personal data related to a data subject are not obtained from the data subject, the data controller in addition to providing the information above also has to provide the data subject with the source of the personal data and the categories of personal data concerned.

3. Right of Access: It is the right of a data subject to to get a confirmation from the controller if his/her personal data is being processed. If yes, the data subject has the right to access such information.

4. Right to Rectification: it is the right of the data subject to obtain correction of inaccurate data regarding him or her from the data controller without undue delay.

5. Right to Erasure: The right to erasure of personal data can be exercised by a data subject on the following grounds:

   - the personal data are no longer needed for processing
   - the data subject withdraws consent on processing of the personal data
   - the personal data have been processed illegally, etc.

6. Right to Restriction of Processing: If the accuracy of the personal is being questioned or the processing is is seen as unlawful, it is the right of the data subject to restrict processing of such personal data. On that premise, the controller should inform the data subject before lifting the restriction.

7. Right to Data Portability: It is the right of a data subject to receive his or her personal data given to the data controller in a structured, commonly used, machine-readable and interoperable format, and to transfer it to another controller if need be. The right to data portability only applies to data obtained from data subjects by consent or contract. It does not apply to personal data obtained for processing on legal grounds.

8. Right to Object: where personal data are processed for direct marketing purposes, the data subject should have the right to object to such processing, including profiling to the extent related to such direct marketing, at any time and without cost.

9. Automated Individual Decision making, including profiling

4.1.2 Scope of GDPR

The focus of GDPR is precisely on the processing of personal data, in whole or in part. It also applies to personal data which forms part of a filing system. A filing system here refers to a structured set of personal data that is accessible and easily retrieved by a specific criteria (related to individuals).
This is however limited and does not apply to processing of personal data

1. by a natural person for personal use, for example: social networking. But it applies to controllers and processors who provide the means for the processing of personal data in this case.

2. by legal or government authorities for protection of national security.

3. to prevent, investigate, detect or prosecute a criminal.

GDPR also makes provision for the protection of personal data of children. The rights a data subject has under GDPR is also applicable to children. According to Article 8 of the GDPR, If a child is at least 16 years old, processing of his or her personal data by a data controller is only lawful with consent from the child. On the other hand, if the child is below 16 years of age, the consent of the parents is needed before any processing of the child's personal data. It is also very important that the data controller verifies that the consent given is actually from the child's parents or legal guardian.
Any processing of anonymous data is not covered by GDPR.

4.1.3 International Data Transfers

The GDPR provides regulations on transfer of personal data from EU to third countries or international organisations. To ensure protection of natural persons, data controllers and processors must comply with the conditions stipulated in GDPR in relation to transfer of personal data to and from third countries or international organisations. These conditions do not prevent member states from entering international agreements with third countries provided they do not conflict with the GDPR and ensure adequate level of protection for the rights of data subjects.
According to the GDPR, transfer of personal data is allowed to a third country without need for added authorisation if there is adequate level of data protection. This decision can be reached if there are legal provisions that offers such level of data protection equivalent to those of the GDPR. Other important factors taken into consideration are the specific processing activities, the respect for the rule of law, and the scope of relevant legislation in the third country.
In the event that an adequacy decision is reached, the European commission should monitor the functioning of decisions on the level of data protection in the third country or international organisation, as well as those adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. The commission should also carry out periodic review of the functioning in consultation with the third country or international organisation. Moreover, the commission should take into account the views and findings of the European parliament, the Council and other relevant bodies and sources.
However, if the commission ascertains that the third country or international organisation no longer ensures an adequate level of data protection, the transfer of personal data would be disallowed. In this regard, the commission would inform the parties involved of the reason for such decision and work together to resolve the issue where possible.
If there is no provision for data protection in the third country or international, the controller or processor can make use of of binding corporate rules, standard data protection clauses adopted by the Commission, a supervisory authority or contractual clauses authorised by a supervisory authority.

4.1.3.1 Standard Contractual Clauses (SCCs)

Standard contractual Clauses (SCCs) are standardised and pre-approved model data protection clauses that allow controllers and processors to comply with their obligations under EU data protection law[13]. The SCCs caters to international transfer of personal data in EU or to countries outside EU. However, data controllers and processors are not obligated to use the SCCs. But integrating the SCCs in their data transfer contractual arrangements with other parties shows compliance to the personal data protection requirements outlined in GDPR.

On 4 June 2021, the European Commission adopted new SCCs. Until that time, the Old SCCs decided upon by the commission since 5 February 2010 has been in use. The old SCCs was limited in scope. It doesn't deal with the common data flows that exists. They could only be used by controllers based in EU. The old SCCs did not allow for controllers or data exporters not established in EU. Only 2 types of transfers are covered in the old SCCs: Controller to Controller transfer of data and Controller to Processor transfer of data. The old SCCs may still be in use now for data processing contracts entered before 27 September 2021, but it would no longer be valid any deal come 27 December 2022. Only the new EU SCCs must be used then.

The new SCCs which is of 2 sets is used for fulfilling the requirements for relationship between controllers and processors in GDPR and the Data Protection Regulation applicable to EU institutions, bodies, offices and agencies. It is also used to comply with the requirements of the GDPR for transferring personal data to countries outside EU (third countries).

4.1.3.2 Architecture of the New EU SCCs For Data Transfer to Third Countries

The new SCCs follows the requirements of GDPR. for data transfer to third countries, it has one set of clauses with 4 modules covering different forms of data transfer:

- Module 1: Controller to Controller
- Module 2: Controller to Processor
- Module 3: Processor to sub-processor
- Module 4: Processor to Controller

An important feature of the SCCs are the annexes. Detailed information on the particular transfer covered by the SCCs must be provided in the annexes. These information include the list of parties involved and their roles, the type of personal data to be transferred and its purpose, frequency of transfer, nature of processing, how long the personal data would be kept and necessary measures taken to ensure security of the data.

In addition to the primary parties binded by this contract, the new SCCs provides a docking clause that allows new parties to join the SCCs throughout the life cycle of the contract. For example, hiring and adding a new sub-processor to widen the processing chain. When new parties are added to the SCCs, the annexes must be updated with the new parties and their roles accordingly.

It is also important to note that the SCCs must be governed by the law of an EU member state as well as its jurisdiction in the event of conflict throughout the duration of the specific transfer. This is to be specified by the parties involved in the data transfer.

4.1.3.3 Transfer Impact Assessment

It is the obligation of parties depending on the SCCs for data transfers to conduct a Transfer Impact Assessment (TIA) to ensure adequate level of data protection in a third country. A Transfer Impact Assessment is an analysis made by a data controller or processor of the impact and security implications of data transfer to a country outside the European Economic Area(EEA) or EU that does not benefit from an adequacy finding by the European commission[14].

When drafting or preparing a TIA, the legal frameworks in the third country and its implication on the security of the personal data to be transferred should be the focal point.

To evaluate the risks to the rights of data subjects that could result from a specific transfer, a TIA should have the following steps:

1. Specific description of the data transfer. This should include the parties involved in the data transfer(the data exporter and data importer), the categories of personal data to be transferred and the purpose for the transfer of such data.
2. Description and evaluation of applicable legislation in the third country that could affect the transfer of data. For example, rules or laws that allow disclosure of personal data to public authorities and/ or grant public authorities' power of access to personal data[15].
3. Evaluation and summary of all relevant details outlined in Steps 1 and 2 above to determine potential risks to the data subject created by the specific transfer of data.
4. Security measures to mitigate any possible risks to data subjects identified in Step 3, to ensure a level of data protection equivalent to that provided by GDPR.
5. A final decision based on the assessment carried out, whether the transfer of data is acceptable given the risks and other factors considered.

A data transfer would only be possible if the final conclusion shows that the third country can provide adequate level of data protection notwithstanding the identified risks to the data subjects[15].

4.1.4 GDPR key concepts

This section presents the important terms and concepts related to privacy and GDPR used throughout this report. The purpose of this chapter is to provide a clear picture of the concepts that we found is necessary to understand the different legislations.

Data Subject

Data Subject is the end user whose data can be collected. In other words, the data subject is an individual person who can be identified through processing different data which is called identifiers, for example name, social security number, passport number, bank account number etc.

Personal Data Vs Sensitive Personal Data

The idea of the personal is indicated while explaining data subject. According to Danish Data Protection Agency, any data that can be related in the process of identification of a subject can be referred to as personal data [16]. For example, e-mail address, photo, fingerprints, etc. Personally Identifiable is the term when any specific data or in combination with other data it is feasible to identify a subject. Such kind of data is not stored in the systems as plain data. The industry practice of storing these sort of personal data is by masking and replacing the data with some code. But these masked data stills remains personal data as they can be traced back using the same code and considered as pseudonymised information. Personal information is classified into two categories sensitive and non-sensitive.
Sensitive personal data is a special type which is emphasized in different legislations. Sensitive data is not allowed to be handled usually with the other general personal data. The scope of processing these sensitive data is held limited by GDPR. In `Chapter 1 Article 4 Paragraph 13 - 15`, GDPR states few examples of such kind of data [17]:

- *Bio-metric data:*

  > 'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data; The term dactyloscopic data refers to images of fingerprints or palm that can be used to identify a person.

- *Genetic data:*

  > 'Genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

- *Health Records:*

  > 'Data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

- *Political or Religious Orientation:* Any data which explicitly indicates someone's political views or religious orientation is considered as sensitive personal data. Also any data that can be processed to identify the racial or ethnic group of a data subject is regarded as sensitive.

Data Controller

A data controller is defined as an organization, legal person, public authority, or agency, that determines the reasons and mechanisms of processing personal data. It can be done separately by it's own or jointly with others. This method of combining other bodies is referred to as Joint Controllers. GDPR has enforced rules for Joint Controllers in `Chapter 4 Article 26`. The responsibilities has to be allocated transparently to each of the controllers.

Data controllers are directly connected to the data subject. They also have to follow obligations like ensuring individuals their right to access their information, being compliant to the international data transfers. Controllers can also be subjected to fines or any allegations made by data subject.

Data Processor

Data processor is an external entity who performs data processing on behalf of the data controllers. GDPR specifies the regulations for data processors in `Chapter4` from `Article 28 - 32`. For the first time, GDPR has made the processors accountable to any damage caused by processing for not being compliant. The processor cannot include any other entity in processing without prior notice to the controller. But GDPR allows sub-processors only if that entity is complaint verified. The processor and controller integrate to provide the substantial security required for the confidentiality, integrity, and availability of the data.
The term processing has diverse set of operations. GDPR states the data processing in `Chapter 1 Article 4`, which includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data. In the same article, GDPR also states about the `"restriction of processing"` that indicates the restrains the scope of processing in the future.
The sensitive personal data described previously in this chapter, requires special management of processing. In `Chapter 2 Article 9 Paragraph 1`, GDPR interdicts processing of any personal data without explicit consents of the data subject.

Data Processing Agreement (DPA)

DPA is the legally binding written agreement between the controller and the processor. The DPA contains the responsibilities and liabilities or handling, processing and protection of personal data. In `Chapter 4 Article 28`, GDPR states the details that should be included in the agreement:

- **General Information:** The type of personal data used, exact mechanisms of processing on the personal data, duration of time for processing, the location of the data storage, and also the terms of termination of the contract
- **Responsibilities of the Controller:**The controller is held responsible for issuing all instructions for processing.
- **Responsibilities of the Processor:** There are good number of responsibilities for the processor from being accountable regarding each stage of data processing and security to delete and return all data to the controller at the end.
- **Technical and Organization Requirements:** Security of the data, access and testing mechanisms to ensure the system resiliency.

Data Profiling

Profiling refers to the automated processing on the personal data to examine and analyze certain aspects related to any subject. For example, the health condition, financial condition, personal interests, or performance at work of a subject. According to `Recital 71`, GDPR allows profiling of data only upon imposed requirements of the subject's rights being met. It is worth mentioning that `Recital 71` holds special protection for any sort of processing of children data as they are less aware of their rights, consequences, and risks. `Chapter 2 Article 8 Paragraph 1` states that any processing of children data is only allowed is at least 16 years old. And the below that age be between 13 and 16 years, it is required to have the consent of the parents of that child [18].

Third-party

GDPR defines third-party in `Chapter 1 Article 4 Paragraph 10` [17] as:

> 'third-party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Data controllers must sign contracts with third-party stating clear instructions on the use and processing of data. A controller has to review and audit the compliance of the third-party. Without any written approval, a third-party can not outsource any GDPR relevant services.

Recipient

The idea of a recipient is described in GDPR `Chapter 1 Article 4 Paragraph 9`:

> 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third-party or not.

However, there are exceptions in categorizing recipients. Any public authority receiving personal data of any subject for particular query is not regarded as recipient. The public authority must have to be in compliance with applicable data protection rules for processing the data [17].

Consent of Data Subject

According to GDPR, `Chapter 1 Article 4 Paragraph 11`, the term consent is defined:

> 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

There are certain conditions that constitutes consent imposed by GDPR in `Chapter 2 Article 7 Paragraph 1 - 4` [19]:

- The consent must be informed, freely given and specific
- The consent must be in written contractual format and the controller has to be able to demonstrate that the data subject has consented to processing of his data.
- The consent must be unambiguous, written in plain language and easily distinguishable from any other issues.
- The data subject can withdraw his or her previously given consent to data processing. And the procedure of withdrawing consent must be as easy as giving consent.

Data Protection Impact Assessment (DPIA)

Recital 84 of GDPR states:

> In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk...

As evident in this recital, a DPIA is required for any processing operations that could lead to a high risk of personal data of natural persons. The DPIA must be done by the data controller before any processing operation begins. It is necessary that the controller consults the data protection officer when carrying out the data protection impact assessment (Chapter 4 Article(35) GDPR). The results of the assessment would determine what additional measures should be put in place during processing to ensure the protection of personal data. Some things that should be included in the DPIA include

- a systematic description of the intended processing operation and its purpose
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes
- an assessment of the risks to data subjects.
- measures to be taken to address the risks, ensure protection of personal data and compliance to GDPR[20].

Data Minimization

Chapter(2) Article5(1) of GDPR defines data minimization as limiting personal data to what is necessary in relation to the purposes for which they are processed. This is one of the principles to be followed when processing personal data[20].

Personal Data Breach

‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed(Chapter 1 Article 4(12) GDPR)[20]

Data Protection by design

In processing of personal data, data protection by design entails that necessary technical and organisational measures are put in place by data controllers when deciding on the means of processing, during the design of products to be used for processing and during the processing itself.

Recital 78 of GDPR states "When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfill their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfill their data protection obligations". It also recommends implementing data minimization and pseudonymization to ensure data protection[20]

Data Protection by Default

Data protection by default means that processing of personal data must be done with the highest privacy protection such that only data necessary for a specific purpose is collected by default. Organisations can for example implement this by limiting access to users' profile, set users' service settings to avoid automatic opt-ins on customer account page, and improving other security features[20, 21, 22].

Binding Corporate Rules (BCRs)

Binding Corporate Rules(BCRs) are internal rules or codes of conduct in multinational or international organisations regarding cross-border transfers of personal data to third countries. They are really essential as they serve as proper safeguards to enable international/ cross-border transfer of personal data in the absence of an adequacy decision. A competent supervisory authority, such as a data protection agency, must approve the BCRs in line with the consistency mechanisms provided in GDPR Article 63[23]. For this to be done, the BCRs must

- be legally binding
- apply to every affected member of the multinational or international organisation.
- be carried out by each of the concerned members
- provide a means for data subjects to exercise their data subject rights
- have detailed information on the organisation, the type of processing and its purpose, the type of personal data involved, etc.[20]

4.2 American surveillance laws and programs

American legislation can be conflicting with the European one. Additionally, American mass surveillance programs have been disclosed in recent years. This has raised many concerns among Europeans citizens and institutions.

4.2.1 Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act (FISA) of 1978 is a United States federal law which establishes procedures for the physical and electronic surveillance and collection of "foreign intelligence information" between "foreign powers" and "agents of foreign powers" suspected of espionage or terrorism [24].

Section 702 In 2008, with the FISA Amendments Act, FISA was amended and the Section 702 was adopted. It authorizes the collection, use, and dissemination of electronic communications content stored by US internet service providers (Facebook, Google, Microsoft, etc.) or traveling across the internet's backbone (with the compelled assistance of US telecommunication providers such as AT&T and Verizon) [25]. The fact that a target is a suspected terrorist, spy or criminal, etc. is not a requirement under Section 702. What is required is that the target is a non-US person "reasonably believed" to be located abroad, and that a "significant purpose" of the surveillance is to obtain "foreign intelligence information". According to Seald, FISA 702 is not extraterritorial, meaning that it only applies to companies operating in the United States. [26] If those companies have the ability to remotely access servers hosted outside of US, then the data stored there can be seized under FISA Section 702.

4.2.2 CLOUD Act

The Clarifying Lawful Overseas Use of Data (CLOUD) Act, is a federal law passed in 2018, that amended the Stored Communications Act of 1986. It allows US courts to issue a search warrant compelling US electronic communication service or remote computing service providers (even if the data is hosted outside the US, e.g. in the EU) to provide all data of an individual, without any authorization from the courts of the country where the individual or the data are located [26]. The conditions that the warrant should meet to be lawful are [27]:

- the request must be addressed to an online services provider.
- this provider must fall under the jurisdiction of the United States. It applies to any US-based company, as well as to its subsidiaries – even if registered abroad.
- the data requested shall be in the provider's possession, custody or control.
- the request must be justified by the needs of a criminal investigation.
- it must be validated by an American judicial authority, which checks the merits (serious suspicion that an offense has been committed or is about to be committed), the relevance (the data sought are actually likely to be of interest to the investigation) and the proportionality.

Should the requested data be physically stored outside the United States, it is no longer an obstacle to its communication to the American authorities. The European Data Protection Supervisor notes that the CLOUD Act does not authorize any systematic, large scale and/or indiscriminate collection of personal data, but rather governs targeted requests, subject to procedural safeguards, concerning specific law enforcement investigations [28].

4.2.3 Executive Order 12333

As stated by the NSA themselves, Executive Order 12333 is the foundational authority by which NSA collects, retains, analyzes, and disseminates foreign signals intelligence information. The principal application of this authority is the collection of communications by foreign persons that occur wholly outside the United States. [29] However, other communications can be collected as well, such as outside communication to and from the US. Collection pursuant to E.O. 12333 is conducted through various means around the globe, largely from outside the United States, which is not otherwise regulated by FISA.

4.3 Evolution of Legislation

Given that the focus of the project is to understand the implications of recent EU legislation on cloud services in terms of transferring the personal data to US. We need to have background knowledge of why different legislation were enacted over time and the limitations they had for which they were invalidated. This chapter reflects how the Schrems trials caused the laws of the time to be declared invalid. And lastly, the basic terminologies regarding the privacy in cloud services is described.

The transfer of personal data of an EU citizen to third countries outside EU has been a burning issue over the last decades. Every EU citizen is assured that the rights of their personal data must be processed and transferred to any third countries with appropriate protection and consent by the Charter of Fundamental Rights of European Union(CFR). Safe Harbour Agreement introduced in 1998, was into play to ensure the transfer of data between EU and US so that private companies do not accidentally disclose or lose personal data.

4.4 The Effect of the Schrems Cases

4.4.1 Schrems I case

In 2013, an Austrian activist and lawyer named Max Schrems called the legitimacy of Safe Harbour Agreement into question. He filed a complaint against Facebook Ireland Ltd to the Irish Data Protection Commission (DPC), Ireland being the European headquarter of Facebook. The agenda of the complain was to prohibit transfer of personal data from Ireland to US as the EU data protection law prevents the data transfer to non-EU countries. This complaint was rejected by DPC at first. Later, Schrems filed for the judicial review in the Irish High Court. The High Court accepted the case and in turn referred the case to the European Court of Justice (ECJ).

4.4.2 Effect of Schrems I: Rise of EU-US Privacy Shield

The case drew enough attention so that an alternative regulation was drafted to provide the required level of data protection. The Safe Harbour Agreement was terminated and was replaced by EU-US Privacy Shield on 12 July, 2016. Controllers at that time could either adhere to the Privacy Shield or the SCC that was already approved at that moment. Although the privacy shield addressed many shortcomings of Safe Harbor Agreement, but still there were many existing loopholes. The privacy shield drew harsh criticism for not being able to ensure the privacy for which it was intended to be designed for. The officials of European Data Protection Agency assessed the privacy shield and expressed their concerns. Few of the main concerns include:

- Lack of accountability enforced on the organizations to delete the personal data immediately after the purpose is fulfilled.
- Lack of protection of data while transferring to any third-party country.
- Lack of clear limits on bulk access of European data by any U.S. officials.

4.4.3 Effect of Schrem II: The Fall of EU-US Privacy Shield

SCC being followed by Facebook to transfer the personal data both in transit and stored from EU to US still was big concern. According to Schrems, this is in violation with GDPR which is described in the next Chapter 4.1. The Schrems II case was reffered to the European Court of Justice (ECJ) for validating whether the Trans Atlantic data transfer was in accordance with the current regulations and to stop data transfer to Facebook. As a result of this case, the ECJ did not find any standard equivalence of data protection with GDPR. The EU-US Privacy Shield was invalidated as a result of the case. The SCC was still held valid with some revision that only if SCC can ensure the equivalent level of data protection in the third countries as promised by GDPR.

Chapter 5

Privacy-preserving techniques

In this chapter, we look at different state-of-the-art solutions to ensure data protection, data privacy and geographical confinement for cloud solutions. The chapter starts with the idea of the trusted proxies and then deep dives into the privacy preserving techniques. We discuss many cryptographic and non-cryptographic techniques, that could be used as part of a proposed recommendations for the different actors of the Chromebook case. Figure 5.1 shows the tree of different approaches we discuss in this chapter.

5.1 Introduction

Figure 5.1 shows the different privacy preserving techniques discussed in the following sections of this chapter. These techniques is considered as the background knowledge analyzing the technical perspectives of the framework we want to formulate later in the Chapter 8.3. This chapter also lays the foundation of the recommended solutions we will try to propose in Chapter 8.5.

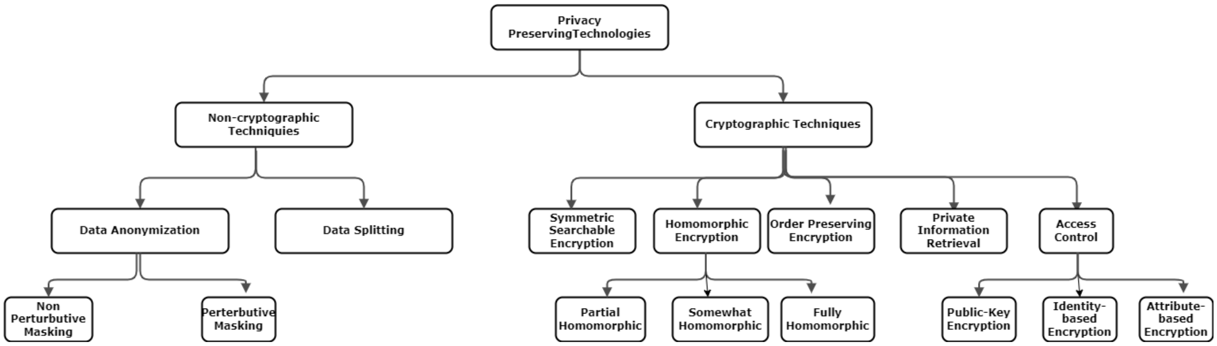


Figure 5.1: Discussed Privacy Preserving Techniques in this report

5.1.1 Trusted proxies

In their paper, Ferrer et al. [30] , describe the basics of a trusted local proxy to outsource data to an untrusted third-party. Figure 5.2 shows the general architecture for a data protection proxy. Clear data can be exchanged with the proxy as it is trusted, and masked data is exchange with the CSP.

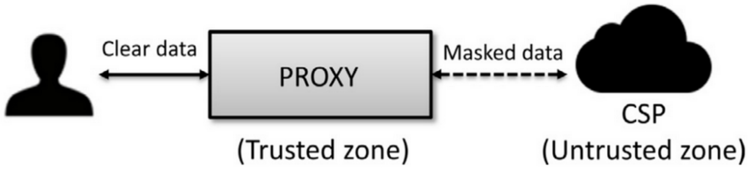


Figure 5.2: General architecture of a data protection proxy implementation

As shown in figure 5.3, the proxy is responsible for the masking of data when outsourcing it, and for the unmasking of data when retrieving it, rendering this process imperceptible to/for? the user.

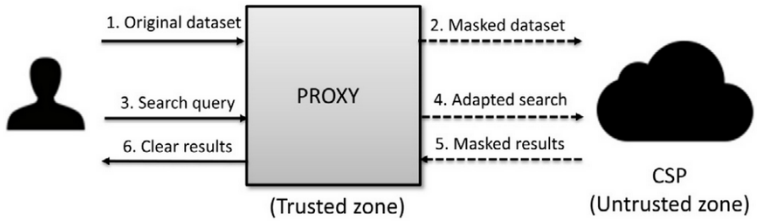


Figure 5.3: Data workflow through proxy to cloud

5.2 Non-cryptographic techniques

5.2.1 Data Anonymization

Data anonymization is the process of protecting sensitive information by masking data attributes. It can be done by different techniques that are described in this section. Whereas encrypted data are useless to whoever cannot decrypt them, anonymized data retain some utility for everyone [31].
Attributes can be classified based on their disclosure potential:

- *Identifiers* - Any data that can be used to identify someone specifically. We can consider the social security number or passport number as examples. Data anonymization does not include any of these kind of data.
- *Quasi-identifiers* - These identifiers are not capable of directly identifying an individual but in combination of other quasi-identifiers it is possible to specify someone. For example, considering attributes like age, zip code, gender, and job cannot specify someone explicitly but in combination of all it is possible for identifying an individual. Quasi-identifiers require to be anonymized.
- *Sensitive attributes* - Attributes that are considered sensitive to a user's identity such as religion, health condition or income, etc. If they can not be associated with an identity, they can be published unaltered, which ensures the preservation of analytical utility.
- *Non-sensitive attributes* - Attributes that are considered non-sensitive to a user's identity. As such, they can be published unaltered.

Domingo-Ferrer et al. [30], distinguish two differents types of masking techniques in data anonymization: non-perturbative and perturbative masking.

5.2.1.1 Non perturbative masking

Although non-perturbative masking reduce the accuracy of the data, it does not alter its truthfulness. Non-perturbative masking consists of three methods:

- **Sampling** - consists of taking a sample of data, and consider it as the population. Re-identification is made more difficult by the fact that a unique record in the sample might not be unique in the original data.
- **Local suppression** - consists of suppressing certain attribute values in order to increase the number of records sharing the quasi-identifiers combination, thus making re-identification more difficult.
- **Generalization** - consists of transforming attribute values into new more general categories, to reduce detail and make quasi-identifiers combinations less rare.

5.2.1.2 Perturbative masking

Perturbative masking, contrary to the non-perturbative one, reduce the truthfulness of the data but may preserve its accuracy. The main methods of perturbative masking are:

- **Noise addition** - Distorts data by adding noise. It can be adding or subtracting a specific value for numerical attributes or adding letters for alphabetical ones.
- **Data swapping** - Consists of picking different records and randomly exchanging their values.
- **Microaggregation** - Consists of regrouping similar records into groups and releasing the average record value.

Depending on what computation has to be done on the data, we may chose one of the two masking techniques and one or more of their methods. Perturbative methods conserves the accuracy of the data while non-perturbative ones preserve the thrutfulness.

5.2.2 Data Splitting

Data splitting is a protection technique based on fragmenting sensitive data and storing the fragments, in clear form, in separate locations. Fragments should be such that a single fragment neither allows re-identifying the subject to whom it corresponds nor reveals confidential information that can be linked to a certain subject [32]. The process of splitting and storing the data is shown in figure 5.4.
Step 0: The user uploads his privacy requirements to the trusted proxy, where data splitting is performed.
Step 1: The user sends his data to the data splitting algorithm.
Step 2: A combination of the name of the fragment and its location is stored in a separated trusted database, managed by the proxy.
Step 3: The segments are sent to the different chosen cloud service providers.

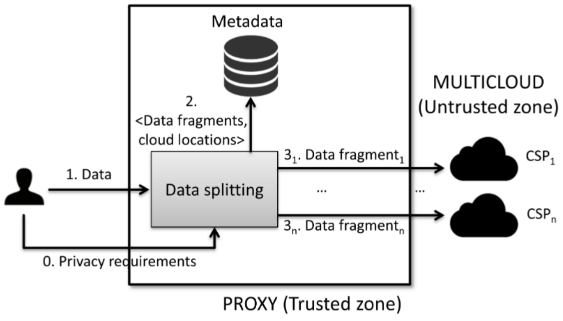


Figure 5.4: Data splitting into multi-cloud

This splitting process is privacy-preserving, as each different fragment doesn't provide enough identifying information on itself, and lossless, as it is possible to reconstruct the original data from the fragments.

The opposite mechanism, that is retrieving the split data, is shown in figure 5.5.
Step 1: The user sends a query to the proxy in order to retrieve split data.
Step 2: All of the fragments locations and names are retrieved by the proxy from the trusted database.
Step 3: The different fragments are queried by the proxy from the different service providers.
Step 4: The proxy receives and aggregates the fragments.
Step 5: The complete result is sent to the user.

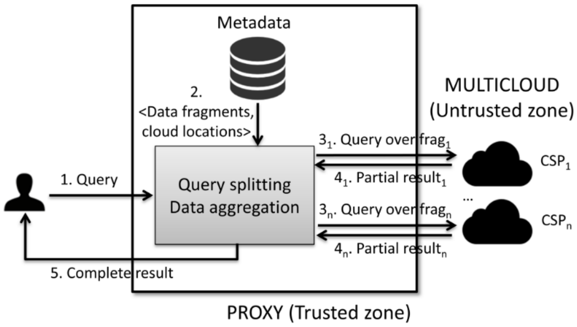


Figure 5.5: Data querying from multi-cloud

It is arguable to say that this mechanism presents a single point of failure in the proxy. If the proxy fails or is compromised, the data can not be accessed or reconstructed. It is hence recommended to have backup plans and redundancy. As the proxy is the only one knowing where the different fragments are and how to reconstruct the original data, it protects against CSPs collusion.

5.3 Cryptographic techniques

The most recognized approach against the data breaches or any data loss is to apply the traditional cryptographic techniques to the data before outsourcing them to any external entity. But providing security is not the only factor in this case. Encrypting the data makes it impossible for the CSPs to perform any sort of complex processing on the data which goes against the actual purpose of using cloud. To address this problem, ongoing researches have been carried out to balance the operation of specific processing on the outsourced data while still ensuring the necessary security.
In the following sections, we described the state-of-the-art cyrptographic approaches to address the burning issue of privacy and security. These approaches enable clients to securely outsource their data, allowing CSPs to execute the necessary processing and functionality. These approaches are intended to provide both end-to-end security and user-side protection. We will concentrate on three functionalities of cloud on the outsourced data that are challenging to satisfy through conventional encryption techniques:

- Data Search Functionality
- Computational Functionality
- Storage control Functionality

5.3.1 Data Search Functionality

Extracting pieces of useful information from the complete dataset is one of the most broadly utilized functionality in any modern system. The biggest challenge in this case is searching not only contain potential sensitive information in the context of the encrypted outsourced data but also in the query and the extracted information with the search. The queries can also be of sensitive nature if it contains personal details. There are cryptographic solutions designed to secure the search operation explained below. These solutions differ in proportion of security and supported queries. **For ensuring the search operation on the encrypted data, we have to consider three entities in this case: the `data owner` who outsource the dataset, `authorized users` who are permitted to perform the search operations, and lastly `the semi-trusted server` in which the operation is performed.** The techniques that are discussed in this report are Symmetric Encryption (SE) using only a single key for both encryption and decryption of the data.

5.3.1.1 Symmetric Searchable Encryption (SSE)

Symmetric Encryption (SE) encrypts the data before outsourcing it to the cloud ensuring secure searching. Among many architectures of SSE scheme, symmetric SE is one of the most widely applied. The SSE scheme is devised with single-user and single-cloud architecture, where a user outsource it's dataset to the cloud and wants to query later. This scheme operates with four polynomial-time algorithms:

1. **Key-gen Algorithm:** The owner initiates with this function which takes one security parameter as input to provide the owner the `security key K`.
2. **Build Index Algorithm:** This algorithm is executed for generating the `index I` of the documents, so that it is possible to search a portion from the encrypted data.
3. **Trapdoor Generation Algorithm:**This algorithm converts any query into it's encrypted version named `trapdoor T`. It takes the query and the security key, K of the owner to generate the encrypted trapdoor.
4. **Search Algorithm:** This algorithm is executed by the server to generate the output of the search. It takes the `trapdoor T` and `index I` as inputs and generates output of the searched `data D`.

The SSE scheme is illustrated in the Figure 5.6. In the outsource phase, the owner encrypts the dataset and the index with security key for outsourcing the data to the cloud. Next, in the query phase, the trapdoor is generated from the query and sent to the cloud server. In the computation phase, cloud integrates the trapdoor with the index to extract the required data from the dataset. The encrypted data is sent to the owner after decrypting the data in the next phase [33].
Depending on the type of supported query SE schemes can be further classified into:

- ***single-keyword:*** The query has only one keyword in it.
- ***Conjunctive:*** The query has arbitrary conjunctions of single keywords
- ***Boolean:*** The query contains Boolean formulas on query

Prominent Security Issues
In terms of security. SE schemes are proved not to be among the best with notable vulnerabilities. SE schemes is found to be leaking information like the number of the `data items` in the outsourced dataset, `search pattern` indicating whether two or more queries are identical, `results of search` having the segments of data for any query. However, Y. Zhang et al. [34] performed `file injection attacks` that leaks information of single-keyword and conjunctive queries.

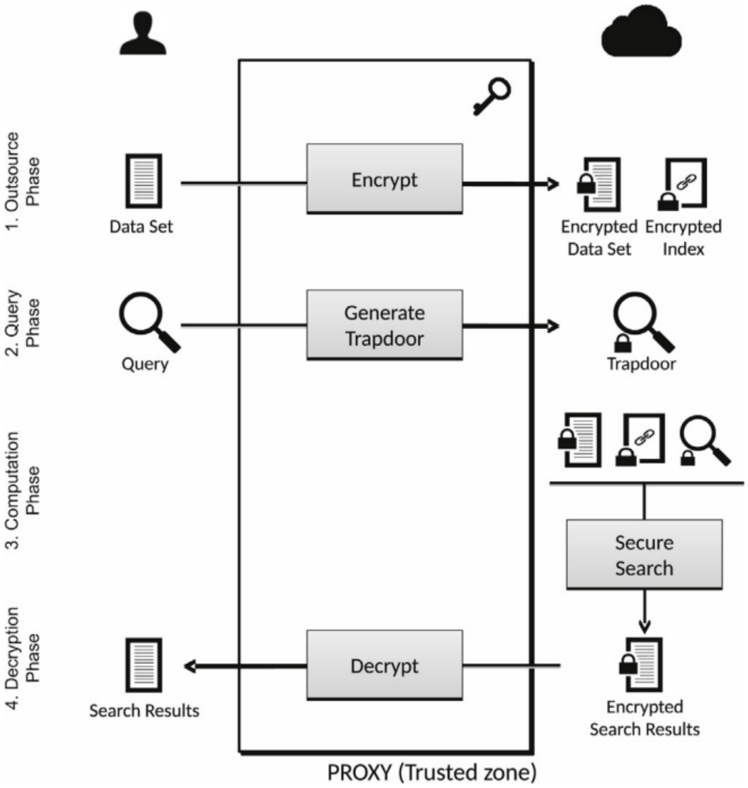


Figure 5.6: SSE scheme for data search on ciphertext

5.3.1.2 Private Information Retrieval (PIR)

The fact that a database operator can identify and follow queries allows him to assume what the user is after and hence can be privacy violating. Protecting the knowledge of what data is retrieved from a database is the aim of this technique [35]. Different assumptions are made for PIR:

- The database is a binary string $x = x_1, x_2, ..., x_n$ of lenght n.
- Copies of the string are stored by k $\geqslant$ 2 servers.
- The user is interested in the value of bit x_i

The scheme is that the user queries $(Q_1, Q_2, ..., Q_k)$ each of the k servers and gets replies $(A_1, A_2, ..., A_k)$ from which the bit x_i can be computed, as can be seen in figure 5.7.

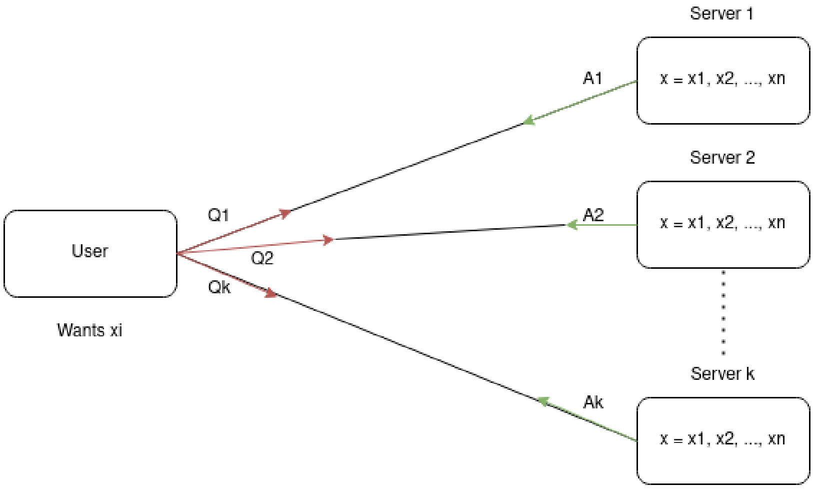


Figure 5.7: PIR scenario with k servers and n bits

This scheme is used to retrieve only one bit from databases. However, Wang et al. [36] propose a scheme to retrieve blocks and multiple blocks of bits, which has the same basis. This scheme reduces computation overhead and client communication.

5.3.2 Computational Functionality

Executing statistical queries to the encrypted data in the cloud server is a critical requirement in the fields like financial technology firms, applications on machine learning, decision support systems. However, it is not hard to understand computation on encrypted data incur massive security threats. To the rescue the confidentiality issues for computing on outsourced data are addressed by Homomorphic Encryption technique.

5.3.2.1 Homomorphic Encryption (HE)

HE technique is a `single-reader` architecture that enables computational operations on the outsourced data. The HE technique is illustrated in Figure 5.8. In a client-server environment, first the set-up algorithm is locally executed to generate a key for the client. In the outsource phase, the dataset is encrypted with the generated key for outsourcing to any cloud server. In the query phase, the user can request for any query for arithmetic operation on the encrypted data. Next, in the computation phase, the server securely computes the query operation and keep the results encrypted. And lastly, in the decryption phase, the user receives the encrypted result of the operation and decrypts it.
The homomorphic encryption scheme is classified into three categories:

- *Partially Homomorphic Encryption (PHE):* This technique can support only a single arithmetic operation on ciphertexts. The two most used partially homomorphic techniques are additive and multiplicative homomorphic encryption. If the operation on the ciphertext generates the sum of the corresponding plaintext, that is called additive homomorphic encryption. And when the operation generates the product of the corresponding plaintext, then that technique is called multiplicative homomorphic encryption. The popular RSA algorithm is one of the example of multiplicative homomorphic encryption. [37].

- *Somewhat Homomorphic Encryption (SHE):* This encryption supports both addition and multiplication operation on the ciphertexts. However, the limiting factor of this technique is the number of the supported operations for computation. Mostly this technique supports a significant number of additions but not so promising number of operation for multiplication. This limitation impedes the use of this technique in most applications.

- *Fully Homomorphic Encryption (FHE):* Craig Gentry was the first to bring up with the construction of lattice-based cryptography in 2009 [38]. His technique addresses the limitations of the previous techniques, removing the number of addition and multiplication operations on the ciphertexts. Gentry's construction was able to create Boolean circuits to perform any number of operations required. One of the main drawback of this encryption technique is the computation overhead. There has been extensive research on this topic in the following years with many upgrades with the design to make the algorithm more efficient and usable.

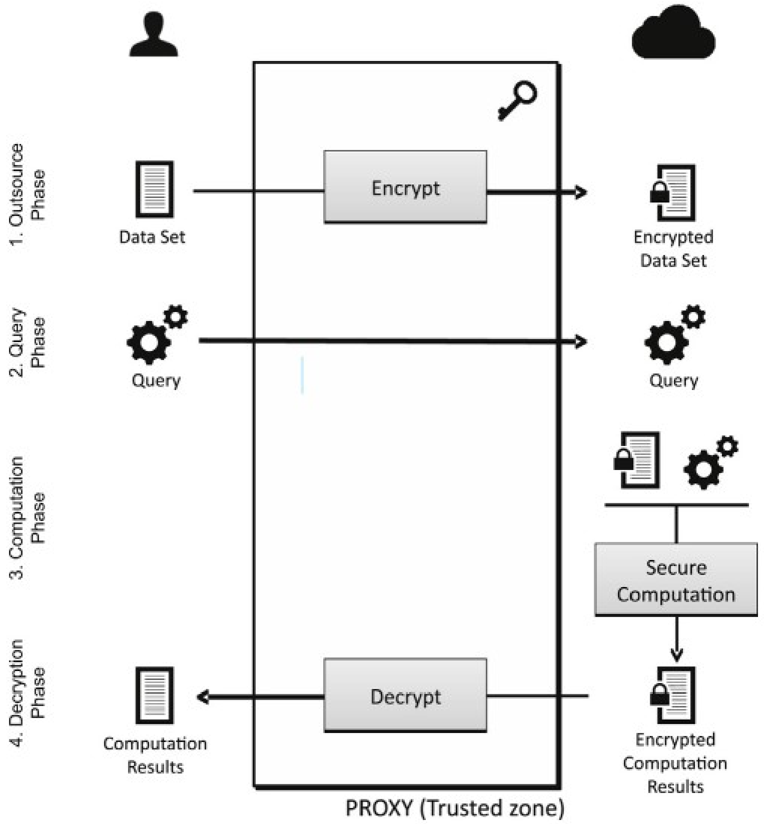


Figure 5.8: FHE scheme for data computation on ciphertexts

5.3.2.2 Multi-party Computation

Multi-party computation is a technique that enables different parties to carry out a computation using their private data without revealing their private data to each other. [39]
Imagine that Alice, Bob and Charlie want to calculate the sum of their bank balances without revealing their actual balances to each other.
First, Alice, Bob and Charlie each encrypt their bank balances using homomorphic encryption.
Next, Alice, Bob and Charlie send their encrypted balances to a third-party, called the computation server, which performs the calculation of the sum. The computation server does not have access to the decrypted data, so it cannot see Alice, Bob and Charlie's actual bank balances.
Finally, the computation server returns the result of the calculation (the average of the three bank balances) to Alice, Bob and Charlie who can then decrypt it to see the result. Because the calculation was performed on encrypted data, the result is secure and cannot be accessed by anyone other than Alice, Bob and Charlie, which are the involved parties.

5.3.3 Access Control Functionality

Many cloud computing applications require a certain degree of data sharing, being log systems, messaging services or file storage, among others. Therefore access control is a critical feature of cloud computing. The following methods shows that access control can be implemented using cryptography.

5.3.3.1 Public-Key encryption

In Public-Key Encryption (PKE) schemes [40], the receiver generates a pair of keys: a public key, which can be posted publicly, and a private key, which is kept secret. The sender uses the receiver's public key in order to encrypt the information he wants to transfer and the receiver decrypts it using his private key. The public keys are either sent to all the senders or stored publicly in a Public-Key Infrastructure (PKI). PKIs certify that the public key correspond to the intended recipient.

5.3.3.2 Identity-based Encryption

It is a type of public key encryption in which the public key of the user is some unique information about him (an email address for instance). No pre-distribution of public keys is necessary, however this scheme requires a trusted third-party, known as central authority, which can be a single point of failure. The central authority handles all the keying material and privately distribute the keys to the involved parties. Identity-based encryption occurs in different steps:

- 1. The first step is for the KG to generate and publish a Master public key as well as a Master private key, which is kept secret, described in figure 5.9.
- 2. If Alice wants to contact Bob, she asks the KG to generate Bob's public key, which is made by combining the Master public key and Bob's email address, described in figure 5.10.
- 3. In order to read Alice's message, Bob has to get his private key, by contacting the KG who will ask for identifying information and combine it with the Master private key, described in figure 5.11.

5.3.3.3 Attribute-based Encryption

This encryption scheme works as the Identity-based encryption scheme. However, instead of encrypting a message to only one user, here the sender is able to encrypt messages to a specific set of recipients, based on their attributes.

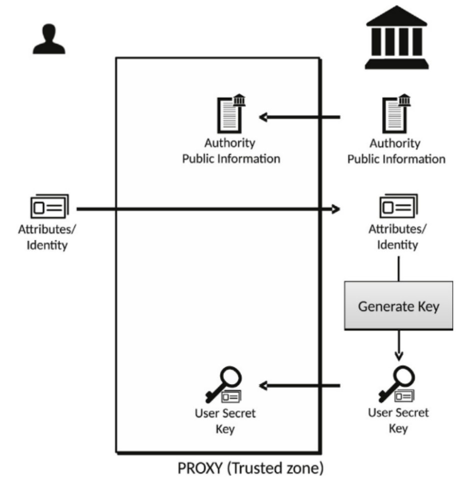


Figure 5.9: Key generation phase for IBE and ABE schemes

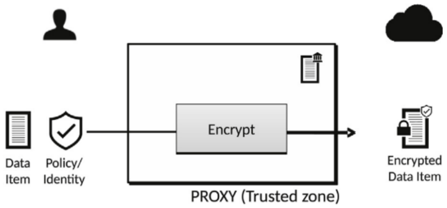


Figure 5.10: Outsource phase for IBE and ABE schemes

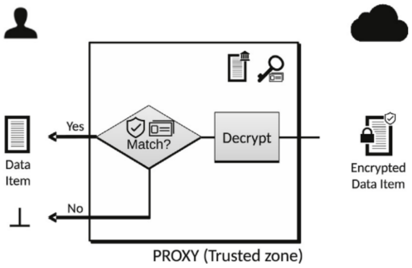


Figure 5.11: Retrieval phase for IBE and ABE schemes

Chapter 6

Relevant Cases

In this chapter, we look at relevant cases that relate to the Chromebook. We dive into each case and highlight what happened and what were the problems. This chapter firstly illustrates a selection of similar cloud computing cases, then talks about the Microsoft Trustee model, followed by Facebook's data leak of it's users, then privacy concerns of the usage of TikTok, and finally the ban of Google Analytics in different countries of EU.

6.1 Cloud Computing Relevant Cases

The Schrems II judgment has made it difficult to transfer personal data to countries outside the EU legally. As a result, since July 2020, many European data controllers have now had to review whether their cloud arrangements are legal. The main concern about these American-based cloud services is the Privacy Shield's invalidation.

The circumstances for using these cloud services are the continuing threat of the American security agencies and laws that permits surveillance. There are numerous ongoing cases of banning or restricting cloud services due to the nature of the processing prerequisite. Google Platform Services and Workspace and Microsoft services are no exception. Of the many cases, some cases stand out. France[41], Germany and Netherlands[42] all had disputes with the use of Microsoft and Google services in recent years.

Firstly, in the Netherlands in 2018, six months after the enforcement of GDPR, the Dutch government longed for Microsoft for its processing activities due to privacy concerns. The problem was about Microsoft systematically collecting data without transparent consent about the individual use of Word, Excel, PowerPoint and Outlook. Later, this year, the Dutch Ministry for Education decided to restrict students' use of Chromebooks in the Netherlands. After confronting Google about the matter, they have promised new updated versions of equipment which would be ready by next year.

Recently in Germany, after two years of a working group debating and reviewing with Microsoft the nature of their processing, it led to the conclusion that public authorities in Germany may not use Microsoft, announced by all 18 German DPAs. Albeit the lengthy talk about changing the conditions of the processing agreement, which it did, the German DPAs still was concerned about subjects' personal data. Furthermore, Google Workspace has also faced challenges regarding the protection of the students' personal data according to the GDPR. Here, the concern lies in the disability to prove adequately how the data is being processed.

Just as in the Netherlands and Germany, in France, the minister of Education urged not to use the free versions of Google Workspace and Microsoft Office 365 in schools, institutions and administrative offices. France is the second EU country to restrict free versions of Microsoft Office 365 for schools. The authorities considered these free services, which stores data in the US, non-compliant with the GDPR. As a consequence, the French DPIA, CNIL, Commission Nationale de l'Informatique et des Libertés, decided to use European solutions that do not transfer data to the US.

6.2 Microsoft Trustee Model

In the light of privacy awareness, Microsoft has promised a sufficient level of compliance for its EU customers. As explained in section 4.2, the US surveillance laws have consistently made it, to some extent, difficult to establish data confinement within EU borders without the risk of transferring the data outside the EU, and by that avoiding illegal access by other governmental agencies. One such effort of Microsoft is to establish local facilities exclusively for locals in EU countries, a Data Trustee model. One of these countries is Germany[43]

In 2015, Microsoft announced a plan to establish new local data centers in Magdeburg and Frankfurt. The data centers would facilitate the Microsoft Cloud services for some of their main commercial services; Microsoft Azure, Office 365 and Dynamics CRM Online, which covers most of Microsoft's services for businesses and consumers. These data centers would be operated and supervised by the independent German company Detuche Telekom which is the data trustee. Oppose to Google's and Facebook's model which intends to keep data centers primarily on US soil, the root of this custom deal is to keep the local cloud traffic local and offer an additional layer of privacy controls.[44] This means that these data centers are isolated from Microsoft's global cloud network and will be under control of Deutsche Telekom, and not Microsoft, making the Deutsche Telekom the data controller By giving German customers the option to choose, although with a price increase of the service, Microsoft will therefore not be the controller. If and when Microsoft requests permission, by either the trustee or by the customer, it's supervised by the trustee.[43].Thus, the Trustee model is one iteration of providing safety and security for information in the cloud.

After 3 year of the collaboration of Microsoft and Deutsche Telekom the deal halted for new customers but continued the current ones. On the cancellation of the deal, Microsoft announced the following; *"Over the past three years, customers' needs have shifted, and the isolation of Microsoft Cloud Germany imposes limits on its ability to address the flexibility and consistency customers desire today."* The Trustee model was to be replaced by the new Microsoft Cloud German regions starting from 2019 which is an attempt to comply to the Cloud Computing Compliance Controls Catalogue (C5) certification in Germany. In the interview with Ole Kjeldsen B, the German option of paying for extra privacy layer was not so popular among cloud customers, and the amount of customers was very underwhelming which may have influenced the decision of cancellation.

6.3 The case of Facebook leaking data

In recent times, one of the biggest setbacks in the technological industry is Facebook leaking user data from a massive 87 million profiles. It started with a Russian American researcher named Aleksandr Kogan working at the University of Cambridge could manage to extract the data with a third-party quiz app application named `"this is your digital life"`. The app was not that complicated asking a series of questions to it's participants. Exploiting a vulnerability in the Facebook API allowed the app to collect data not only from the quiz-takers' profiles, but also from the Facebook friends of the participants without their knowledge. Facebook prohibits trading with user data but with the help of Kogan, Cambridge Analytica captivated the mass data and sold the data anyway. This scenario was more a trust abuse of the users on Facebook rather than hacking. It was more of a wake-up call for everyone that how much users can trust Facebook or any other social sites with their personal data. [45].

6.3.1 Types of Data Leaked

The actual purpose of Cambridge Analytica for collecting these massive amounts of data was to build a psychological warefare tool, that was published to help Donald Trump being elected as President. The tool was expected to perform personality profiling without user permission [46] which is applicable in the digital marketing campaigns. The Facebook server was not hacked or infiltrated for stealing any password or sensitive data. All the stolen data was public in the profile and was gathered from the Facebook user profiles. The app collected all the data by exploiting a vulnerability in the "Graph API", which is an API that interacts with all the incoming and outgoing traffic and allows any third-party apps to integrate with Facebook platform. The API did not have any authentication process to track and terminate if any third-party application is requesting for too many specific information for a user, So this vulnerability in the system let Kogan pull out the massive amount of data of the users. The data included different activities, check-ins, pictures, location, details regarding relationships, religious beliefs, political beliefs, and many more [47].

6.3.2 Consequence of the Data Leaks

There were consequences in different aspects. Facebook had to undergo a lot of scrutinizing of their technical flaws and also respond to the world about such a massive data leak. When Facebook discovered the role of Kogan behind this data leak, Facebook immediately revoked all accesses of his app. Also Facebook requested Cambridge Analytica to delete all the gathered data. Later, when it was revealed that the data was not deleted, then Facebook terminated the access of Cambridge Analytica as well. The company instigated an investigation of thousands of similar third-party apps regarding their access to the platform restricting how much data was visible to the third-party developers, what features any app could access. They started monitoring all the third-party apps that request more than the usual data for their service like list of friends, e-mail addresses, etc. The investigation also included the verification of the identities of the administrators of special Facebook pages and also advertisers who had content related to current debated topics. With the emerging negativity in the market, Cambridge Analytica CEO was suspended. As a result, Cambridge Analytica's ability to do their business declined as they were losing all their clients and finally filed a petition to declare bankruptcy [48].

As the case progressed, the CEO of Facebook Mark Zuckerberg was forced to testify before Congress and Senate. As the case developed there were multiple lawsuits being filed against Facebook. A San Francisco court filed a case against Facebook for breaching the trust of the users. In April 2018, Mark Zuckerberg with his associates had to attend a Senate hearing where lawyers questioned him for hours about the privacy policies of Facebook and scope of advertisements in the platform. Multiple fines were subjected to the tech-giant for violating the laws of privacy of user data. Since then Facebook has been in the spotlight and they were subjected to multiple fines [49]:

- In 2019, Facebook was fined by United Kingdom the maximum possible amount of $644,000, under the law of Data Protection Act 1998.
- In 2019, the Federal Trade Commission (FTC) charged Facebook Inc. for raising concerns regarding their ability to provide sufficient security on the personal data of the users. The penalty was the largest ever in the history for any company, an immense amount of $5 billion [50].
- In 2018, a privacy violation case was filed in San Francisco federal court. The allegation was the company tracked their users' location since 2015 by tracing IP addresses even when the users have turned the location service off. Facebook had agreed to settle this case for $37.5 million claiming that the company used the location for showing personalized advertisements [51].
- The data watchdog of Ireland fined Facebook an amount of $400 million Euros, for failing to protect children's privacy on Instagram which is owned by Facebook. One side of the case demonstrated

that children ware permitted to use the business account in Instagram platform. And few information like phone number and e-mail address of the business account holder is publicly visible which is violating the privacy laws [52].

6.4 TikTok

TikTok owned by the Chinese company ByteDance, is a video hosting service that allows people to upload or keep short videos. This social media platform used by millions of people around the world have created concerns on data privacy and security in recent times. Such concerns are as a result of some terms in its updated privacy policy which allows limited access to a user's data, to some persons in certain countries outside the resident country of the user.

6.4.1 TikTok Privacy Policy

The personal information of subjects that TikTok uses for its processing is collected from

1. Information they provide: This include
   - profile information such as date of birth, username, email address and/or telephone number, and password.
   - Contents created by users and messages sent to or received by others on the platform, as well as when, where and by whom the contents were made are also collected.
   - In cases where payment is required, the user's transaction and purchase history, payment card information, and third-party payment information(e.g. paypal) are collected.
2. Automatically generated information: This includes but are not limited to:
   - The user's device model, operating system, keystroke patterns or rhythms, IP address, and system language. They also collect service-related, diagnostic, and performance information, including crash reports and performance logs.
   - Location information
   - Cookies, usually after getting consent from the user.
3. Information From other sources such as advertising, third-party platforms and partners, etc.

As stated clearly in their privacy policy these information are collected for security reasons, to provide a better experience and important functions for the platform. These functions include storage, content delivery, security, research and development, analytics, online payments, customer and technical support, and content moderation.

6.4.2 TikTok Global Operations and Data Transfers

TikTok stores the information it collects on its users in servers in the United States and Singapore. For its users in the EEA, the United Kingdom or Switzerland, the joint controllers of users' information processed is TikTok Ireland and TikTok UK.

To ensure the running of its global operations, and to provide important functions, TikTok allows limited and secure access to users data by certain entities in its corporate group. Countries such as Canada, UK, Israel, Japan, and South Korea are granted limited remote access to information based on adequacy decision. While Brazil, China, Malaysia, Philippines, Singapore, and the United States are granted access based on standard contractual clauses.

The access granted to China has created concerns over data privacy to countries such as the United States. This is likely as a result of China National Intelligence Law. Article 7 of China National

Intelligence Law states that "All organizations and citizens should support, assist and cooperate with national intelligence work in accordance with the law, and keep the secrets of national intelligence work that they know"[53]. Article 14 also states that National intelligence agencies may request relevant agencies, organizations, and citizens to provide necessary support, assistance, and cooperation to carry out intelligence work in accordance with the law[53]. Referencing this, CNN Business, Washington reports that US policymakers are speaking up that the Chinese government could pressure TikTok or its parent company, ByteDance, to turn in personal data of users under its national security laws[54]. This is despite the statement by TikTok in its privacy policy, that the access to users' data within its corporate group applies specifically to users in the EEA and/or the UK[55].

Implications on Data Protection

A study was conducted last year by researchers from the Centre for IT and IP Law of KU Leuven, for the European Data Protection Board(EDPB) on government access to data in third countries. The study looked into the PRC Constitution, its secondary laws and Personal Information Protection Law(PIPL). It was discovered that certain assumptions in the Western legal system are not applicable in China. These include the regulation and constraint of public authorities by the law, limitation of the government on access to personal data, the people having rights against the government and the ability of citizens to object to certain decisions of the government[56, 57]. Additionally, Article 3 of the PRC (People's Republic of China) constitution states:

> "[...] All administrative, supervisory, adjudicatory and procuratorial organsof the state shall be created by the people's congresses and shall be responsible to them and subject to their oversight [...]"

Article 1 of the constitution of The PRC states that the PRC is led by the Communist Party of China (CCP). It is clear from Article 3 of the constitution quoted above that the National People's Congress creates and is in control of the legislative, executive and judicial system. And the NPC is directly supervised by the government and CCP[58]. This makes clear that there is no separation of power in the PRC, nor is there an independent entity that controls or restrains the government's access to data. Based on these facts, it is also argued that the Chinese government is said to have no restrictions when requesting companies to provide access to personal information [57].

6.5 Google Analytics

Google analytics is a web analytic tool that collects and tracks web traffic with the aim of analysing it, measuring its performance and making better decisions[59]. It is one of the many online services owned by the American multinational technology company, Google LLC.

Google analytics 3 (Universal analytics) has a feature anonymize_ip that enables anonymization of IP addresses. This is not by default but is optional. A website owner may choose to anonymize the IP addresses of its users. When this choice is made, the IP addresses of users are anonymized once they are received by Google and before they are stored. Google analytics has designed the anonymize_ip feature to help website owners comply with the various data protection regulations in their states or countries. Nevertheless, it is the responsibility and decision of website owners to make on whether to anonymize the IP addresses of its users or not[60].

In an effort to secure user data and web traffic, Google uses an encryption protocol called HTTP Strict Transport Security (HSTS) over browsers that support HTTPS [61]. However, a number of Data Protection Agency in EU members states have decided on the discontinuation of its use, as it is not in compliance with the GDPR. The first to do this, is the Austrian Data Protection Agency or Datenschutzbehörde(DSB). On a complaint filed by a data subject in August 2020 against a website provider (employing the services of google analytics) and Google LLC, the Austrian DSB came to a ruling. It held that according to Article4(1) of the GDPR, the data transferred to Google LLC by the website provider, namely: user identities and IP address, constitute personal data, as a data subject can be identified using these. Additionally, despite the signed SCC between the website provider and Google LLC, Google does not provide adequate protection of the personal data of the subject. One reason for this is that Google is subject to surveillance by US Intelligence services according to FISA 702. And the measures it has in place does not prevent surveillance and access to data of EU data subjects by the US intelligence service. Thus, the Austrian DSB considers the use of Google Analytics as unlawful unless additional measures are put in place for the protection of personal data of data subjects[62]. Following this, other EU states such as the Danish, French and Italian Data Protection Authority have a similar decision on the use of Google Analytics[63]

6.5.1 Google's Attempt To Solving This Issue

In this light, Google LLC is introducing Google Analytics 4(GA4). In GA4, the IP address of EU users is not stored or logged. But if a client requests for an IP address, the IP address is anonymized. When Google Analytics obtains the IP address of an EU user, it is only used to derive the geolocation and device data such as city (Latitude and Longitude of city), browser minor version and User-Agent string, device brand, model and name, OS minor version, platform minor version and screen resolution. As soon as these data are obtained, the IP address is discarded. However, these data are obtained by default, but the website or application owner can choose to disable them[64].

In summary, Google Analytics is only a product or service offered by Google. To ensure the privacy of users, it does not collect certain information about a user which it views as PII for example, email addresses, personal mobile numbers, and social security numbers[65]. But certain things might require a user to provide such details on a website employing Google Analytics. Therefore, it is the sole responsibility of website or application owners using this service to implement the necessary steps. These could be enabling or disabling some features in Analytics, or even more on their one website such as enabling consent banner, or not sending personal data among Analytics data to google [66, 65], among others.

Chapter 7

Case of Chromebook Gate

This chapter investigates the Chromebook-gate case. At first we give a brief overview of the Google Workspace for Education (GWfE) and then the development of the case where we also reflect upon the four verdicts of the case till present.

7.1 Chromebook-gate

The use of computers in elementary schools has been increasingly integrated into the teaching program in Denmark, specifically Google's Chromebook laptop running Chrome OS. In fact, almost half of Denmark's elementary school use this type of laptop with a collection of Googles services and programs for education purposes ie. Google Workspace for Education.[67] This includes Google Classroom, Google Drive, etc. In some cases, the collection of software Google provides is the core building block in the teaching program of the elementary schools. With the rising trend of using computers as a core function is as convenient and rewarding as it is (might be) complicated.

However, as any controller or processor doing business in EU, Google's Workspace must comply with the GDPR, which is explained in Section 4.1. So where did it went wrong using Google Workspace? - Before diving into the on ongoing case of Elsinore and Datatilsynet, lets first visit tool of Google Workspace.

7.1.1 Google Workspace for Education - A Brief Overview

Google Workspace is an all-around productivity tool for businesses and institutions that want to use Google services. Workspace includes the many known free services from Google Cloud Platform (GCP), such as Gmail, Google Calendar, and Google Docs. A series of Google Workspace standard series of in Figure 7.2.

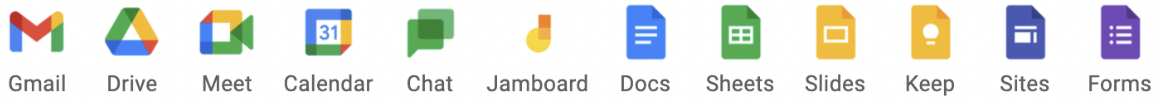


Figure 7.1: Services every version of Google Workspace includes

Since 2015, Google has offered a free version of Workspace for qualified educational institutions, which includes tailored applications for education purposes called Google Workspace for Education (GWfE). At the start of 2021, with over 170 million students enrolled worldwide, GWfE, formerly called G-suite for Education, announced a name change, new features, and new GWfE editions to choose from according to institutions' needs[68]. This report will mainly focus on Google Workspace for Education.

Workspace for Education requires each student to have a Google account as well as access to a Chromebook Laptop. A Chromebook laptop is a computer that runs a Linux-based operating system called ChromeOS. Typically, every Workspace student acquires a personal Chromebook device for usage in school as well as at home usage.
For every Workspace environment, there are the roles of the administrator. The administrator's role is to create and maintain a school class environment on the administrator's page according to educational purposes; this includes setting up classes and configuring which Google services and functionality are available for the students. [69].

Oppose other Workspace editions, GWfE does not include the standard services Client-Side Encryption, Currents, Google Cloud Search, Google Workspace Migrate, and Workspace Add-Ons, but includes Assignments, Classroom and Chrome Sync as Core Services.

To expand the possibilities of GWfE, Google offers paid versions of GWfE. Educational institutions pay monthly for each student enrolled, the paid subscription extends the services such as storage for each student or additional administrative controls. The three subscription plans are listed below.[69]

- "Google Workspace for Education Standard"
- "Google Workspace for Education Teaching and Learning Upgrade"
- "Google Workspace for Education Plus"

Every service and functionality which is included in GWfE Fundamentals are included in the paid subscriptions. An overview of the content of the paid editions is illustrated in Figure 7.2. The four editions offer a variety of functionality according to institutions' needs.

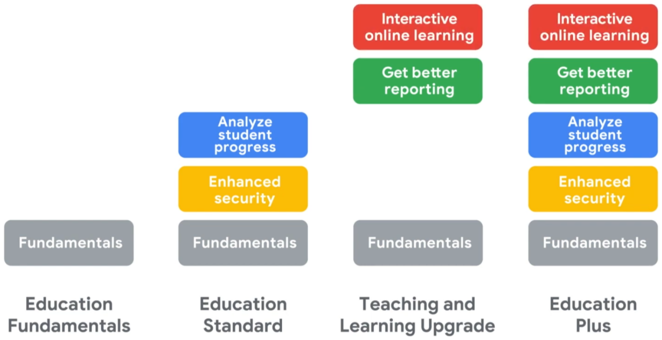


Figure 7.2: Differences of Google Workspace for Education paid editions[70]

7.2 The development of the Case

In the following section, we will investigate the development of the case. Today, there have been four verdicts on the Chromebook case of Elsinore, followed by several recent remarkable events. The cases' development from the first and second verdicts is explained, followed by the current state of the case. We start with the origin of the problem.

The Danish DPA received a complaint in December 2019 regarding a violation of privacy by Elsinore municipality, followed by a notification submission by the municipality itself. The complaint referred to the school in Elsinore creating a Google account while processing students' personal data without parental consent. Consequently, a child's information appeared in a comment on Google's video platform Youtube, unwillingly by a minor child. When the Danish DPA receives the complaint and a request from the municipality, The Danish DPA initiates a case to investigate the use of GWfE at Elsinore municipality. [71]

The news of an initiated Chromebook case starts to spread, making other institutions using GWfE suddenly turn to the Danish DPA with questions. These inquiries led to the Danish DPA recognising a pattern and, as a result, began assessing the cases as one. Specifically, some institutions were cautious because, in those institutions, YouTube also was used in some form. Along with around 50 municipalities, the Danish DPA began investigating the cases but focused a great deal on Elsinore municipality as they were the ones furthest ahead, and spearheading the case.

However, in light of the initiation of this case, some municipalities did not stop giving Chromebooks to primary school students. At the start of schools in August, Aarhus Municipality issued 24.000 Chromebooks pre-installed with GWfE to students in grades 2 to 10.[72] Knowingly neglecting the concerns for third-country data transfer, Ole Hersted Hansen, digitalisation chief for Children and Youth in Arhus municipality, states that they cannot stop using IT equipment from day to day. They assessed the likeliness of US intelligence agencies requesting students' personal data as being low.[73]

In the meantime, the schools of Elsinore municipality stopped using additional services, ie. Youtube, and therefore not obligated to make a DPIA. [74]

7.2.1 1. Verdict

The first verdict from the Danish DPA arrived on the 21st of September 2021. The DPA stated that the municipality is the data controller and, as the data controller, was responsible for using the IT equipment and software, in this case, Chromebooks and Workspace, according to the laws of GDPR. The Danish DPA ordered Elinsore municipality to devise adequate documentation of using Chromebooks in its schools with a submission deadline of the 1st of November. The documentation should include a not yet made risk assessment and appropriate additional documentation relating to the processing nature, suggesting DPIA(konsekvensanalyse). Furthermore, the Danish DPA also warned Elsinore municipality that the processing of GWfE personal data would not be legal without making a DPIA. The DPIA should address the risks of processing students' data reduced to less than a high risk for the privacy rights and freedoms of the data subjects. The order was not without attached critiques and concerns about the municipality's processing of personal data. If the municipality could not provide the documentation, they should stop using GWfE. [75]

The Danish DPA states that the individual municipality's task is to do the necessary assessments when implementing tools and software into the student program. Elsinore, in this case, needed to conduct the necessary documentation of the enrolled student's usage of Chromebook and GWfE. According to the Danish DPA, the missing assessments caused several violations of the GDPR and refer to the laws of elementary schools of Denmark for processing data of students.[75]
Furthermore, the Danish DPA also warned Elsinore municipality that the processing of GWfE personal data would not be legal, especially without making a DPIA. The DPIA should show that the risks of processing students' data using GWfE were reduced to less than a high risk for the rights and freedoms of the data subjects, which they have yet to be able to do.

If the risk assessment that the Elsinore municipality was ordered to conduct showed a high risk for a violation of the privacy rights of the students, and the municipality had not, before the deadline period, reduced these risks to a level less than high, the processing would be banned.

7.2.2 2. Verdict

Since the first verdict, not without dialogue between the municipalities and the Danish DPA, the second verdict arrives on the 14th of July 2022. The documentation Elsinore assembled was based on the processing of personal data based on GWfE. The Danish DPA applauses the municipality for the effort of mapping how the processing occurs, but at the same time, it also highlights the data protection issues using big tech companies. Again, the Danish DPA criticises the municipality's ability to process personal data.

The DPA argued in their first order that Elsinore municipality should make a risk assessment of their processing activity, which reflects the flows of students' personal data that the data processing involves in using GWfE. The risk assessment should address the lawfulness of using Chromebooks and GWfE according to Danish primary school law, which the municipality requests upon the students.

However, the second verdict resulted in a suspension of Elsinore municipality carrying out all forms of third-country data transfer without an adequate level of data protection. Furthermore, the suspension includes a general ban on data processing with GWfE until adequate documentation and a DPIA until the data processing conforms to the GDPR. This means a ban on using GWfE in the schools of Elsinore municipality altogether.
The banning of Chromebooks and GWfE would take effect immediately. However, Elsinore municipality was granted a deadline of the 3rd of August 2022 to withdraw, terminate and delete users as well as already transferred information.

The Danish DPA notes that many of this decision's conclusions probably apply to other municipalities that use the same GWfE configuration, although they were not ordered a suspension using GWfE. However, the Danish DPA expects these other municipalities using GWfE to take appropriate steps based on the decision - even if the Danish DPA was finalising a series of cases concerning said municipalities at the time.
However, within the deadline of the Danish DPA's order, Elsinore sent a revised DPIA to the Danish DPA on the 1st of August [76]. This DPIA can be seen here.[74]. In the DPIA, Elsinore states that this DPIA gives a basis for future students' usage of Chromebooks.

However, a few days before the start of schools in Elsinore on the 3rd of august, the City Council of Elsinore municipality has an emergency meeting to address the Chromebook ban. The City Council acknowledges the consequences and decides that only the teachers can use Chromebooks at the start of the school and await a decision from the Danish DPA.[77]
In light of the disarray of the situation, a new meeting was held by The National Association of Municipalities a few days later, which invited several municipalities to listen to a presentation given by the Danish DPA about recommended proceedings of the case. [78]

7.2.3 3. Verdict

On the 18th of August, based on the new material sent by Elsinore municipality, the third verdict of the Danish DPA arrived. It is the Danish DPA verdict to maintain the ban on using Chromebooks and GWfE. The Danish DPA believes that processing students' personal information still entails a probable violation of the student's rights. In addition, the revised DPIA does not live up to the demands of the Danish DPA. For example, in the third verdict, the Danish DPA writes that Elsinore municipality did not assess relevant risks and, in other parts, only asses partly the necessary safety measures.[79]
The Danish DPA reminds Elsinore that if they can recognize the high risks of using Chromebooks, then the Danish DPA is ready to aid the municipality with a plan to legalize it.

7.2.4 4. Verdict

However, on the 8th of September, 21 days later, due to a continuous dialogue between the Elsinore municipality and the Danish DPA, they agreed to suspend the ban for two months. The students would get their Chromebook back for two months until the 8th of November. The Danish DPA admit that many other municipalities use GWfE, which are under the similar processing challenges.

The Danish DPA states in its announcement that Elsinore has shown serious commitment to solving the problem by describing what needs to be achieved. This commitment also includes starting a process of talking with Google to shed light upon the specificities of the processing agreement. Ultimately, if the municipality cannot assess or change the processing nature of students' personal data, the Danish DPA will ban it.

Again, the Danish DPA asks for a revised DPIA to be sent by the end of the ban's suspension. With no time to waste, Elsinore municipality sends the DPIA plus notification of the dialogue with Google. Recieving the DPIA, the Danish DPA states they will have a conclusion by the end of the year.

7.2.5 Current state of the Case

The Chromebook case has been developing for years, and articles and announcements are still reaching the surface. As of the 14th of December, the recent announcement of the Danish DPA states that, on the basis of several municipalities sending newer documentation for the Danish DPA to review, the Danish DPA has now extended the deadline until the 23rd of January.[80]

Chapter 8

Analysis

In this chapter, we do an in-depth analysis of the Chromebook case. We start by analyzing the interviews we conducted, followed by our analysis of the case itself, where we thoroughly describe the problems we found. Subsequently, we propose a privacy enhancing framework and apply it to different cases we have already discussed in Chapter 6 and 7 to investigate if the framework can address the issues of those cases. Lastly, we recommend solutions that we think could solve this Chromebook case.

8.1 Analysis based on Interviews

We have been able to have two interviews regarding the burning issues of all the cases. The two interviewees are experts in their respective fields. The first interview we conducted was with Ole Kjeldsen, the director of technology and security at Microsoft, Denmark. He enlightened us with many ongoing issues regarding privacy and, how Microsoft is dealing with all the challenges, how effective and promising the solutions Microsoft has implemented over time. The other interview was with Allan Frank, the ICT security specialist and lawyer at Danish DPA. This interview has been precisely about the Chromebook case, the problems, the role of the Danish DPA, national laws and foreign legislation coming into effect. The key takeaways from both interviews are highlighted below:

8.1.1 Interview with Ole Kjeldsen - Microsoft

In our interview with Ole Kjelsen, we discussed topics linked with Microsoft, such as the EU Data Boundary project and the trustee model they had with a German company; and other non-Microsoft specific services such as the Chromebook case and foreign legislation. The quotes that we use in this section are from the Appendix B and C.

Data Collection for Product Development not Marketing

Data collection is a trivial process nowadays. It seems to be near to impossible to find any company who does not collect any data from the users. The companies collect the data from the users for their business growth. They promise to use the data for analytics to improve the user experiences. Ole challenged this practice of collecting user data is common among all companies and considered it lawful in the interview stating:

> "Danish companies who are providing apps to municipalities and when I read their privacy terms, even though it's five guys in a basement somewhere in their privacy terms are all saying we reserve the right to use the data you create"

It is very obvious form his statement that even a small company is also collecting user data. But later he brings up the most important point which is "what kind of data" is allowed to be collected. He specifies clearly that the data that users put in the applications are not collected, the logs of data, data about the pattern of consumption by the users of different features of the application. Ole indicates the importance of these collected data towards the growth of any company by saying the following from the perspective of those companies:

> we will analyze and use for our business granting for our product development. We cannot do marketing and all that, but we can do product development. We gain some knowledge about how our service works, how you use it. We will use that for our own purpose, typically what they will refer to as a user experience. It is for the customers' benefit and it is."

It becomes very obvious that Ole thinks it is crucial to get insights from the user data for better product development but he also meticulous mentioning about the marketing and profiling on users with that data. He explicitly said that later:

> "I think it's unlawful if you do marketing, if you do profiling all that, that is what GDPR is all about."

Microsoft's Approach to Data Collection

From the discussions above, it is certain that Microsoft also collects data. Regarding this, Ole asserts that Microsoft does not collect and install data from the users commercial services. He mentioned that:

> "... A municipality using Microsoft 365 for their email, intranet, sharing, online meetings, all that for those services. Microsoft does not collect, install data."

Ole further points at the log data from the users that is collected by MS. He clarifies the collected log data is not the content of operation done by the user but the events from the user. For example, Microsoft does not collect what e-mail a user is sending or who is the receiver but just the log data. Ole explained what is log data stating:

> "They do collect logging data, so whenever Ole logs on it happens at a given point of time, from this IP address, synchronized this amount of data. That is a log entry"

The collection gets more interesting when Microsoft is the data processor. They need more information to provide specific services like invoice. For invoicing, Microsoft need to know how many unique users are using the which services, how many transactions are happening, the amount of data going back and forth. He assures that this is handling of personal data under legitimate business operations under GDPR. He says:

> "There are four or five of these legitimate business operations where we do collect data."

For these operations, Ole mentions about the technical and security measure taken to keep the data safe. They apply Hashing of 256 bit characters and aggregate the data, pseudonumize the data. Concluding this topic Ole mentions about Microsoft's participation on profiling or marketing and the reason for collecting the data:

> "We can't profile, we can't do marketing, we can do capacity planning, we can fix errors, we can make sure there are no security vulnerabilities. It is very clear from our DPA what we can and can't do with this data."

4 key Factors for Microsoft's Data Transfer

The transfer of user data is a very crucial concept for this project. We discussed the reasons of Microsoft's data transfer with Ole. He has mentioned four scenarios for the data transfer and they are:

- **Support or Operations outside EU:** The CSPs provide user support 24/7. So when a customer in EU wants user support and someone from US provides that support doing remote access. The person can access the data. That is a potential case for data transfer. Ole mentions about the idea of lockbox which is an interface where users can see the requests for their data. They have the choice to accept or deny it. If the users denies the request, then he might have to wait for someone to provide the support within EU.

  > "We have one called customer lockbox. It's a service we built about 10 years ago saying if that happens when he needs to do this, he would be able to see the customer's data"

- **Microsoft's Business Continuity:** One of the key characteristics of cloud services is availability. Even there is a catastrophe in any of the EU country, all the services will still be available. Microsoft will change the resources to provide services from that country to any other within EU. Ole states about this:

  > "We are certified on this as a separate ISO standard for doing business continuity. If we have business continuity, all help break loose in Ireland, we have ways of making sure the service available inside. So it will move to Frankfurt, it will move to the UK, which is still a safe third country. We have so much capacity in the business. Continuity is not a problem."

- **Law Enforcement Order:** CSPs need to transfer data when law enforcement agencies request for data of any individual or a company. Ole clearly defines the stand of Microsoft regarding this issue:

  > "We want to serve the police and intelligence agencies. If it's a proven terrorist orientation or a human trafficking organization, we don't see that as a violation of GDPR. So of course we can limit the privacy if it's criminal intent."

- **Logging of User Data:** The importance and practice of logging user data is already mentioned in the first point. Ole recognizes the significance of analyzing those log data for analyzing any security breach happening. Microsoft have Cyber Defense Operation Center department who are looking for patterns in signals to decode any cyber threat. He states that:

  > "For security we process security signals daily, we are letting the machines analyze that, looking for patterns. If there is a side attack happening in Tokyo at the moment using a tool. We want to have more resilience in New york or Amsterdam because the attack might spread into the rest of the locations."

  He also added:

  > "Data transfers are not unlawful. You can still do them. You just have to take your precautions. You have to assess is this happening within the, the frame of the law and , in our case, we would stipulate absolutely it is."

Foreign legislation

When asked about foreign legislation and the reach of American legislation, Ole Kjeldsen mentioned their ability to fight it.

> "The intelligence services, they don't want to go through us. They know how hard it is. They know they're gonna be met by 140 lawyers who are gonna challenge them every step of the way."

It is interesting to note that he did not talk about CLOUD Act which is extra-territorial and more far reaching, especially for European subsidiaries of American companies, than FISA 702.

Alternative solutions

Ole Kjeldsen did not want to pronounce himself on alternative solutions other than Microsoft ones and outlined:

> "I believe a customer would be able to implement Microsoft 365 Education in a compliant manner."

In this statement, he implies that it is not the product itself which is not compliant, but its implementation.

8.1.2 Interview with Allan Frank - Datatilsynet

In our interview with Allan Frank (see Appendix), we discussed different themes such as the Data Protection Agency in Denmark and its role, foreign legislation, the Chromebook case as well as possible alternative solutions. The quotes that we use in this section are from the Appendix E.

The Danish Data Protection Agency, its roles and processes

For the first theme, we learned a lot of things about the Danish Data Protection Agency, its roles and processes. The DPA is the competent authority by law, as stated in chapter 6, article 51 of the GDPR. The DPA focuses on the laws that hold issues around the protection of human rights within personal information, so both GDPR and National laws. The Danish DPA receives around 400 new cases every week and, even though not all cases are investigated thoroughly, they all get a decision. The cases that present the highest risks for the individuals are investigated and the ones that take too much resources to investigate or are minor infringements are sorted out. The Danish DPA has a decentral way of working, meaning that case handlers have some responsibilities and can decide in some cases. It is supervised throughout the hierarchy until a director from DPA makes a formal decision. Allan Frank also states that the Danish DPA is held in very high esteem in the European family of Data Protection Agencies.

> "I think that we have a very high esteem, making very good law decisions and having a very good way of communicating our decisions to the public. And we are the DPA in Europe that has most published decisions, by far. So they (the other European Data Protection Agencies) are quite happy with us because normally when they get a case, they can take a Danish decision and then they can transcript what we did."

Foreign legislation

For our second theme, we chose to talk about foreign legislation. When asked about his opinion on American surveillance laws, Allan Frank states that we have a double standard regarding surveillance in Europe.

> “one, have to admit that the rules in Chapter 5 in GDPR, the rules about foreign transfers, is a little bit of a double standard because within the GDPR, the way that the secret law enforcement is done is exempt from the GDPR. So in Denmark, Politiets Efterretningstjeneste(PET), Forsvarets Efterretningstjeneste(FE), they are not, they don’t have to abide by the GDPR. And now we are telling the US to adhere by a standard that even our own secret services, shouldn’t adhere to.”

He voiced concerns about the FISA 702 and the CLOUD Act. FISA 702 is concerning because how US Intelligence Agencies collect data about foreigners is under secrecy. CLOUD Act is also problematic as it’s extraterritorial and applies to US companies - and their subsidiaries, even if registered abroad. With that law, US Agencies can force companies to hand over data stored on European servers despite it being prohibited by GDPR.

The Chromebook case

Our third chosen discussion theme was the Chromebook-case. He confirmed our understanding of the case and agreed on the four problems we extracted from our case study.
He stated that the case was strongly caused by Google's business model.

> "I would like to emphasize that a lot of this is going to Google's own fault because the software they have developed originally was designed to gather people's information to sell us, yeah, white sneakers or brown shoes or something like that. So all their software originally was built that way. And when used in unison in the technology stack, they are still dripping out data everywhere because there are leaks everywhere in the code designed to benefit the Google model".

However, he also told us that it's the data controller's job to research how data is being processed:

> “the data controller should be in control of all the processing being done with the citizens' data. [...] And being in control is knowing what you're doing with the data at every stage of the processing being done.”

The content of this important part of the interview is further discussed in section 8.2.

Alternative solutions

Finally, we discussed possible alternative solutions. He agreed that the Data Confinement Framework was a plausible solution, and confirmed that some of the techniques we discussed in Chapter 5 are being researched and may be used in the future.

8.2 The Case of Chromebook in Elsinore

This section goes into details of the four core problems we identified by investigating the Chromebook-gate case. We mention the four problems next and we discuss in depth about each of them. We also reflect key takeaways for each of the problems from the interview with Allan Frank.

8.2.1 The core of the problem

- Lack of Risk Assessment
- Lack of control of support scenarios leading to data transfers to outside EU
- Assuming Google processing agenda
- Lawfulness of sharing identifiable data on students.

Lack of Documentation

In many ways, Elsinore municipality's ability to provide fulfilling documentation has been underwhelming. Like many other municipalities, Elsinore did not make an initial risk assessment of any kind at the initial purchase of Chromebook computers or the GWfE software. This practice of not doing some sort of risk evaluation is not uncommon. Danish Business Authority, in pursuit of helping small to medium-sized companies, states that only 42% of SMV companies do risk assessments for their IT usage.[81] This was no exception the case for the usage of Chromebook laptops and the GWfE software. Allan Frank recognizes this pattern from companies and institutions utilizing big-tech companies, stating;

> "And that has been the problem with some of the big vendors, not Microsoft as such, but other vendors as well. We are just bought in to a service and, and, and says, okay, this solves my business problem. But we have not, we have not walked that step further and, and been in control of what is happening in that black box over there. A lot of processing is going on in there, but I'm only interested in the results as, as a controller. But the GDPR tells you that you have to be in control with all the [00:39:00] processing being done, even though you only care for the results so to speak."

At the start of the case in 2019, the DPA's interest formed somewhat unexpectedly, as the complaint of Elsinore municipality was the concern of a child on youtube. The Danish DPA quickly uncovered some additional challenges. Regarding the initial assessment of the complaint, Allan Frank states;

> "..the problem being that we had this complaint for, from a parent in Elsinore municipality. And when we got into that, the municipality themselves, quite frankly, stipulated that they have not made any risk assessment about this."

Allan Frank did not address whether the majority of the municipalities which use Google services, which is about half of Denmark's municipalities, did any risk assessment before buying, but this was the case of Elsinore municipality. But as the other municipalities joined the conversation, Allan Frank, referencing municipalities' ability to choose their own GWfE configuration, continued saying;

> "..the problem is that we could have 50 different ways of doing things, and we had maybe not 50, but 30 different ways of implementing because there's a lot of configuration opportunities within the Chrome stack itself."

As a consequence, in order to be able to assess all already established GWfE environments, the Danish DPA allowed themselves to create their own version of GWfE. Additionally, when explaining the Danish DPA's own initial assessment of the GWfE environment, Allan Frank says;

> "...when we assessed this, we took the strictest way of configuring the system. And even though we did that, we still found problems. ... We assume that every municipality and uses the strictest version of a configuration. But on top of that, we have to do more to be certain that the GDPR is adhere to. ... then you, you(the municipalities) are going to fix the rest.

Allan Frank states in the above quote that, as many of the municipalities may have a different configuration, in their assessment of GWfE, they choose the most strict configuration possible. Allan Frank expresses this in some sense as the benefit of the doubt. As the municipalities had little assessment to display of the initial purchase, the Danish DPA had little material to asses, so they assumed every municipality uses the strictest configuration possible of GWfE as a start.

After the Danish DPA's first and second verdicts, Elsinore's ability to adhere to the Danish DPA's rulings and expectations has been troublesome. Specifically, after the first verdict, the Danish DPA advised Elsinore municipality to construct DPIA considering the nature of the processing. Elsinore did not make the DPIA one until the second verdict, the banning of GWfE of the Danish DPA. Subsequently, due to the quality of the documentation, the chairman of the IT political association, Jesper Lund, at the time of banning the Chromebooks in July, stated that he understands the challenge that school leaders and teachers in Elsinore are facing but that he believes that the municipality has ignored the problems for several years.

Furthermore, the processing nature of using Chromebook and GWfE can be troublesome, so a company called Privacy Company did a DPIA on the Enterprise edition of Google Workspace, which can be seen here[82]. As a comparison, with Elsinore's DPIA sent and Privacy Company's DPIA, there are obvious differences in the thoroughness, size, and quality.

In summary, the first of the problems identified is the lack of risk assessment and additional documentation needed for using Google equipment and services. As a final remark on this problem, Allan Frank states it clearly:

> "..they should have done a risk assessment. They should have done a DPIA and by doing so, they have, they should have seen a lot of other problems and all the problems that come after that they stem from not doing a risk assessment, not doing a DPIA.

Lack of control of support scenarios leading to data transfers to outside EU

Institutions that use Google services, specifically GWfE, may need some form of Technical support. This may include transferring data required to solve an issue to the office's location, which provides support, whether Google in Ireland or Google in the US. In the case of GWfE, Google uses the Follow-the-sun workflow model that dictates which offices are available according to the open hours of Google technical support worldwide.

However, as GDPR states, when a data controller needs to send data anywhere, even nationally, they need an "overførselsgrundlag" or transfer basis. In the case of Elsinore, when support scenarios are needed that would require sending data, they need a basis for data transfer. This must be the case in every case as a data controller. Referring to the data controller needing the legal basis for processing data, i.e. transferring data, Allan Frank states;

> "..99.9% of the cases, I have a legal basis for processing data. That doesn't make 0.01% (rest) legal.

Until July 2020, that basis for transfer to the EU-US Privacy Shield agreement, as explained in Section[Section Privacy Shield], the Schrems II case invalidated the Privacy Shield, i.e. invalidated the Data Processing Agreement(DPA). Going forward, any third-country data transfer to a third-country must occur on another basis than Privacy Shield, i.e. the SCC's.

While Elsinore municipality diligently chose a setting of having the GWfE data in data centres located within the EU border, this is not the case 100% of the time. When in fact, when support is given from an unsafe third-country, some information is processed. In the Danish DPA's first verdict, referring to support scenarios, they state

> "...the data processing agreement states that information transferred to third-countries in support situations without the required level of security."

The above statement refers to situations where GWfE support needs to be given, and that support would be provided from a third-country outside the EU which does not acquire the required level of security.

By the time of the banning of GWfE in July, Elsinore municipality provided the DPIA. The DPIA addressed this issue slightly, but not enough, according to the DPA's verdict. In that DPIA, Elsinore municipality presented a concern about Google's practice of handling subprocessors, i.e. subprocessors in support scenarios. Google explains that, first of all, these scenarios are never initiated by other than a data controller.

When Google works with a subprocessor, they go through a "rigorous selection process to ensure it has the required technical expertise", according to Google. From this, Elsinore suggests providing Google guarantees saying Google does not process information other than data controllers' needs. It is, therefore, Elsinore municipality's assessment that the measures implemented mean that the probability of the risk of privacy violation, in reality, becomes a low risk.

Elsinore municipality, accordingly, evaluated that the basis of data transfer to the third-country is in the form of the Standard Contract Clauses and is effective enough given the nature of the transfer, including an assessment of whether there is legislation or convention that would go against the Standard Contract Clauses agreement.

The problems here lie in the aftermath of the Google architectural processing structure, the follow-the-sun model. Elsinore cannot guarantee low risk regarding personal data in every case of data transfer in support scenarios.

Not a Google Purpose

Given the nature of the Google model, which is data-driven, it is essential to know what data is being collected and processed. Elsinore municipality has yet to demonstrate an understanding of those risks that come. It is relevant whether there have been cases where Google processes personal data for other purposes other than the legal or expected purpose, even if the data controller, Elsinore municipality, has instructed it or not. There may also be cases where the data controller does not have the necessary control over the processing of the information. The Google infrastructure and terms and conditions on their services can be hard to understand and, in some cases, incomprehensible, even.

Google is known for providing services for free, where the ability to process data yields the dividend. Google may process information as it does, using the data for advertisement, platform, etc. Nevertheless, this is different for EU subjects, especially for Elsinore municipality students. It is limited to which data is allowed to be collected and used and for which purposes.

When talking about how the limitation in the processing of students' data, Allan Frank states;

> "...even though we are not even talking advertisements or something like that. That would be a big no-no. But for one example, the way that Google makes their software better if they use the children's data to that, that's not allowed either."

In the above quote, Allan Frank states which restriction exists on the data the students generate. It is the Data Protection Agreement that dictates what measure is allowed to be taken between the parties. However, the data controller nevertheless has to ensure the rules apply to the data. Elsinore has to consider all types of user data that could be used or processed by Google, such as service data[83]. Service data is another type of data that Google collects and processes. Service data is personal information google collects or generates of a user when provisioning or administering cloud services or providing technical support.

Moreover, Allan Frank states;

> "There were a lot of problems about the contractual situation with Google in this case because Google in their contract says, yeah, okay. We are using the data, some of the data, not the content data, but some of the meta-data generated by the children."

Furthermore, in an interview with Version2[84] Frank states that one must not blatantly trust its supplier but recognise its own interest and get another competent and objective opinion on the matter.
The Danish DPA has assessed that Elsinore municipality simply cannot completely rule out that Google breaks the contractual obligations and uses personal data for marketing or other unintended purposes for which Elsinore municipality has not given instructions.

Lawfulness of sharing identifiable data on students

Every primary school is subject to the Folkeskoleloven or Primary School Act which includes primary schools' purpose, teaching content, and structure, to name a few. While Elsinore municipality must adhere to GDPR, they also must adhere to the national laws of Denmark. When a municipality like Elsinore chooses to give Chromebooks to students as learning material, it must be in conformity with the Primary School Act, which may be problematic.

Allan Frank states on the subject;

> "Every municipality in Denmark can choose from, from themselves. And every school within one municipality have a lot, a wide range of different choices that they can do. It's up to the school themselves, but the municipality is as a whole, they are the ones responsible under the primary school law."

Allan Frank states here that a school can choose for themselves; this includes IT equipment. This is apparent for about half of the schools in Denmark which use Chromebooks and GWfE. However, it is the municipalities role to ensure that the children's information is not utilized for purposes other than those permitted by the Primary School Act. This includes marketing, profiling or product development.

Allan Frank, when speaking about the initial assessment of the case, states;

> "..the only legal basis that the municipality had was folkeskoleloven(primary school law) was it the Danish school law and maybe some communal laws about how the municipality should act in general, and none of those places stipulated that they were allowed to give away the children's information to Google."

Elsinore municipality had not asked the students' parents for consent to create a Google account as they evaluated it to be according to the Primary School Act. The Danish DPA agreed upon this.

Furthermore, the municipality assesses that the Primary Schools Act is not the only basis for this processing of student data but the actual legal basis. However, the Danish DPA says that Elsinore municipality's processing of personal data, according to the Primary School Act, does not cover situations where personal data is processed for purposes other than those provided in the Primary School Act. The students' personal data can, therefore, not lawfully be transferred to other data controllers for use other purposes than intended when it is a purpose considered that is not stipulated in the Primary School Act.

8.3 Data Confinement Framework

Throughout the report, we first investigated the technical architecture of cloud computing in Chapter 3. We explored various legislation impacting cloud services in Chapter 4 as well as cases that lead to challenges with GDPR in Chapter 6. In the aforementioned cases, we discussed the concerns in cloud computing and privacy, and in Chapter 7, we thoroughly discussed the Elsinore-Google Chromebook-gate case. As a result, we finally discussed whether it is possible to provide solutions to satisfy the security and privacy requirements of GDPR, including relevant laws. The finding of those subject matters has pointed to the culmination of diverging the problem areas into three components; the technical, organizational and legal aspects of Data Confinement.

From the investigation, we believe that the means required to address the technical, organizational and legal aspects of processing personal data are all components to satisfy. We have argued different issues and challenges concerning handling personal data. Having investigated all the different aspects of the cases mentioned above, we propose the Data Confinement Framework, which can be considered an approach to solving those challenges. The Data Confinement Framework does not encapsulate 'what' rather than 'how' data processing should be realized. It re-views the measures of that of processing data, whether it is collecting, storing or processing personal data, and of those methods to reach a satisfying goal—furthermore, personal data from the data subjects to address the appropriate legislation on the operating territory. The framework has an emphasis on the technical aspect concentrating on technical steps towards a solution that can be perceived as software or mechanical. The organizational aspect sets both the partakers in the procedure of processing personal data as well as end-users.

The Data Confinement Framework is built upon three main components and is illustrated in Figure 8.1. Each component has its own expected purpose and outcome. We have tried to separate the roles of the different stakeholders in each component in order to make the problem easier to understand and provide a solution for it. All the components can function individually but we recommend to consider the complete framework as one unit to produce the maximum outcome.

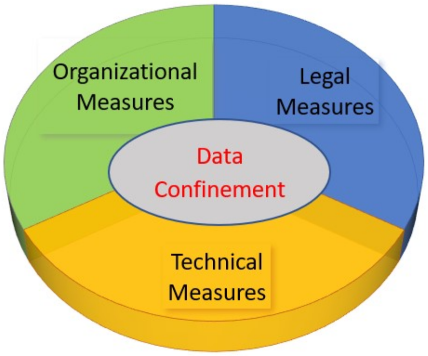


Figure 8.1: Data Confinement Framework

Figure 8.2 shows the complete workflow of the framework. The three components of data confinement and how they collectively collaborate as a single module to build a secured user environment. To begin with the framework, it is important to understand the three key stakeholders involved here: the CSPs and the two types of consumers: business organizations and end-users. The CSPs develop and provide the services. Next is the business organizations or any institutions making use of CSPs' services. An enormous number of businesses and organizations rely heavily on the cloud not only just for storing their data but also on different cloud solutions like AI tools and analytical tools. The consumers build their

systems on top of the cloud. The third stakeholder is the end-users who use the systems offered by the business organizations. In a nutshell, the CSPs and the business organizations work closely to collaborate for smooth operation. GDPR differentiates between these stakeholders by an agreement called Data Protection Agreement (DPA) described in
Section 4.1.4, which assigns specific roles to actors such as Data Controller, Data Processor, and third-party.

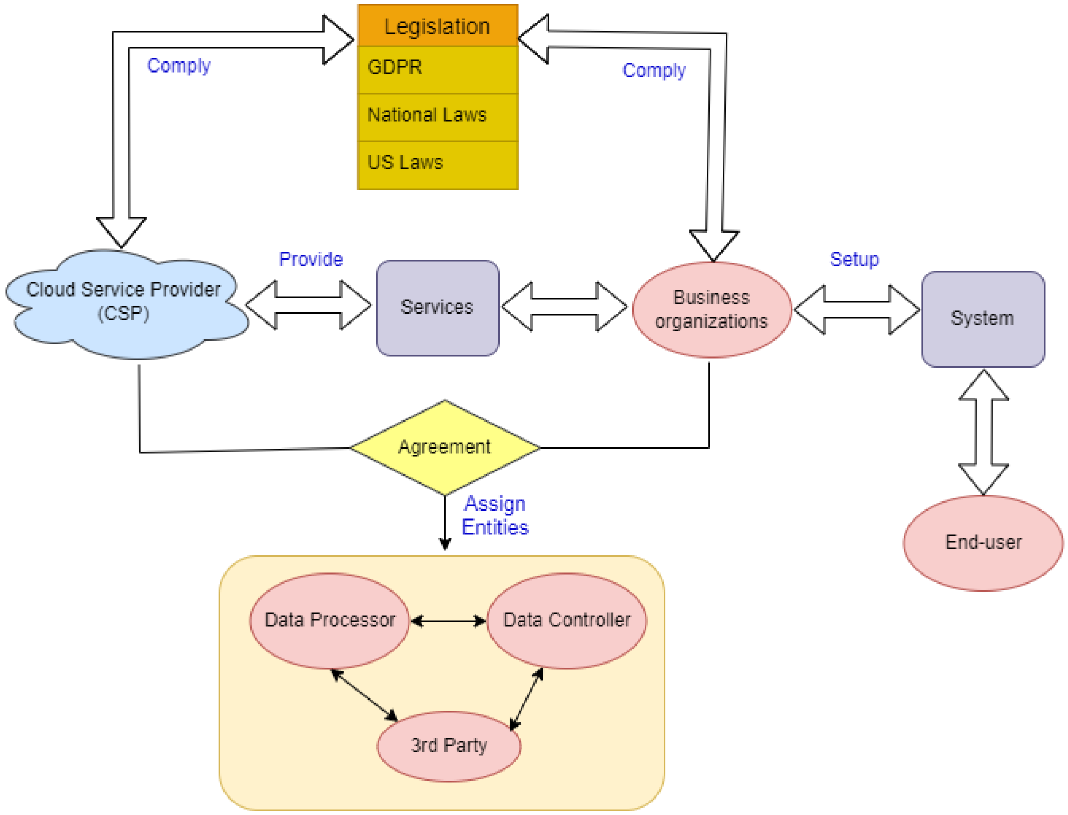


Figure 8.2: Workflow of Data Confinement Framework with different Stakeholders

The model initiates with its first component, legal measures. The CSPs and the business organizations must assess the legislation of the location where the business is operating. In this case, the legislation of the geographical territory of operation has to be followed by both CSP and the business organization. There are strict fines on any stakeholder for diverging from the laws. The agreement between CSP and business organization (DPA for GDPR) is a key player having a great impact on the complete architecture. It binds and assigns all the different stakeholders specifying what each of them is supposed to do and what clauses they will have to maintain. The further is explained in Section 8.3.1.

The next component of this framework is the technical measures described in section 8.3.2. The CSPs implement the services based on the parameters set by legal measures. The technical measure deals with all the development of the services used by the consumers. That takes the model into the framework's last phase, which is organizational measure explained in Section 8.3.3. The organizational measures are divided into two based on the consumer and end-user responsibilities. This component encompasses how the consumers should set up their system using the services from the cloud. It also holds the end-users responsible as well while using the system.

8.3.1 Legal measures

Data confinement aims to ensure adequate protection of the personal data of data subjects. To enforce this, laws and standards are provided in different regions and states worldwide. These laws and standards stipulate the part each party involved in processing or transferring personal data must play. Thus, it is imperative that legal measures should be in place with regard to data confinement.

The provider and the consumer here have shared responsibilities:

- **Identifying relevant legislation**: The specifics on what each party is required to do should be based on the available and applicable standards, depending on the region. For example, the GDPR and local data protection laws if it is an EU member state, the California Consumer Privacy Act or other applicable laws if it is American, or other foreign laws available in a particular region or state.
- **Complying with the legislation**: The actors must comply with the relevant legislation and standards they have identified.
- **Define stakeholders and their responsibilities** The roles of the different stakeholders, like the provider and the consumer, must be clearly defined beforehand. It is mandatory to limit the scope of processing and other activities each stakeholder can perform.

The responsibilities of the end user are:

- **Know the rights**: The user must know his rights for different reasons. He has to be able to see if those rights are violated, and he has to know and understand what he can do in that situation.

8.3.2 Technical measures

This aspect of data confinement is quite broad as it encompasses different technical layers. It goes from the measures used to handle and protect data in cloud computing to measures needed to operate the underlying physical infrastructure. We found the following responsibilities on the shoulders of the provider:

- **Set up and maintain hardware**: To provide the cloud computing service, the provider has to set up hardware resources such as computers, network devices or storage devices. Infrastructure maintenance operations and the maintenance of the data center itself, such as heating or cooling, ventilation, etc., are also to be taken into account.
- **Resource abstraction**: The provider also has to provide the connection from the user interface to the underlying hardware, which is done through resource abstraction. Measures here include choice and setup of hypervisor, and virtual machines, among other things.
- **Set up and maintain the cloud architecture**: The higher level of technical measures include the providers' choices on architecture (for example, Microsoft's method of separating servers for commercial and private customers), and user interfaces, among others.
- **Security requirements**: Cloud providers here address different security requirements such as confidentiality, integrity and availability, which we discussed in section 3.3. Here protection techniques such as encryption are investigated by the providers. Effective access control mechanisms are mandatory to maintain the hierarchy inside the organization and the separation of consumers. Our model imposes the obligation on the organization to ensure that an actor is limited to operate only within his assigned part. In order to secure the access control even more, we suggest using one of the cryptographic access control mechanisms we described in section 5.3.3.

- **Privacy by design**: CSPs have to consider the idea of privacy by design while implementing any cloud service. Privacy by design contains two critical principles: privacy as the default setting and privacy embedded into the design.

The responsibilities of the user are:

- **Activating and using the features**: Despite most of the technical measures being directly chosen by the service provider, the user still has to do some configuration. For instance, the provider sets up everything needed for Multi-Factor Authentication. However, the user still has to activate it and link his phone or authenticating device in order for it to be helpful.

8.3.3 Organizational Measures

The third component of our concept for data confinement is the organizational measure. This term features all associated human interventions of the data subjects, stakeholders, and their respective roles throughout the entire life cycle of the data, starting from the collection to storing data in the cloud. The scope of our projects entails the cloud providers, consumers, data controller, processor or third-party (if any) as stakeholders or actors. Therefore, this concept is a collective approach to ensure each actor's precise execution of their responsibilities on the cloud platform. In the technical measures of data confinement, the cloud providers are held responsible for implementing and deploying effective solutions to guarantee security and privacy. Moreover, organizational measures explain the consumers' liability to have a clear understanding of how to use those solutions. The necessity of the awareness of the end-users is also addressed in this block of the model. To provide a secure cloud environment to the users, there lies a lot on the consumer's shoulder. According to our research, we find the following responsibilities on the shoulder of the consumer, and we put those responsibilities in modules as follows:

- **Formulate Policies:** The consumer organization must verify the providers' policies. The policy should reflect smooth operation for both cloud providers and consumers. They must have to be well informed about the legislation. The requirements and implications of the legislation are discussed in the legal measures in Section 8.3.1. Before starting a service with any third-party, consumers must build their business model, prepare the policies to support the business, and map their policies with the local or international laws that might apply to the business model.
- **Perform Risk Assessment:** The consumers must identify the possible risks involving the end-users using the system and also, before making any deal with cloud providers or third-party, assess the risks and include every possible measure to protect the privacy of the users. The consumers must have proper documentation to record the risks and the measures they implement to mitigate them.
- **Efficient Design of the Business Architecture:** It is solely on the consumer to choose the location where the organizational data is flowing and stored. In this case. The consumer will have to be well informed about the possible locations of the regions and availability zones. It is not wise to operate a business in Asia while the data is stored in Europe and vice versa. Considering the compliance issues, selecting the geographical region of the data centers closest to your business operation is best. The architects of the consumer organization have to provide an efficient design.
- **Service Configuration:** While using a cloud solution, the consumers must guarantee that it is well-configured. The role of different administrators of the consumer organization is critical in this case. He must configure the firewall to protect the network from malicious external requests. The devices have to be updated and patched regularly.

- **Circumventing Default Configuration:** Depending on the default configuration is not ideal in business environments. The tendency to trust the default setup might jeopardize the entire system's security.
- **Training:** Educate everyone, the employees of the organization and the end users. Nowadays, consumer organizations arrange training for their employees to make them more aware of the current cyber trends.
- **Monitoring and Incident response:** Two most critical services are monitoring and incident response. The system's network must be monitored and log events in case of abnormalities. During any data breach, the primary job is to identify the breach first, which is possible only with proper network monitoring. Consumers must deploy a security operations center(SOC) to handle such incidents.

The responsibilities of the users in each module are described as follows:

- **Awareness of consents:** While giving consents, users must be aware of what they are allowing the world to know about them. The consumer organizations will provide sufficient safeguards, but still, there are rooms for the end-users to make it more efficient and private. Some applications need to be configured precisely on the end-user device level. It is tough to find someone who reads the privacy terms before accepting, which is not always a good practice. Later in this chapter, we reflect upon some configuration recommendation that makes a device more adapt to privacy in 8.6.
- **Responding to the requests:** On many occasions, may it be user support or improving the services, the cloud providers or the consumers need to access the user's private data. They send a request to the users to accept such kind of access to personal data. Caution is required before providing those access requests. For instance, the idea of Microsoft's implementation of Lockbox is already mentioned in the technical measure. The request is received in the interface of the Lockbox, waiting for users' responses that can be reviewing, accepting or rejecting as well.

8.4 Case Study with Data Confinement Framework

As we have formulated the Data Confinement Framework, in this section, we will use the framework to analyze three cases from all the cases we have discussed in Chapter 6 and 7. We will try to analyze the actual problems of the different cases and see whether our framework is suitable to address the problems and propose any satisfactory solution.

8.4.1 Data Confinement Framework on Chromebook-gate case

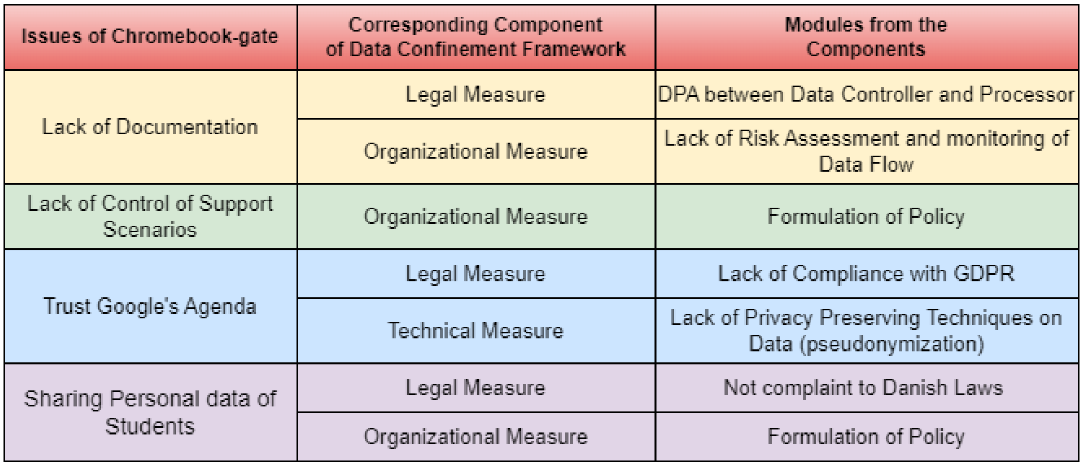
We have dived deep into the Chromebook-gate case in Chapter 7, describing what actually happened and all four verdicts, including the current state of it. Then we analyze the case further in Section 8.2 to identify the four core issues that caused the Danish DPA to ban the use of Google Chromebook and Google Workspace for Education. We will discuss each of the four issues and correlate them with the Data Confinement Framework. We will map each issue with the three components of the framework and refer to specific points of those components.

First, we consider the lack of documentation. The Elsinore municipality did not perform any risk assessment before buying them and setting up the Chromebooks at schools. They did not check the configurations of the devices before starting the operation. Therefore, according to our designed framework, all these issues point to both the lack of **legal measures** and **organizational measures** as well. Legal measures enforce the data controller and the data processor to act in accordance with the agreement DPA according to GDPR. If the data controller (Elsinore municipality in this case) were compliant with GDPR, the data of the students would have been confined. The modules from the organizational measure that look prominent are the lack of risk assessment and the lack of monitoring of the data flow. The municipality did not monitor the data flowing out of its network.

Second, we look at the lack of control of support scenarios leading to data transfer outside the EU. The municipality was relying on Google to provide them with user support. It solely points to the lack of **organizational measure**. The module that could be applied to solve this issue is formulating the policies between the data controller and the processor. There should have been strict policies and security controls between the two parties to ensure no data is being analyzed for any purpose out of scope. Another solution in this case, can be introducing local user support, which is described in the recommended solution in Section 8.5.1.

Third, we inspect the next issue of having trust on the business model of a giant tech company like Google and assuming that they will not analyze the data of their users'. After the complaint being filed against Elsinore municipality, the Danish DPA initiated the investigation and requested the municipality to carry out the impact assessment and submit to them. As a consequence, it was clear that the municipality was not compliant to GDPR as data was processed outside EU. This issue points to two components of the framework. **Legal measures** and **technical measure**. The legal measure impose the compliance with GDPR on the data controller and processor to solve the dispute. And technical measure identifies the lack of pseudonymization on the data, which is included under security requirements. The privacy preserving techniques must be applied to any data to guarantee privacy. If the data were pseudonymized, the CSP could not analyze it. One technical solution is constructed with the help of encryption and data splitting explained in Section 5. The solution is illustrated in the section of recommended solution in Section 8.5.2.

Fourth, we examine the issue of the lawfulness of sharing personally identifiable data of students. This issue is pretty straightforward that the municipality did not adhere to Danish national laws. This issue indicates the lack of **legal measure** and **organizational measure** of the municipality. The implication of legal measures is that the municipality did not comply with Danish laws, which resulted in the unlawful data sharing of the students. The module concerning the verification of the policy in the organizational measure is also key here. If the municipality had considered the national laws, then this data sharing could not happen. We have also devised a third recommended solution that, if applied, will cease any kind of data transfer outside the EU in Section 8.5.3. Figure 8.3 summarizes all the key points discussed above.



Issues of Chromebook-gate	Corresponding Component of Data Confinement Framework	Modules from the Components
Lack of Documentation	Legal Measure	DPA between Data Controller and Processor
	Organizational Measure	Lack of Risk Assessment and monitoring of Data Flow
Lack of Control of Support Scenarios	Organizational Measure	Formulation of Policy
Trust Google's Agenda	Legal Measure	Lack of Compliance with GDPR
	Technical Measure	Lack of Privacy Preserving Techniques on Data (pseudonymization)
Sharing Personal data of Students	Legal Measure	Not complaint to Danish Laws
	Organizational Measure	Formulation of Policy

Figure 8.3: Data Confinement Framework on Chromebook

8.4.2 Data Confinement on Relevant Cases

We consider three of the cases described in Chapter 6 one at a time and try to analyze the problems to investigate the feasibility of the Data Confinement Framework. The cases we are considering are the data leak of Facebook, the TikTok case, and the Google Analytics case.

The Facebook case

The breach that happened with Facebook is described in detail in Section 6.3. The foremost issue that caused the data leak of Facebook is the vulnerability in an API named "Graph API", which lets third-party apps to integrate with the actual platform. After the data leak happened and Facebook responded with tons of follow-up tasks to mitigate the issue. The authority restricted the access of all the similar third-party apps to the massive data generated on Facebook. They monitored all third-party apps requesting for any unnecessary data for the services they provide and to ensure proportionality. We could find three major issues in this case.

First, Facebook did not consider the impact assessment of their features and the Graph API was not considered a bug in the system. If they had done the impact assessment correctly, they were supposed to identify the unlimited access of those third-party apps. This issue points to the lack of risk assessment of **privacy by design (privacy embedded into design)** module from the **technical measures** component.

Second, The developer team of the Graph API did not certainly consider privacy by design while implementing it. For the lack of privacy by design, the third-party app could have access to whatever data they wanted. This issue directs to the **privacy by design (privacy embedded into design)** module from the **technical measure** as well.

Third, There was a lack of awareness among the Facebook users participating in the quiz app, querying for personal preferences and interests. This issue points to the **lack of awareness of users** module from the **organization measures**.

The TikTok case

The issues of the TikTok case are discussed in Section 6.4 in detail. The most significant privacy concern we investigated, in this case, is the collection of sensitive personal data according to GDPR and also personally identifiable information (PII) according to US laws. These data include name, date of birth, e-mail address, phone number, messages sent or received by the content creator, all purchase history with payment card details, and user location, and the list goes keeps growing.

First, this issue of collecting this enormous amount of data of the users points out to the **legal measures** component. TikTok being a large-scale company providing service to users across boundaries. There are many international legislations that do not support this sort of data collection.

Second, we can identify the lack of **privacy by design** which directs to **technical measures**. One of the seven principles of privacy by design is "privacy as the default setting". This principle is claimed to protect personal data, which requires purpose specification, data minimization, data retention, and many others.

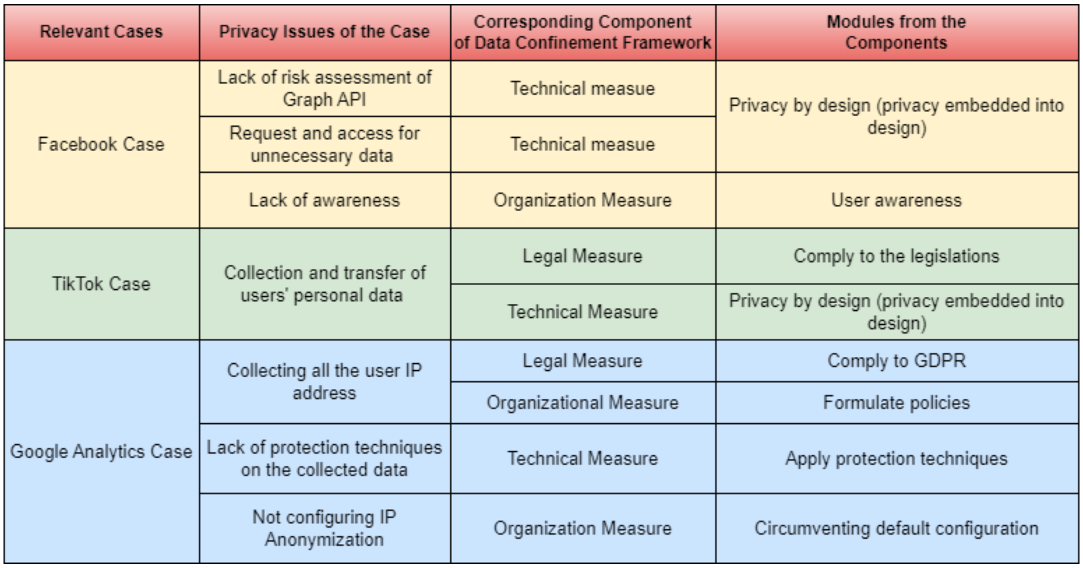
The Google Analytics case

The Google Analytics case is described in Section 6.5. The case started with a complaint filed by an Austrian data subject against a local website provider using Google Analytics. The complain was due to the collection and transfer of personal data to Google LLC outside the EU. We bring three privacy concerns to light after our investigation. We will discuss each of the problems as well as the component of the Data Confinement Framework interpreting the issues to solve.

First, the complaint against the website provider is about collecting personal data of the users, which can identify specific users. There is no satisfactory purpose found for collecting IP addresses by the website provider that makes it non-compliant with GDPR. It regulates both **legal measures** and **organization measures**. For legal measures, the module we can refer to is the lack of compliance with GDPR, which is supposed to be monitored and audited by the DPO. For organizational measures, the module to formulate policies can be pointed out easily. Certain flaws were exhibited in the company policy of the website provider sharing personal data outside the EU to Google LLC.

Second, there was a lack of adequate protection techniques applied to the data transferred to Google. This points to the **technical measures** with the suitable protection techniques. Also, the feature of anonymizing the IP address was not considered by default. Google left this feature to the consumer organizations to configure based on their preferences. We can conclude by saying that the privacy embedded into the system was not considered.

Third, following the previous point, we also find the lack of **circumventing the default configuration** module from **organization measure**. The website provider did not configure Google Analytics to be compliant with GDPR. Figure 8.4 shows the complete summary of all the arguments explored above.



Relevant Cases	Privacy Issues of the Case	Corresponding Component of Data Confinement Framework	Modules from the Components
Facebook Case	Lack of risk assessment of Graph API	Technical measue	Privacy by design (privacy embedded into design)
	Request and access for unnecessary data	Technical measue	
	Lack of awareness	Organization Measure	User awareness
TikTok Case	Collection and transfer of users' personal data	Legal Measure	Comply to the legislations
		Technical Measure	Privacy by design (privacy embedded into design)
Google Analytics Case	Collecting all the user IP address	Legal Measure	Comply to GDPR
		Organizational Measure	Formulate policies
	Lack of protection techniques on the collected data	Technical Measure	Apply protection techniques
	Not configuring IP Anonymization	Organization Measure	Circumventing default configuration

Figure 8.4: Data Confinement Framework on all the relevant cases

8.5 Recommended Solutions for Data Confinement

We have already discussed the Data Confinement Framework and the collective impact of its three components on all the stakeholders in Section 8.3. In Section 8.4, we analyzed that our framework is robust enough to address all the issues in each case. Enforcing the framework would have resolved all these issues to make it GDPR compliant. This section proposes three solutions suitable to fit the Data Confinement Framework and achieve GDPR compliance. The solutions are described in detail below.

8.5.1 Public Cloud to hybrid cloud

This solution is devised specifically considering the Chromebook-gate problem. We have identified and explored the core four problems in Section 8.2. Next, we have extensively investigated the modules in the respective component of the Data Confinement Framework to solve each of the four problems summarized in Figure 8.3. The proposed solution is displayed in Figure 8.5. This solution is capable of solving each of the four identified problems. The architecture of the solution is described below.

Hybrid Cloud Model

One of the major concerns in the Chromebook case was the use of software-as-a-service by the schools in the public cloud, which caused a lack of control of support following the sharing of the students' personal data. This solution's primary objective is to ensure that the students' personal data never have to leave Denmark for any scenario. Serving that goal, we come up with this solution of clustering the schools under municipalities and installing a hybrid cloud model. The architecture is devised, replacing the public cloud with the hybrid cloud model.

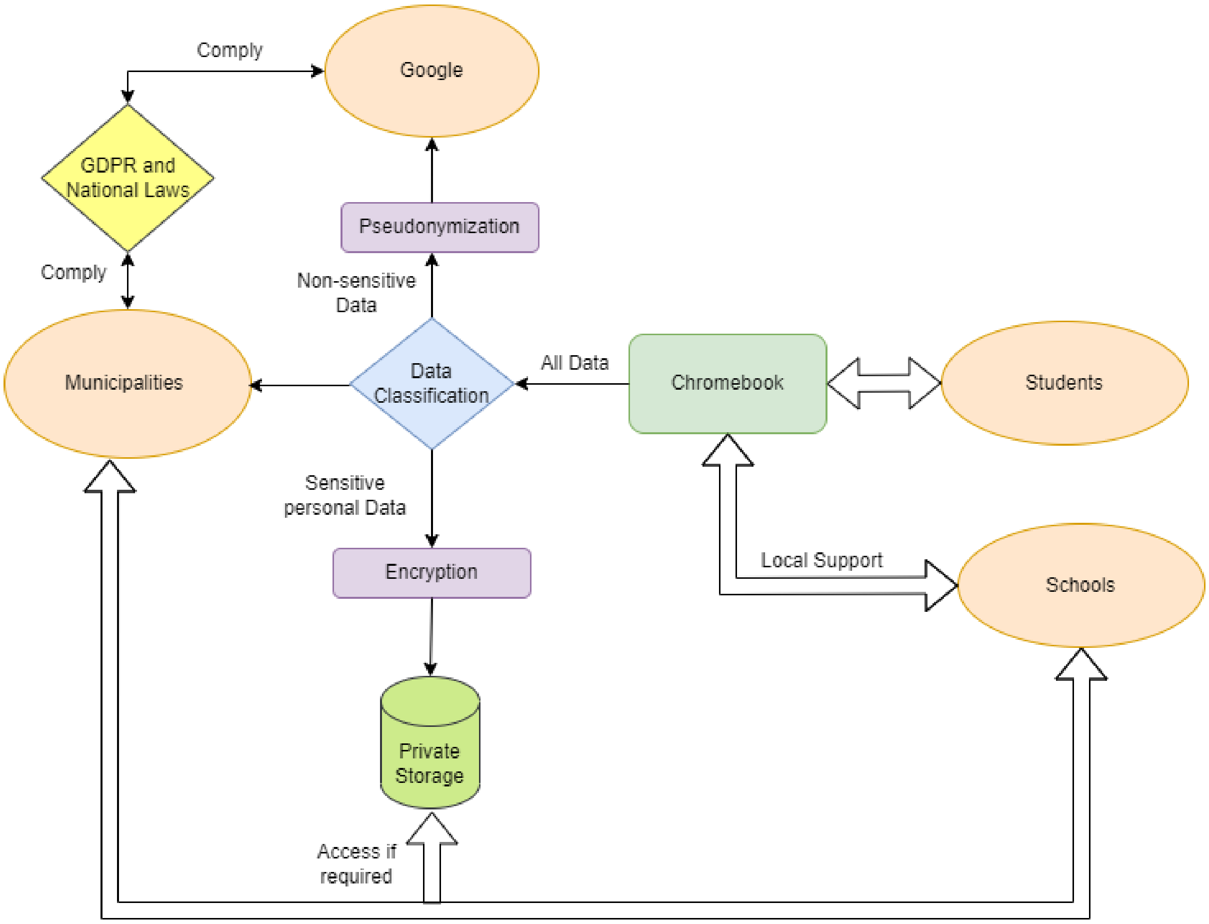


Figure 8.5: The proposed solution for Data Confinement using Hybrid Cloud Architecture

The Architecture

- The schools set up the Chromebooks at the campus for the students. While on campus, the students can access their data directly. If they are outside the campus, they have to log in through remote access to access the data.

- As a hybrid cloud is installed, the schools under the municipalities will have both private and public storage. So now, the schools have the option to deploy a private infrastructure for personal purposes, and a public infrastructure would be for general purposes.
- The data out of the Chromebook does not go to Google directly anymore. Instead, the data will feed a classifier which will separate and tag data into two types: sensitive personal data and non-sensitive data. There will be two outputs from the classifier: one will send any data classified as sensitive to the private storage after encrypting it. The other output will pseudonymize the non-sensitive data and pass it to the public cloud.
- We have studied the single-reader architecture of the Symmetric Searchable Encryption (SSE) in Section 5.3.1.1 and Homomorphic Encryption (HE) in Section 5.3.2.1. We can achieve the expected privacy protection by applying these encryption techniques in our solution.
- The schools will have to employ an appropriate IT support team capable of providing local support. The IT support team must have network and security professionals to analyze the traffic flow, searching for unusual traffic patterns.

Data Controller and Data Processor

We re-define the data protection agreement between Google and the schools or municipalities. Previously, the schools were the data controllers, and Google was the data processor. In our solution, we eliminate any third-party processing and provide local user support empowering the schools under municipalities to process the data only. The new agreement makes the schools under municipalities both data controllers and data processors. To provide support, Google goes through the schools and the operations are monitored.

8.5.2 Solution using Multi-party Computation

Allan Frank mentioned in the interview that multi-party computation could be a viable solution for this case. As explained in Section 5.3.2.2, multi-party computation enables different parties to perform a computation using their private data without sharing that data between them. In our case, we assume that Google needs data from the Chromebook and the municipality. However, the municipality does not want to share users' data directly for privacy reasons. The users do not want data collected from their Chromebook devices without their knowledge. A multi-party computation architecture, in this case, can permit Google to do computation on data while the users' privacy is assured. The result is communicated to Google without them having to see the users' data directly. This proposed solution still allows Google to process data but gives the other parties better transparency and control over what is being processed.

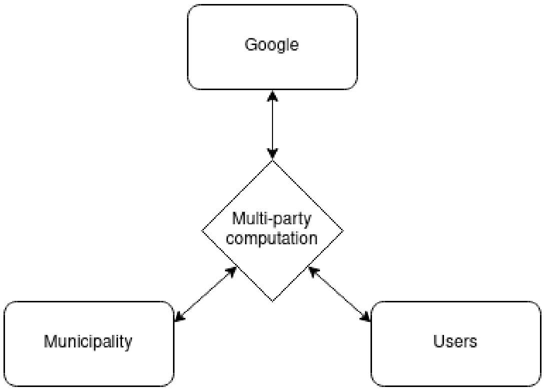


Figure 8.6: The proposed solution for Data Confinement using multi-party computation

8.5.3 Enforcing EU Trusted Party

The third recommended solution is to enforce a trusted local party primarily operating within the EU that should provide the required cloud service. The idea of such a solution is inspired by the way the Chinese government handles cloud services. In 2015, the Ministry of Industry and Information Technology (MIIT) issued the "Classified Catalogue of Telecommunications Services". With the imposition of this law, cloud services are categorized as value-added telecommunication services (VATS) in China, which requires special VATS license. However, only the local Chinese companies can avail these licenses [85]. The only workaround for international CSPs to enter the Chinese market is establishing a Joint Venture with a local company. For example,

- Microsoft Azure runs their cloud services in China, partnering with a local company name 21Vianet that independently operates all the services themselves [86].

- Amazon Web Services (AWS) is running two joint ventures in China. One with Sinnet Technology Co., Ltd., which operates in Beijing. Moreover, the other venture is with a company named Ningxia Western Cloud Data Technology Co., Ltd. (NWCD) for the Ningxia region [87].

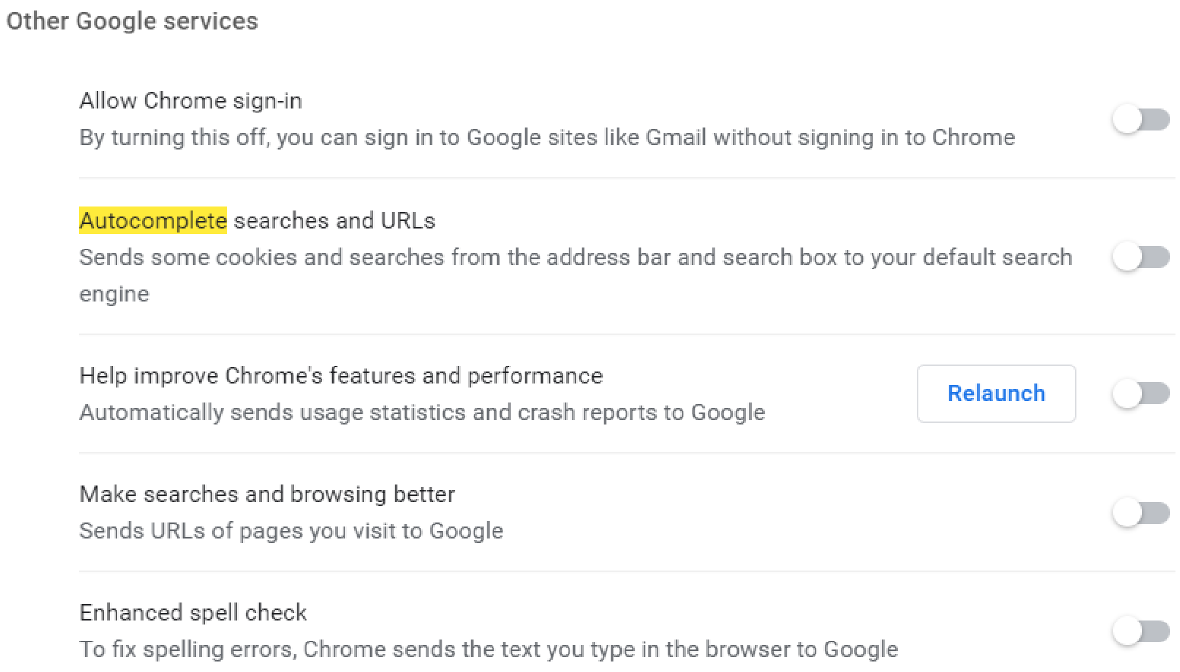
For EU territory, we propose to have such kind of joint venture programs between international CSPs with the EU local company. There will be a regulatory boundary which holds the right for any data transfers outside the EU to the parent company. All the infrastructure, resources, and support should be delivered by the EU company only. Both commercial and personal consumers will only contact the local company. This approach might be a viable solution to implement data confinement inside the EU. Nevertheless, it is not difficult to understand that this kind of solution will cause a drastic change in the entire cloud market of the EU and will require attention from the highest level of the European Commission.

8.6 End-device Configurations to Enhance Privacy

This section will discuss configuration recommendations for the users' end devices that will improve their privacy. It is not a checklist or a guideline for buying privacy but rather suggestions. There is a never-ending debate about the usefulness of some features against the users' privacy. A considerable lack of awareness among the users escalates the possibility of data leaks. In this project, as we put more emphasis on user privacy, we list a few features below that users could consider turning off for better privacy. We will reflect the Chromebook settings first and then Microsoft settings.

8.6.1 Configure your Chromebook

- **Disable Automatic Services:** The prediction service of Google is built to improve the browsing experience. After many debates from the experts, the prediction services are removed by Google, but some similar automatic features still exist. Users can turn off the features shown in the Figure 8.7. Users can find these features by navigating to: ***Settings > You and Google > Sync and Google services***.



Other Google services

Allow Chrome sign-in
By turning this off, you can sign in to Google sites like Gmail without signing in to Chrome

Autocomplete searches and URLs
Sends some cookies and searches from the address bar and search box to your default search engine

Help improve Chrome's features and performance
Automatically sends usage statistics and crash reports to Google

Make searches and browsing better
Sends URLs of pages you visit to Google

Enhanced spell check
To fix spelling errors, Chrome sends the text you type in the browser to Google

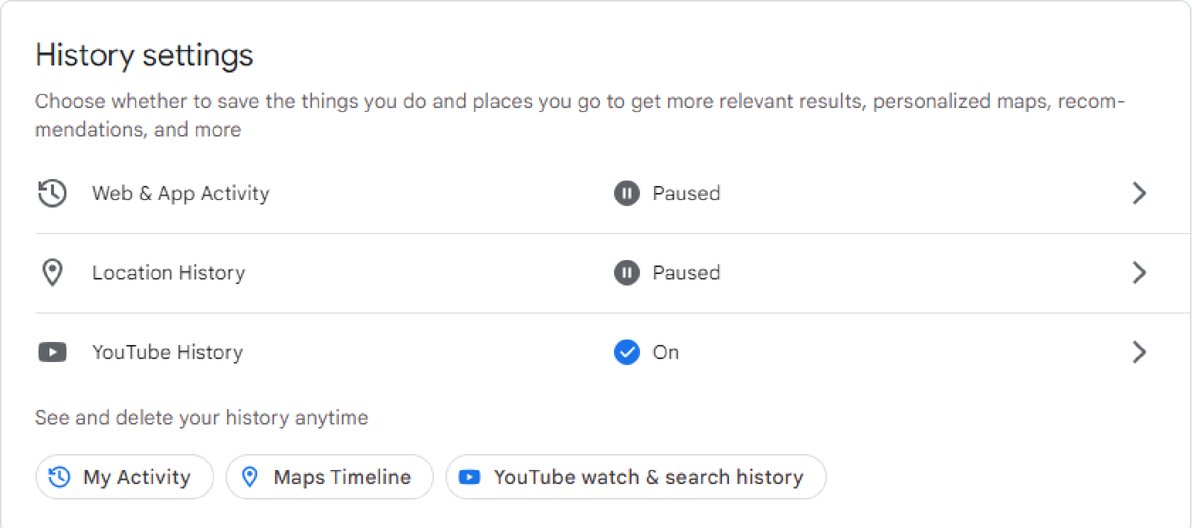
Figure 8.7: Configuration of automatic services

- **Cookies and other site data:** Tracking cookies can compromise user privacy as it tracks users' browsing patterns. The cookies of Chrome can be configured. One can navigate to cookies in Chrome browser by following: ***Settings > Privacy and Security > Cookies and other site data***. There are currently four settings to choose from. The best recommended is the third one named "Block third-party cookies". It does not let sites see users' browsing activity which sites mostly require for making personalized ads. Users can also enable the setting of sending a **"Do Not Track"** request that should also protect the browsing traffic.

- **Autofill:** This feature of Chrome saves user addresses and payment methods of the user. To configure, users can find this feature in: *Settings > Autofill > Payment methods* and ***Settings > Autofill > Addresses and more***. Users are recommended to turn all the toggles in these two settings.

- **Search Engine:** Some browsers promise to ensure user privacy to the fullest. Users can change their default search engine to one of those. A few examples are Brave Search and DuckDuckGo, among others.

- **History in Google Account:** Users can tweak a lot of essential privacy functionalities in the Google account. They can change the settings so that their online activities and locations are not tracked. To find this, go to: ***Google Account > Data and privacy > History settings***. Turn off both "Web and App Activity" and "Location History". Figure 8.8 shows the settings.



History settings

Choose whether to save the things you do and places you go to get more relevant results, personalized maps, recommendations, and more

Web & App Activity — Paused

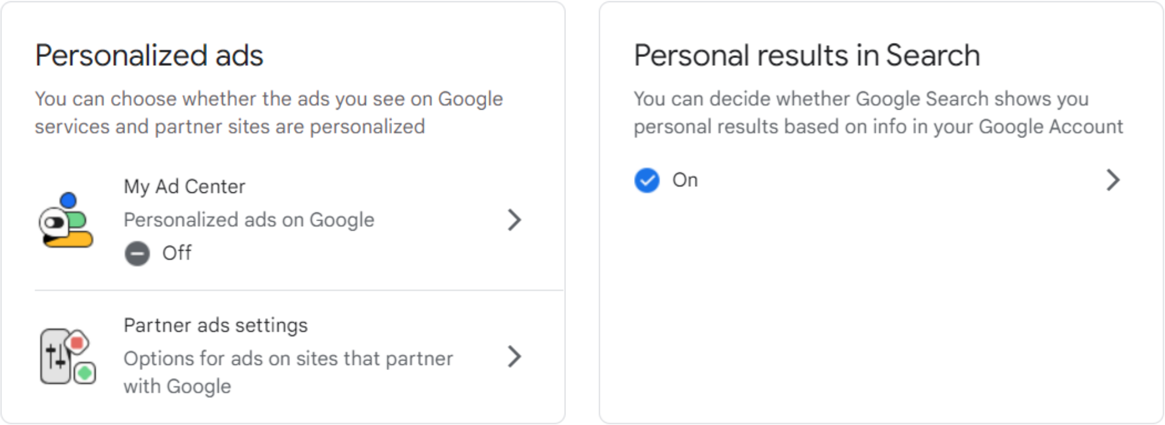
Location History — Paused

YouTube History — ✓ On

See and delete your history anytime

Figure 8.8: Configuration user history in Google Account

- **Personalized Ads and Search in Google Account:** Users can also turn off any personalized ads and search results. These features allow Google to analyze tons of user data like browsing patterns, shopping behavior, travelling patterns, etc. Users can find it going to: ***Google Account*** > ***Data and privacy***. Figure 8.9 shows the two mentioned settings



Personalized ads

You can choose whether the ads you see on Google services and partner sites are personalized

My Ad Center
Personalized ads on Google
Off

Partner ads settings
Options for ads on sites that partner with Google

Personal results in Search

You can decide whether Google Search shows you personal results based on info in your Google Account

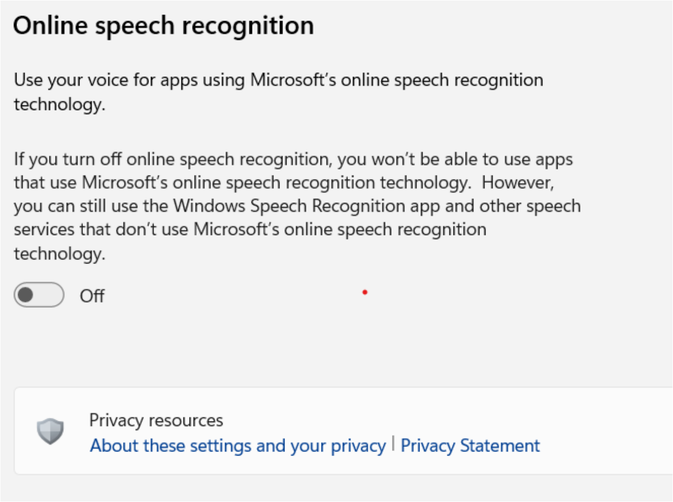
✓ On

Figure 8.9: Personalized ads and search results

8.6.2 Configure Microsoft Features

Some features that users might think of invading their privacy are built into the system by default. If the users do not know about these, they might end up providing their data to Microsoft, even unknowingly.

- **Speech Recognition:** Windows records users' speech for their own resource purpose by default. If users do not want Microsoft to get their recordings, they must turn them off themselves. To find the speech recognition, users have to follow: ***Settings*** > ***Privacy and Security*** > ***Speech***. The users can turn off the feature. Figure 8.10 illustrates the configuration.



Online speech recognition

Use your voice for apps using Microsoft's online speech recognition technology.

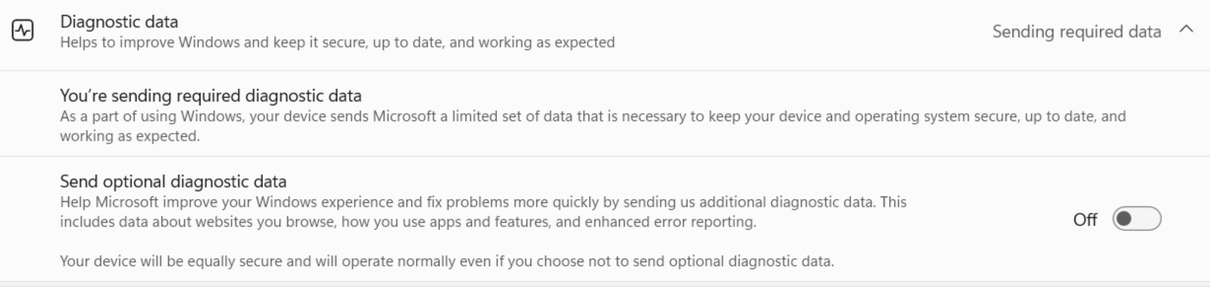
If you turn off online speech recognition, you won't be able to use apps that use Microsoft's online speech recognition technology. However, you can still use the Windows Speech Recognition app and other speech services that don't use Microsoft's online speech recognition technology.

○ Off

Privacy resources
About these settings and your privacy | Privacy Statement

Figure 8.10: Speech recognition for research purposes

- **Optional Diagnostics Data:** Microsoft captures required data from the users to improve their system. The process is called diagnostics service. However, users can ensure data minimization by configuring their devices. Users can turn off the setting to send optional diagnostic data by going to: ***Settings > Privacy and Security > Diagnostics and feedback***. Figure 8.11 shows the setting.



Diagnostic data
Helps to improve Windows and keep it secure, up to date, and working as expected
Sending required data

You're sending required diagnostic data
As a part of using Windows, your device sends Microsoft a limited set of data that is necessary to keep your device and operating system secure, up to date, and working as expected.

Send optional diagnostic data
Help Microsoft improve your Windows experience and fix problems more quickly by sending us additional diagnostic data. This includes data about websites you browse, how you use apps and features, and enhanced error reporting.
Off ○

Your device will be equally secure and will operate normally even if you choose not to send optional diagnostic data.

Figure 8.11: Configuring optional diagnostic data

Chapter 9

Discussion & Conclusion

9.1 Discussion

Throughout the duration of our project, we had to be careful in our case selection as a lot of new cases, that would be relevant and could be included in Chapter 6, kept coming. We also had to be attentive to the development of the Chromebook case, with a decision from the Danish DPA coming as late as December 14th 2022, with new interpretations and newspaper articles also coming out every week.

Speaking of our main case, the question of whether Google collects too much data is a matter of debate. It depends on the perspective one has on the balance between the benefits of data collection for personalized experiences and the potential privacy risks. We believe reducing the amount of data collected and processed through legislation is possible. However, one can ask himself whether Google will have to rethink their business model due to this.

Alternative solutions

Alternative solutions, such as open-source software, are interesting to consider. One of the main benefits of open-source software is that it is typically free to use. This can be especially useful for institutions and organizations with limited budgets. Open-source software can be modified and customized to meet an organization's specific needs. This allows greater control over the software and hence, over the data collection. Lastly, it encourages collaboration and community involvement. One could imagine a software replacing GWfE being shared and controlled among municipalities and schools.
A professor of IT at Denmark's Institute for Pedagogy and Education, Jeppe Bundsgaard, thinks that Elsinore municipality could have avoided the ongoing Chromebook case by installing the Linux operating systems on the Chromebooks. He states that the changeover is simple. [88]

> "It is a fairly simple operation to do if you have a little technical flair. And if you have to do it with a thousand computers in a municipality, you could probably figure it out." (translated from Danish)

However, open-source software has its limitations. Some open-source software may have less support than proprietary software. This can be a problem for organizations and institutions that rely on software for critical processes and need timely support in case of issues or bugs. Furthermore, some open-source software projects may need more resources or funding than proprietary software companies do, which can limit their development and maintenance.

Future of cloud computing

Cloud computing has become increasingly popular in recent years due to its ability to offer scalable, flexible, and cost-effective computing resources to businesses and individuals. Looking ahead, it is likely

that cloud computing will continue to grow and evolve. With the market trend in recent years, briefly described in section 3.5, it is likely that the cloud will be adopted by even more companies and institutions around the world. As cloud computing becomes more prevalent and critical to businesses and individuals, there will likely be a greater focus on ensuring the security and privacy of data stored in the cloud. This is achievable through more transparency from the cloud providers about what data they collect and how they process it, more control from the lawmakers over what the providers do and more awareness from the users.
Legislation plays a crucial role in regulating and shaping the development and use of cloud computing, helping to ensure that the technology is used in a legal, ethical, and responsible manner.

Future laws

An executive order was signed by Joe Biden back in October 2022 to implement a new EU-US Data Privacy Framework, also known as Privacy Shield 2.0, which will protect the privacy of personal data shared between the US and the European Union. [89] If all goes well, the new agreement will be published in March 2023. It addresses concerns raised in Schrems II, as mentioned in section 4.4. However, Max Schrems and his privacy rights organization NOYB expressed concerns over this executive order saying that:

> "At first sight, it seems that the core issues were not solved and it will be back to the Court of Justice of the European Union sooner or later." [90]

In the future, the EU will likely continue to strengthen and update its data protection laws to protect personal data. For example, the EU is currently working on a new data protection framework known as the ePrivacy Regulation, which is expected to come into effect in the near future. The ePrivacy Regulation sets out that interference with electronic communications between individuals is prohibited unless a listed exception is applicable. In addition, the Regulation offers some ground rules for when data may be processed. [91]

We can also mention the Digital Services Act (DSA), which is a proposed legislation being developed by the European Commission to regulate the online activities of digital service providers in the European Union. [92] The DSA is expected to set out rules for the operation of online platforms and other digital services in the EU, including requirements for transparency, fairness, and accountability. For example, the DSA has a measure addressing deceptive design. On paper, it should prevent all online platforms from designing and operating their interface design in a deceptive and manipulative way. [93] The Digital Markets Act (DMA) is another proposed legislation developed along with the DSA by the European Commission, which intends to create a level playing field for digital service providers operating in the EU and to ensure the fairness and transparency of online markets in the EU. [94]

9.2 Conclusion

Throughout this report, we highlighted various challenges the different actors of cloud computing have to address to satisfy the respective expected requirements. We first investigated the technical elements of cloud computing and the role of personal data in cloud. We then studied the legislation settings of cloud computing it surrounds. The cloud-related legislation investigation contains an overview of GDPR and related concepts, including relevant US legislation. To support the arguments of cloud computing and national and international legislation, an additional investigation of privacy-preserving techniques was conducted.

With these criteria, some relevant cases were investigated and analyzed in order to illustrate the recent problems as well as solutions in these cloud, privacy and data-related cases. After investigating relevant fields, we then conducted our Elsinore-Google case study, where we described the development of the case, supplemented with interviews, to help illustrate the problems in real-life situations.

We presented the Data Confinement Framework and applied it to our main case and relevant cases in order to understand if it is relevant. Finally, we proposed solutions that fit our framework and help the relevant actors keep their data in the EU. For future work, one could try to improve on our solutions, investigate more recent cases and look into other regulations, such as the Chinese one.

Bibliography

[1] *Use of Cloud computing services, 2020 and 2021.* Accessed: 2022-09-16. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises#Enterprises_using_cloud_computing.

[2] *2022 Q2 Cloud Market Trends.* Accessed: 2022-09-16. URL: https://www.srgresearch.com/articles/q2-cloud-market-grows-by-29-despite-strong-currency-headwinds-amazon-increases-its-share.

[3] Google. *Google privacy policy.* Accessed: 2022-12-18. URL: https://policies.google.com/privacy?hl=en-US.

[4] *The world's most valuable resource is no longer oil, but data.* Accessed: 2022-09-04. URL: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[5] Louise Holst Andersen. *Kommuner: Danmarks skolesystem er blevet afhængigt af Google og Microsoft.* Accessed: 2022-09-24. URL: https://www.version2.dk/artikel/kommuner-danmarks-skolesystem-er-blevet-afhaengigt-af-google-og-microsoft.

[6] Robert K. Yin. *Case study research - Design and methods.* SAGE Publications, 2003.

[7] Peter Mell and Timothy Grance. *The NIST Definition of Cloud Computing.* Tech. rep. 800-145. Gaithersburg, MD: National Institute of Standards and Technology (NIST), Sept. 2011. URL: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[8] Fang Liu et al. *NIST Cloud Computing Reference Architecture.* en. Sept. 2011. DOI: https://doi.org/10.6028/NIST.SP.500-292. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=909505.

[9] Protection Regulation. "Regulation (EU) 2016/679 of the European Parliament and of the Council". In: *Regulation (eu)* 679 (2016), p. 2016.

[10] *The EU General Data Protection Regulation (GDPR) : A Practical Guide.* eng. Elektronisk udgave. Cham: Springer International Publishing, 2017. ISBN: 9783319579597.

[11] Intersoft Consulting. *Directive 95/46/EC Harmonisation.* Accessed: 2022-09-19. URL: https://gdpr-info.eu/recitals/no-3/.

[12] CMS. *GDPR Enforcement Tracker.* Accessed: 2022-09-19. URL: https://www.enforcementtracker.com/.

[13] European Comission. *Standard Contractual Clauses (SCC).* Accessed: 2022-12-20. URL: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

[14] Law Office of S. Grynwajc. *International Data Transfers: When and How to Perform a Transfer Impact Assessment.* Accessed: 2022-11-07. URL: https://www.transatlantic-lawyer.com/international-data-transfers-when-and-how-to-perform-a-transfer-impact-assessment/.

[15] ePrivacy. *"Transfer Impact Assessment" (TIA) – New transfer mechanism to ensure adequate level of data protection in third country*. Accessed: 2022-11-08. URL: https://blog.eprivacy.eu/?p=1310.

[16] Danish Data Protection Agency (Datatilsynet). *What is Personal Data?* Accessed: 2022-11-07. URL: https://www.datatilsynet.dk/english/fundamental-concepts-/what-is-personal-data-.

[17] GDPR. *GDPR Article 4 Definitions*. Accessed: 2022-11-16. URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_en.

[18] European Commission. *Can personal data about chilren be collected?* Accessed: 2022-11-16. URL: https://gdpr-info.eu/art-4-gdpr/.

[19] GDPR.eu. *GDPR Article 7 Conditions for consent*. Accessed: 2022-12-01. URL: https://gdpr.eu/what-is-gdpr/#:~:text=The%5C%20General%5C%20Data%5C%20Protection%5C%20Regulation,to%5C%20people%5C%20in%5C%20the%5C%20EU..

[20] European Union Law. *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*. Accessed: 2022-12-15. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3063-1-1.

[21] European Commission. *What does data protection 'by design' and 'by default' mean?* Accessed: 2022-12-15. URL: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en.

[22] Data Protection Commission. *Data protection by Design and by Default*. Accessed: 2022-12-15. URL: https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-design-and-default.

[23] i-Scoop. *International personal data transfers: binding corporate rules (BCRs) under the GDPR*. Accessed: 2022-12-17. URL: https://www.i-scoop.eu/gdpr/binding-corporate-rules-bcrs-gdpr/.

[24] *50 U.S. Code Chapter 36 - FOREIGN INTELLIGENCE SURVEILLANCE*. [Online; accessed 14-December-2022]. URL: https://www.law.cornell.ed/uscode/text/50/chapter-36/subchapter-I.

[25] *Section 702: What it is How it works*. [Online; accessed 05-December-2022]. URL: https://cdt.org/wp-content/uploads/2017/02/Section-702.pdf.

[26] seald. *Cloud Act, FISA, ... why the Privacy Shield is now invalid?* Accessed: 2022-12-08. URL: https://www.seald.io/blog/privacy-shield-invalid.

[27] Groupe d'etudes geopolitiques. *The CLOUD Act: Unveiling European Powerlessness*. Accessed: 2022-12-08. URL: https://geopolitique.eu/articles/the-cloud-act-unveiling-european-powerlessness/.

[28] European Data Protection Supervisor. *Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence*. Accessed: 2022-12-08. URL: https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf.

[29] NSA. *Signals Intelligence - EO 12333*. Accessed: 2022-12-11. URL: https://www.nsa.gov/Signals-Intelligence/EO-12333/.

[30] Josep Domingo-Ferrer et al. "Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges". In: *Computer Communications* 140-141 (2019), pp. 38–60. ISSN: 0140-3664. DOI: https://doi.org/10.1016/j.comcom.2019.04.011. URL: https://www.sciencedirect.com/science/article/pii/S0140366418310740.

[31] Benjamin CM Fung et al. "Privacy-preserving data publishing: A survey of recent developments". In: *ACM Computing Surveys (Csur)* 42.4 (2010), pp. 1–53.

[32] Ji-Jiang Yang, Jian-Qiang Li, and Yu Niu. "A hybrid solution for privacy preserving medical data sharing in the cloud environment". In: *Future Generation Computer Systems* 43-44 (2015), pp. 74–86. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2014.06.004. URL: https://www.sciencedirect.com/science/article/pii/S0167739X14001253.

[33] Yunling Wang, Jianfeng Wang, and Xiaofeng Chen. "Secure searchable encryption: a survey". In: *Journal of communications and information networks* 1.4 (2016), pp. 52–65.

[34] Yupeng Zhang, Jonathan Katz, and Charalampos Papamanthou. "All your queries are belong to us: the power of {File-Injection} attacks on searchable encryption". In: *25th USENIX Security Symposium (USENIX Security 16)*. 2016, pp. 707–720.

[35] Benny Chor et al. "Private Information Retrieval". In: *J. ACM* 45.6 (Nov. 1998), pp. 965–981. ISSN: 0004-5411. DOI: 10.1145/293347.293350. URL: https://doi.org/10.1145/293347.293350.

[36] Luqin Wang et al. "A Fast Multi-Server, Multi-Block Private Information Retrieval Protocol". In: *2015 IEEE Global Communications Conference (GLOBECOM)*. 2015, pp. 1–6. DOI: 10.1109/GLOCOM.2015.7417246.

[37] Ronald L Rivest, Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems". In: *Communications of the ACM* 21.2 (1978), pp. 120–126.

[38] Craig Gentry. "Fully homomorphic encryption using ideal lattices". In: *Proceedings of the forty-first annual ACM symposium on Theory of computing*. 2009, pp. 169–178.

[39] Cem Dilmegani. *In-Depth Guide Into Secure Multi-Party Computation*. Accessed: 2022-12-15. URL: https://research.aimultiple.com/secure-multi-party-computation/.

[40] R. L. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Commun. ACM* 21.2 (Feb. 1978), pp. 120–126. ISSN: 0001-0782. DOI: 10.1145/359340.359342. URL: https://doi.org/10.1145/359340.359342.

[41] Qëndrim Fazliu. *Frankrig forbyder Office 365 og Google Workspace i skolerne*. Accessed: 2022-10-02. URL: https://www.computerworld.dk/art/263195/frankrig-forbyder-office-365-og-google-workspace-i-skolerne.

[42] danske lærerorganisationer international. *Holland og Google Workspace for Education - databeskyttelse*. Accessed: 2022-10-02. URL: http://www.dus.dk/media/1297/2022-10-dli-notat-holland-og-google-workspace-for-education-databeskyttelse.pdf.

[43] Microsoft Corp. *Microsoft Announces Plans to Offer Cloud Services from German Datacenters*. Accessed: 2022-11-2. URL: https://www.prnewswire.co.uk/news-releases/microsoft-announces-plans-to-offer-cloud-services-from-german-datacenters-545594412.html.

[44] David Curry. *Microsoft announces local data centers for German cloud users to avoid U.S. spies*. Accessed: 2022-11-2. URL: https://www.digitaltrends.com/computing/microsoft-german-data-centers/.

[45] Aja Romano. *The Facebook data breach wasn't a hack. It was a wake-up call.* Accessed: 2022-11-17. URL: https://www.vox.com/2018/3/20/17138756/facebook-data-breach-cambridge-analytica-explained.

[46] Harry Davies. *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*. Accessed: 2022-11-17. URL: https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

[47] Oliver Laughland Olivia Solon. *Cambridge Analytica closing after Facebook data harvesting scandal*. Accessed: 2022-11-17. URL: https://www.theguardian.com/uk-news/2018/may/02/cambridge-analytica-closing-down-after-facebook-row-reports-say.

[48] Sasha Ingber. *Cambridge Analytica is shutting down after Facebook data controversy.* Accessed: 2022-11-17. URL: https://www.npr.org/sections/thetwo-way/2018/05/02/607782799/cambridge-analytica-is-shutting-down-after-facebook-data-controversy.

[49] Sahana Venugopal. *What does Facebook's settlement in the Cambridge Analytica lawsuit mean for the platform?* Accessed: 2022-11-17. URL: https://www.npr.org/sections/thetwo-way/2018/05/02/607782799/cambridge-analytica-is-shutting-down-after-facebook-data-controversy.

[50] Federal Trade Comission (FTC). *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook.* Accessed: 2022-11-17. URL: https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

[51] Business World. *Meta Reaches $37.5 Mn Settlement Of Facebook Location Tracking Lawsuit.* Accessed: 2022-11-17. URL: https://www.businessworld.in/article/Meta-Reaches-37-5-Mn-Settlement-Of-Facebook-Location-Tracking-Lawsuit/24-08-2022-443460/.

[52] Reutors Davi Ruvic. *Ireland fines Instagram a record $400 mln over children's data.* Accessed: 2022-11-17. URL: https://www.reuters.com/technology/irish-regulator-fines-instagram-400-million-over-chidrens-data-2022-09-05/.

[53] Ltd. Peking University Legal Information Center Beijing Beida Yinghua Technology Co. *National Intelligence Law of the People's Republic of China. CLI.1.297110.* Accessed: 2022-11-21. URL: https://www.pkulaw.com/chl/297110.html?isFromV5=1.

[54] CNN Business. *TikTok makes clear European data can be accessed by China-based employees.* Accessed: 2022-11-21. URL: https://edition.cnn.com/2022/11/03/tech/tiktok-european-data-china-staff/index.html.

[55] TikTok. *Tiktok Global Operations and Data Transfers: Storage and Limited Remote Access within our Corporate Group.* Accessed: 2022-11-21. URL: https://www.tiktok.com/legal/page/eea/transferee-countries/en.

[56] Marianne von Blomberg. "The social credit system and China's rule of law". In: *Social Credit Rating.* Springer, 2020, pp. 111–137.

[57] Centre for IT and IP Law of KU Leuven. *Government access to datain third countries.* Accessed: 2022-11-21. URL: https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf.

[58] Zhizheng Wang. "Systematic government access to private-sector data in China". In: *International Data Privacy Law* 2.4 (2012), pp. 220–229.

[59] WebFX. *What is Google Analytics? Google Analytics Definition, Uses, Benefits, and More.* Accessed: 2022-11-28. URL: https://www.webfx.com/analytics/glossary/what-is-google-analytics/.

[60] Google. *IP Anonymization (or IP masking) in Universal Analytics.* Accessed: 2022-12-7. URL: https://support.google.com/analytics/answer/2763052?hl=en&ref_topic=2919631.

[61] Google. *How Google Analytics secures your web traffic.* Accessed: 2022-12-6. URL: https://support.google.com/analytics/answer/6385009?hl=en&ref_topic=1008008.

[62] GDPRhub. *DSB (Austria) - 2021-0.586.257 (D155.027).* Accessed: 2022-11-28. URL: https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2021-0.586.257_(D155.027).

[63] datatilsynet. *Press release: Use of Google Analytics for web analytics.* Accessed: 2022-11-28. URL: https://www.datatilsynet.dk/english/google-analytics/use-of-google-analytics-for-web-analytics.

[64] Google. *EU-focused data and privacy.* Accessed: 2022-12-8. URL: https://support.google.com/analytics/answer/12017362?hl=en.

[65] Google. *Best practices to avoid sending Personally Identifiable Information (PII).* Accessed: 2022-12-8. URL: https://support.google.com/analytics/answer/6366371hl=en&ref_topic=2919631#zippy=%5C%2Cin-this-article.

[66] Google. *Manage user consent.* Accessed: 2022-12-8. URL: https://support.google.com/analytics/answer/12329599?hl=en&ref%5C_topic=2919631.

[67] Anders Melchior Frigaard. *Chromebooks skal ud af folkeskoler.* Accessed: 2022-09-21. URL: https://www.dr.dk/nyheder/indland/chromebooks-skal-ud-af-folkeskoler-kan-ikke-garantere-elevers-data-ikke-havner-i-de.

[68] Google. *Introduction of Google Workspace Education.* Accessed: 2022-09-21. URL: https://workspaceupdates.googleblog.com/2021/02/introducing-google-workspace-for-education.html.

[69] Google. *GOOGLE WORKSPACE FOR EDUCATION PRIVACY NOTICE.* 2022. URL: https://workspace.google.com/terms/education_privacy.html#privacy-police-revamp-intro.

[70] Google. *What you can do with Google Workspace for Education paid editions (Full version).* Accessed: 2022-11-2. URL: https://www.youtube.com/watch?v=qdhQ3XGlrsk.

[71] Louise Olifent. *Fra vred far til kommuner i krise: Få overblikket i Helsingørsagen.* Accessed: 2022-10-09. URL: https://www.version2.dk/artikel/fra-vred-far-til-kommuner-i-krise-faa-overblikket-i-helsingoersagen?check_logged_in=1.

[72] Århus Kommune Børn og Unge. *Chromebooks til eleverne.* Accessed: 2022-10-02. URL: https://detvigoer.aarhus.dk/faelles-rammer/digitalisering/chromebooks-til-eleverne/.

[73] Version2. *Skarp kritik af Aarhus Kommune: Sender skolebørns data ulovligt til Google.* Accessed: 2022-10-02. URL: https://www.version2.dk/artikel/skarp-kritik-af-aarhus-kommune-sender-skoleboerns-data-ulovligt-til-google.

[74] Helsingør Kommune. *Konsekvensanalyse for Google Chromebooks og G-Suite for Education.* Accessed: 2022-10-03. URL: https://images.radarmedia.dk/app/uploads/2022/08/Konsekvensanalyse-DPIA_Chromebook-Workspace.pdf.

[75] Datatilsynet. *Alvorlig kritik af Helsingør Kommune i Chromebook-sag.* Accessed: 2022-09-29. URL: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/sep/afgoerelse-vedroerende-brud-paa-persondatasikkerheden.

[76] Århus Kommune Børn og Unge. *Eksperter undrer sig over Helsingør i Chromebook-sag: De har misforstået konsekvensanalyse.* Accessed: 2022-10-03. URL: https://radarmedia.dk/eksperter-undrer-sig-over-helsingoer-i-chromebook-sag-de-har-misforstaaet-konsekvensanalyse/.

[77] Berlingske. *Byråd i Helsingør sætter stop for brug af Chromebook.* Accessed: 2022-10-04. URL: https://www.berlingske.dk/danmark/byraad-i-helsingoer-saetter-stop-for-brug-af-chromebook.

[78] Version2 Louise Olifent. *KL holder hemmeligt Chromebook-krisemøde for kommunerne.* Accessed: 2022-10-04. URL: https://www.version2.dk/artikel/kl-holder-hemmeligt-chromebook-krisemoede-kommunerne.

[79] Datatilsynet. *Datatilsynet fastholder forbud i Chromebook-sag.* Accessed: 2022-10-04. URL: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/aug/datatilsynet-fastholder-forbud-i-chromebook-sag.

[80] Datatilsynet. *Yderligere materiale udsætter afgørelse om Chromebooks.* Accessed: 2022-12-13. URL: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/dec/yderligere-materiale-udsaetter-afgoerelse-om-chromebooks.

[81] Erhvervsstyrelsen. *Nyt IT-risikovurderingsværktøj skal hjælpe virksomheder med at styrke deres digitale sikkerhed.* Accessed: 2022-12-5. URL: https://erhvervsstyrelsen.dk/nyt-it-risikovurderingsvaerktoej-skal-hjaelpe-virksomheder-med-styrke-deres-digitale-sikkerhed.

[82] Privat Company. *DPIA on the use of Google G Suite (Enterprise) for Education.* Accessed: 2022-11-02. URL: https://www.surf.nl/files/2021-06/updated-g-suite-for-education-dpia-12-march-2021.pdf.

[83] Niels-Peter Kjølbye. *Understanding the Danish Chromebook-case.* Accessed: 2022-12-14. URL: https://openli.com/community-posts/understanding-the-danish-chromebook-case.

[84] Version2 Louise Olifent. *Datatilsynet om Helsingørs Google-forklaring: »Man kan ikke bare tro på sin leverandør«.* Accessed: 2022-11-02. URL: https://www.version2.dk/artikel/datatilsynet-om-helsingoers-google-forklaring-man-kan-ikke-bare-tro-paa-sin-leverandoer.

[85] Guilia Interesse China Briefing. *China's Cloud Computing Market: Developments and Opportunities for Foreign Players.* Accessed: 2022-12-15. URL: https://www.china-briefing.com/news/chinas-cloud-computing-developments-and-opportunities/.

[86] Microsoft. *Microsoft Azure operated by 21Vianet.* Accessed: 2022-12-15. URL: https://learn.microsoft.com/en-us/azure/china/overview-operations.

[87] Amazon. *Amazon Web Services in China.* Accessed: 2022-12-15. URL: https://www.amazonaws.cn/en/about-aws/china/.

[88] Jesper Knudsen. *Professor: Kommuner kan løse Chromebook-problemer med gratis styresystem.* Accessed: 2022-12-20. URL: https://www.folkeskolen.dk/chromebook-helsingor-kommune-it/professor-kommuner-kan-lose-chromebook-problemer-med-gratis-styresystem/4667392.

[89] The White House. *FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework.* Accessed: 2022-12-20. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.

[90] Aleksandra Szczepańska. *Privacy Shield 2.0: What it is and how it will affect your business.* Accessed: 2022-12-20. URL: https://piwik.pro/blog/privacy-shield-2-0-what-it-is-and-how-it-will-affect-your-business/#the-european-union-us-data-privacy-framework-called-privacy-shield-2.0:-what-we-know-so-far.

[91] Deloitte. *ePrivacy Regulation - The current state of play.* Accessed: 2022-12-20. URL: https://www2.deloitte.com/nl/nl/pages/risk/articles/eprivacy-regulation.html.

[92] European Comission. *Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment.* Accessed: 2022-12-20. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545.

[93] Elisa Pirkova. *The Digital Services Act: your guide to the EU's new content moderation rules.* Accessed: 2022-12-20. URL: https://www.accessnow.org/digital-services-act-eu-content-moderation-rules-guide/.

[94] European Comission. *Digital Markets Act: rules for digital gatekeepers to ensure open markets enter into force.* Accessed: 2022-12-20. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6423.

[95] 360Advanced. *SOC® Reports*. 2022. URL: https://360advanced.com/our-services/soc-reports/.

[96] Google. *Google Workspace security whitepaper*. Accessed: 2022-09-21. URL: https://workspace.google.com/learn-more/security/security-whitepaper/page-5.html.

[97] ISO. *ISO/IEC Standards*. Accessed: 2022-09-21. URL: https://www.iso.org/standards.html.

[98] ISO. *ISO/IEC 27001 and related standards Information security management*. Accessed: 2022-09-21. URL: https://www.iso.org/isoiec-27001-information-security.html.

Appendix A

Prepared questions for Ole Kjeldsen

Introduction:

- What is your background, and position?
- How does Microsoft collect and store data?
  - Is there a difference between collecting data according to GDPR oppposed to outside the EU?
- How does Microsoft confine data within the EU?
  - Can any entity outside the EU lawfully request that EU data?
- Who audits cloud providers in general?
  - In Microsoft's experience, how has EU done auditing on its business?

EU Data Boundary

- What is the EU Data Boundary project?
- How much does it cost to build infrastructure in the EU?
- How many servers did you build for that project?
- Which consideration did Microsoft have for the EU Data Boundary? These considerations could be privacy, security, etc.
- Who decides what EU data should be processed?

Microsoft-Germany

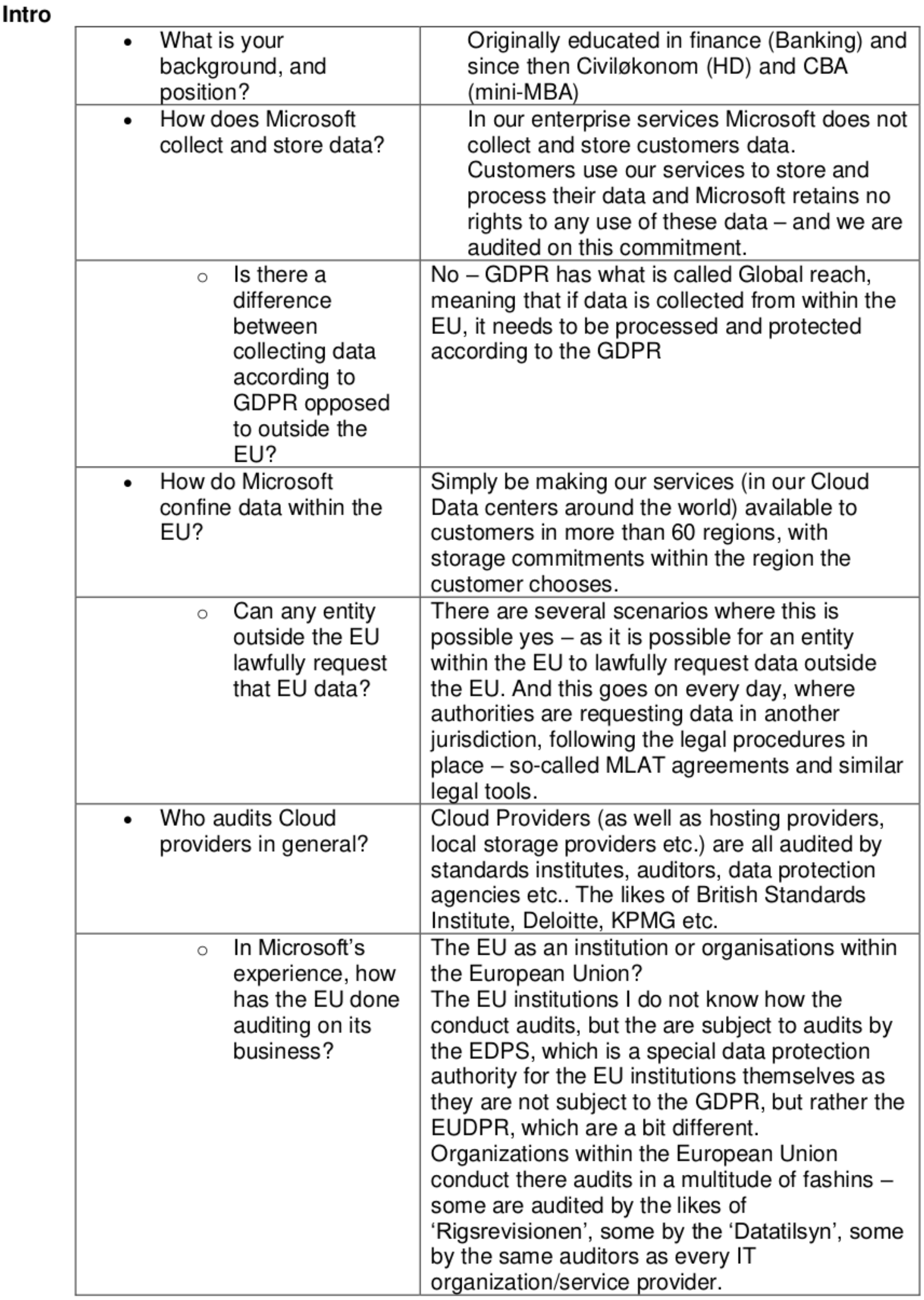
- What was the reason for the termination of that custom contract?
- Does Microsoft plan to license/rent its own assets to companies in each of the EU countries?
- What is Microsoft policy/view on how much control countries should have on their own data?

Chromebook

- Is there a Microsoft product which complies with GDPR in Denmark which can replace Google Workspace for students?
- Given Chromebook-gate, do you see Google complying to GDPR as Microsoft has/is doing? Or more precisely for the use of Google products in elementary schools.

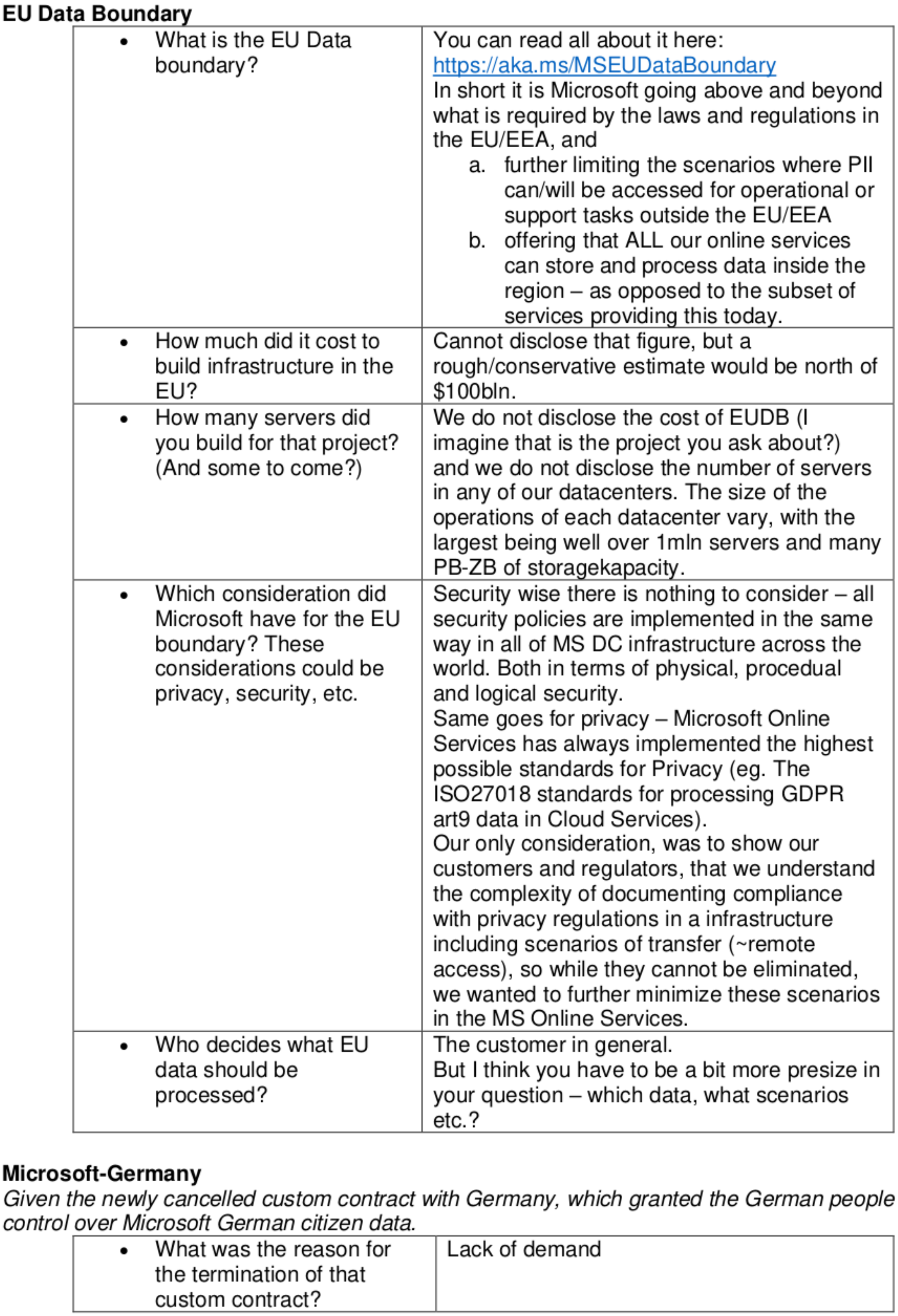
Appendix B

Ole Kjeldsen - Written answers



Intro

• What is your background, and position?	Originally educated in finance (Banking) and since then Civiløkonom (HD) and CBA (mini-MBA)
• How does Microsoft collect and store data?	In our enterprise services Microsoft does not collect and store customers data. Customers use our services to store and process their data and Microsoft retains no rights to any use of these data – and we are audited on this commitment.
○ Is there a difference between collecting data according to GDPR opposed to outside the EU?	No – GDPR has what is called Global reach, meaning that if data is collected from within the EU, it needs to be processed and protected according to the GDPR
• How do Microsoft confine data within the EU?	Simply be making our services (in our Cloud Data centers around the world) available to customers in more than 60 regions, with storage commitments within the region the customer chooses.
○ Can any entity outside the EU lawfully request that EU data?	There are several scenarios where this is possible yes – as it is possible for an entity within the EU to lawfully request data outside the EU. And this goes on every day, where authorities are requesting data in another jurisdiction, following the legal procedures in place – so-called MLAT agreements and similar legal tools.
• Who audits Cloud providers in general?	Cloud Providers (as well as hosting providers, local storage providers etc.) are all audited by standards institutes, auditors, data protection agencies etc.. The likes of British Standards Institute, Deloitte, KPMG etc.
○ In Microsoft's experience, how has the EU done auditing on its business?	The EU as an institution or organisations within the European Union? The EU institutions I do not know how the conduct audits, but the are subject to audits by the EDPS, which is a special data protection authority for the EU institutions themselves as they are not subject to the GDPR, but rather the EUDPR, which are a bit different. Organizations within the European Union conduct there audits in a multitude of fashins – some are audited by the likes of 'Rigsrevisionen', some by the 'Datatilsyn', some by the same auditors as every IT organization/service provider.



EU Data Boundary

• What is the EU Data boundary?	You can read all about it here: https://aka.ms/MSEUDataBoundary In short it is Microsoft going above and beyond what is required by the laws and regulations in the EU/EEA, and a. further limiting the scenarios where PII can/will be accessed for operational or support tasks outside the EU/EEA b. offering that ALL our online services can store and process data inside the region – as opposed to the subset of services providing this today.
• How much did it cost to build infrastructure in the EU?	Cannot disclose that figure, but a rough/conservative estimate would be north of $100bln.
• How many servers did you build for that project? (And some to come?)	We do not disclose the cost of EUDB (I imagine that is the project you ask about?) and we do not disclose the number of servers in any of our datacenters. The size of the operations of each datacenter vary, with the largest being well over 1mln servers and many PB-ZB of storagekapacity.
• Which consideration did Microsoft have for the EU boundary? These considerations could be privacy, security, etc.	Security wise there is nothing to consider – all security policies are implemented in the same way in all of MS DC infrastructure across the world. Both in terms of physical, procedual and logical security. Same goes for privacy – Microsoft Online Services has always implemented the highest possible standards for Privacy (eg. The ISO27018 standards for processing GDPR art9 data in Cloud Services). Our only consideration, was to show our customers and regulators, that we understand the complexity of documenting compliance with privacy regulations in a infrastructure including scenarios of transfer (~remote access), so while they cannot be eliminated, we wanted to further minimize these scenarios in the MS Online Services.
• Who decides what EU data should be processed?	The customer in general. But I think you have to be a bit more presize in your question – which data, what scenarios etc.?

Microsoft-Germany

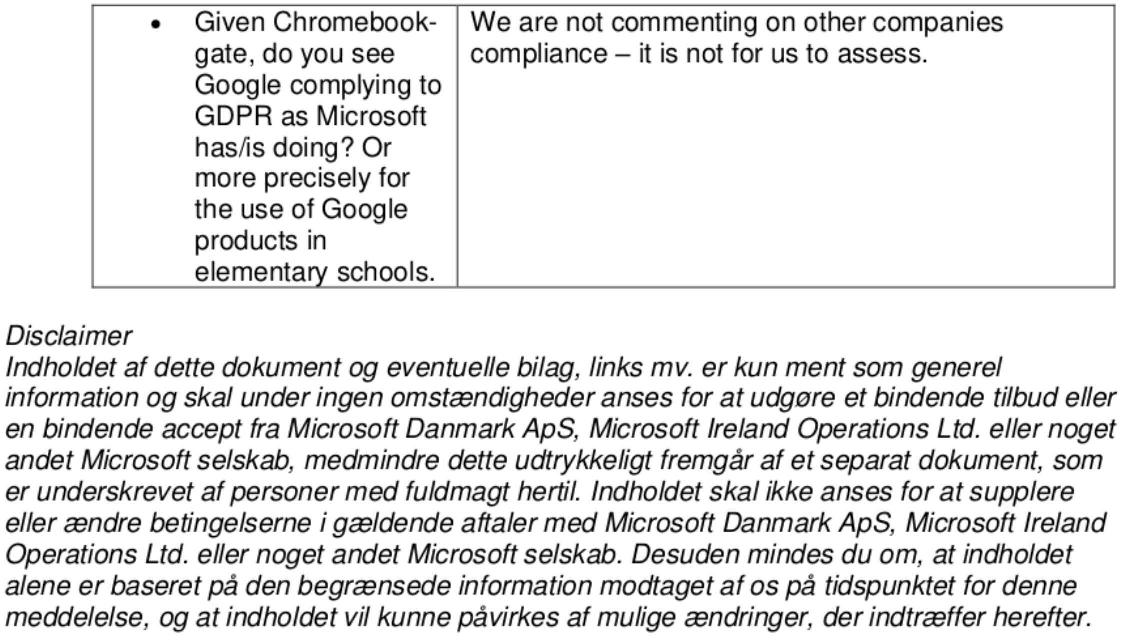
Given the newly cancelled custom contract with Germany, which granted the German people control over Microsoft German citizen data.

• What was the reason for the termination of that custom contract?	Lack of demand

• Does Microsoft plan to license/rent its own assets to companies in each of the EU countries?	If you mean, having a local/national provider to act as the operator of a MS facility, the answer is no. No regulation in the EU requires this setup, and history has proven it is neither in high demand nor does it provide any added security or privacy protection.
• What is Microsoft policy/view on how much control countries should have on their own data?	This I believe is best answered in the blog posts of our Privacy Officer Julie Brill – here links to three of those that clearly states the Microsoft position on those matters: - Increasing transparency and customer control over data - Microsoft On the Issues - Assuring Customers About Cross-Border Data Flows (microsoft.com) - Protecting our data infrastructure through some new approaches to privacy - Microsoft On the Issues

Chromebook

• Is there a Microsoft product which complies with GDPR in Denmark which can replace Google Workspace for students?	I belive yes – remember - I cannot state that the Google workspace for students is incompliant and while I understand your to be a result of the 'Chromebook' case in the city of Elsinore, I have to remind you to read the Data Protection Authority decisions once more – in the end this is about the legal and technical implementation and preparation by the organization and not a decision of wether a online service itself is compliant or not, - And I cannot guarantee any compliance implementing any product/solution – it will always be up to the actual case, how you assess, prepare, configure, use etc. the service/product. The laws, regulations AND decisions by the DPA does not evaluate a product or service, but exactly that – its implementation. The laws are technology neutral – highlighted by the DPA several times! But I believe a customer would be able to implement "Microsoft 365 Education - Service Descriptions | Microsoft Learn" in a compliant manner.



- Given Chromebook-gate, do you see Google complying to GDPR as Microsoft has/is doing? Or more precisely for the use of Google products in elementary schools.	We are not commenting on other companies compliance – it is not for us to assess.

Disclaimer
Indholdet af dette dokument og eventuelle bilag, links mv. er kun ment som generel information og skal under ingen omstændigheder anses for at udgøre et bindende tilbud eller en bindende accept fra Microsoft Danmark ApS, Microsoft Ireland Operations Ltd. eller noget andet Microsoft selskab, medmindre dette udtrykkeligt fremgår af et separat dokument, som er underskrevet af personer med fuldmagt hertil. Indholdet skal ikke anses for at supplere eller ændre betingelserne i gældende aftaler med Microsoft Danmark ApS, Microsoft Ireland Operations Ltd. eller noget andet Microsoft selskab. Desuden mindes du om, at indholdet alene er baseret på den begrænsede information modtaget af os på tidspunktet for denne meddelelse, og at indholdet vil kunne påvirkes af mulige ændringer, der indtræffer herefter.

Appendix C

Ole Kjeldsen Interview

Hac: I think maybe we can start lightly. Yeah. Uh, maybe we can start by speaking a bit about yourself. A bit about yourself. Uh, what is your background and your position? Mm-hmm. . So,

Ole: um, I'm, I'm 55. I, um, I straight out of, uh, high school at Gymnasium. Um, I went into banking, this is back in the eighties.

Uh, so I took a, uh, banking degree, worked, uh, for about 12 days in banking. Then I joined the military services, and I was there a year and a half. Um, came back to banking. Did, uh, I was a, a trader. So FX, uh, futures options, simply speculative deals for the bank. Mm-hmm. investing, you would call it. But, uh, So derivatives, futures, options, all that.

uh, I did that for, uh, 14, 13 years. Um, primarily Copenhagen, but I had a few posts in Luxembourg in the UK and the US three years, uh, back in the nineties. Um, at that point I was, uh, fed up. I, I want to do something else. I love programming. I taught myself to program. I built a ton of systems, trading systems for the bank I worked for.

Okay. Um, and I wanted to change careers. I didn't wanna do financing, I thought was a whole little bit big??, great fun on Wall Street, but still I wanted to do something other with my life. Um, and by chance, uh, a head hunter back then contacted me and said, well, we see, you know, a bit of this, you know a lot of that.

Why don't you, I think I have a job for you. . So I met back then, Microsoft was a very small company in Denmark. 28 people, I think I was number 28. Uh, and the CEO, the director for Microsoft, Denmark, came into this meeting and was just an amazing person. Uh, so I said, sure, I'll, I took a pay cut, a huge pay cut, uh, but I wanted to work for this guy.

So I started back in 2000 and, um, haven't looked back. So I took a, uh, HD. So, uh, I guess Danish we call it Civiløkonom. And then, um, I took a, a mini MBA during the first couple of years with, uh, with Microsoft. So I've been, I'm now on my 23rd year, uh, in Microsoft, um, working, uh, primarily in technical, uh, capacity.

I was the head of development in Microsoft for a couple of years. Um, . And then I think two weeks before Snowden, back in 2013, July, 2013, uh, I had had so many, like I said, uh, student workers, a ton of employees, and I've done all that. And I looked at the CEO here and said, I want to do something else. I think that my skills are better used than doing people management.

I wanna do something strategic. So we created a new position for me, director of technology, where I could look into the future, try to inspire people about new technology, cloud was just a thought back then. And two weeks later, Snowden broke, all the 1.2 million documents, a ton of work on PRISM, on, um, key key, um, X key score and all those.

Everything, privacy, compliance and security related. And, uh, at the board of directors in Microsoft, uh, we just looked around. I was the only technical person you, "you are it", so I started to focus on cyber security or privacy and all that. And I've been doing that since, uh, 2013. And I would love to talk much more about future technology, quantum AI, I do, but it's such a small part of what I do today. 98% of my time goes more talking about cybersecurity a little bit, but primarily about compliance, legal, compliance technology, doing risk assessments with customers, making sure they understand all the moving parts in the cloud and in legislation. So that's what I do now.

Hac: I think maybe it would be wise now to actually, uh, speak about with position we, uh, are in asking these questions. So as you know, we briefly mentioned before, we are looking into the, uh, transferring of data issue with the outside, uh, EU and, uh, what problems comes with it, and, you know, the fundamental issues that we have had that these two policies, specifically the US, are colliding. So these, these questions are somewhat, not vague, but maybe they can be seen as such. Uh, so please, please, uh, answer them freely and then maybe we have a follow up question.

Ole: Of course.

Hac: So the first question is, uh, how does Microsoft collect and store data? So what is the process of it?

Ole: right, Um, Microsoft, I mean, I'm just gonna talk about our enterprise service. The commercial services consumer is different, but for, uh, the Microsoft Commercial Services, those that our customers are using, like a municipality using Microsoft 365 for their email, intranet, sharing, online meetings, all that for those services. Microsoft does not collect, install data. The customers are creating their own data. They're uploading, they're downloading their processing. It's all being created in their container. A tenant, we call it. What we, of course, any service, Microsoft Online Services does the same thing. They do collect logging data, so whenever Ole logs on it happens at a given point of time, it happens from an IP address depending on the service I log onto, there's a login. Right. So all from this IP address at this point, logged onto Exchange. Uh, he synchronized two gigs of data. That's a log entry. Now we don't collect what it is all is doing up there. We don't collect what emails did he send you? Uh, who did he send to? What's the content, but the lock entry of what we call service generated data, this happened. And that could also be one, one service calling, another service could be a, a look up in a database, uh, returning some, some data, all kinds of transaction that goes on in a service is of course part of this, uh, service generated data.

That's all log entries. These data are primarily used for the customer's own administration. They have an administration portal. They have a couple of administrators who of course, then looking at their tenants saying, well, Hannah, Bent, and Anna all have access to this. We need to add Ole to it as well so he can see that SharePoint side, that's their own administration.

That's all using these logs of course to see what's going on in their own tenants. For what we call business operations, under GDPR, article 6 page 1 litre F?? there's something called legitimate business operations. So if it's legitimate for your process, and Microsoft is data processing in this case, a municipality use M365 legitimate business interest could be we need to send them an invoice.

The only reason or the only data we need for that is how many unique users, how many transactions, how much data back and forth, what were they using, what service were they using? all this is when it's created. Of course, personal identifiable because it's Ole, Hanne, Bent. Now we aggregate all this because we don't care that it's Ole, Hanne, Bent.

We just want unique users. So we hash this meaning instead of Ole, Hanne, Bent, we use a mathematical hash 256 bit characters. And then we aggregate it and say, well, customer X has had 120 unique users. This is how much they transacted. That all adds up to their bill. The only personal identifiable information we have on that is who should we send the invoice to?

And there's, uh, four or five of these legitimate business operations where we do collect data. We've, uh, published how we process that data, how do we aggregate, how do we pseudonymize, um, and what can we do with this data? Meaning we can't profile, we can't do marketing, we can do capacity planning, we can fix errors, we can make sure there are no security vulnerabilities and we can send them invoices.

It's very clear from our DPA what we can and can't do with this data. So that's the data we collect.

Hac: Okay. Is there any difference? You, you mentioned there's a commercial and then there's a consumer.

Ole: Yep.

Hac: Let's say if a company pays for, um, you know, the enterprise package, and then there's the outlook, and then there's an consumer Jens in Herlev who uses Outlook.

Ole: Thats two different scenarios. Yeah. if you have a, now in our data centers, we run both. We run them, uh, I guess you could say in parallel. So of course a data center is just a huge line of racks??, right? With ton of servers, VPNs, network, whatever. Now in our data centers, you will see what we call, um, high business impact, and then we have low business impact. Now, they are separated in different halls in our data centers. Low business impact are those that we know are not containing any personal identifiable information. It's our own internal systems. We know that we are keeping these separate, high business impact if they are customer data.

Hac: So these are actually servers?

Ole: These are servers. I mean the cloud is just servers, right? The cloud is just Humongous data service. We're building three on scene, actually, uh, in the moment. They'll be operational within a couple of years.

Hac: So they are separated and they don't speak with each other?

Ole: No. And even in high business, we have consumer services and then we have commercial services.

The reason why these are different is that these racks over. And it's not just one rack, right? These are soccer fields, maybe soccer fields wise, the services running on these needs to be not just cutting edge, but beyond cutting edge.

This consumer (racks) is something we run ourselves, right? So this is Hotmail, this is Xbox Live.

And so on all the, the consumer services we run, we decide ourselves because here in consumer services, MS is data controller in terms of GDPR. For commercial MS is data processes. So these we handle for these. Most of them are free services. We do have consumers who pay to avoid advertising, for instance.

But we are data controllers over here, meaning, yep. Here we collect much more. We are the administrators. We have separate personnel who does nothing other than administer all this. And that's a one to 1 billion users over here. We are not administrators other than the hypervisor layer, so the virtualization hypervisor.

And for some we also have the app layer and the database layer. Those are software as a service solutions like M 365. Right. If people use Azure, we don't have the app and database layer. We only have access to the high device??. But, um, what the, oh yeah, we collect here, we collect nothing. Other than the log, we only use the log for the business operations, what is needed to provide the service, invoicing, capacity planning, security, all that.

The rest, this is customer data. This is what the customer uploads creates in their own tenants. We don't have access to it. We don't want access to it. If, and it happens occasionally. I've had these, uh, customers who for five years never had that scenario, but it could happen that at some point they have a support request or something odd happens in the, uh, customer data tenant.

They ask us what I, we need to get privileges, meaning we can see their data in clear text. That's why I say we then have to ask them, are you okay with this? This is what lead doing it in Frankfurt, and the customer then accepts or rejects or whatever, but we don't have access to customer data. The only thing we collect are locks and aggregated locks, so statistics.

Hac: is, uh, it is the same model, uh, that, uh, was, uh, was at, at hand when Sweden, for example, as some other country, they actually banned some of their Microsoft services.

Ole: Two things about Sweden. Uh, one thing is they have a, uh, I think it's called OMA?. They have a separate, uh, separate law governing public sector. What kind of services and how they can use, uh, so that's a special Swedish law doesn't apply to Denmark. That was the basis for the city of Stockholm making a decision. We can't use the cloud service. We don't have that law in Denmark. The only thing we have in Danish law is the, um, the Danish, again, data Protection Act data, "databeskyttelsesloven, uh, article 9 section three. This is called in daily talking, the location demand.

That paragraph says, if a system is of vital national security interest, the server running it has to be on Danish ground. Now, you can export data on the GDPR as you want, but the server running the system is critical national security. So it has to remain on Danish soil. The reasoning is the military needs to be able to move out and secure it with awareness, right. Now, this is a, um, a positive list, and right now there are six systems, only six systems. Whenever you renew a, it's only public sector. And it's only those six systems. If you renew a system, build a new system, or renew it, build it on a new architecture, you have to assess if it's subject to occasionally??, but they are only six systems and these hardly have any data in it.

Not even the CPR system is on that list. No, CPR is not a a special, we only have two kinds of data now on the GDPR. We have normal, personal identifiable information and special. And special isn't CPR. It says nothing about you except your birthday. It's so easy to find everybody's CPR number if you want.

You can't authenticate with the CPR number. That's why we have been med nemid and MitID .

Farhan: Yeah. So just to be clear on that, who will be the data controller on the commercial deal, commercial perspective?

Ole: That's the customer. That's the one. Who will the processor in in Microsoft.

Yeah, we are. Yeah, we, yeah, we're both, but I mean, there's no doubt as data control much higher demands on you and we don't, uh, use third parties.

So we are the process. Yeah. What, I'm sorry. Nope, please go.

Farhan:I had just another question, which is, um, we have been talking about data transfers. So what is actually data transfers? Like taking the hardwares from one server and transporting it physically to us or itself,

Ole: If we did that, but we don't, the data transfers that happens. Good question. So what are data transfers in this scenario? I'm not looking at consumers now, separate thing. Data transfers that could happen. There are four scenarios, potential. There are potential, uh, support or operations outside EU.

So that's the scenario. Molik?? sits in New York. It's a Danish customer. It's out our allow? in Denmark what he needs to do, something he remotes accesses. That's a transfer,lLegal terms, that's a potential. Now we ask Cut customer?. We have one called customer lockbox. It's a service we built about 10 years ago saying if that happens when he needs to do this, he would be able to see the customer's data.

We then would, uh, request from the customer. Excellent. The customer can say, no, we don't want that. They can say, yep, go ahead. We'll follow the lock. We'll see what Will does. Nothing risky. All they could say, it's not critical. Why don't we wait until Heinz in Frankfurt is available and we'll do that when Heinz ops?? fine.

If it's critical, you would probably want it to do it and be happening anyway and remind yourself. Data transfers are not unlawful. You can still do. You just have to make, take your precautions. You have to assess is this happening within the, the frame of the law and our, we would stipulate absolutely it is.

We have implemented a ton of security controls. The customer can follow the law, they can document. Nothing happened here. It can't be part of FISA 702 because it's a one point how the on earth would NSA know that will lead would have the opportunity to gain access to that particular customer that they need, uh, data.

And even if they did what lead, we have our own lockbox. So lockbox is a Microsoft internal process. Any time any engineers needs to go in and do anything on customer data, that's customer lockbox. And down here it's lockbox. Down here you can't see that customer data. You can only see the logs.

You wouldn't have access to what is considered personal. The Microsoft lockbox is if we lead, were pressured by some, let's say, intelligence agency saying you should get access to the business authority in Denmark. Their data. So we'll lead dreams of a business justification cause he doesn't have access and he can't gain access unless he goes through the Microsoft.

He says, well, okay, I need access to this 10 because then he has to do a business justification. Why do I need to do this? Why do I need these privileges? What are the tests that I need to go do and how long do I assess that will take me? It then goes to a managerial level at Microsoft saying, funny, we haven't seen any of these indicators.

Why should I don't understand your business? Uh, justification. And you are asking for all these permissions. You don't need that to, I mean, there's so many questions that will be asked if that fails. If that fails and a Microsoft manager still says, great money, go ahead and do your stuff. If well then tries to exit customer data, the customer lockbox that steps in.

Now it's not a manager, Microsoft, now it's the custom. Who's to say, why is believe doing this? I don't think so. So again, if they are under pressure by some intelligence services, there's so many controls steps that they have to walk through. So many things where it has to break down until it could happen.

Hac: Does Microsoft have access to this data?

Ole: which data?

Hac: like, uh, to this, uh, to, you know, entering the lock box without the consent? Somehow

Ole: we are getting to the, uh, so that's the first scenario. That's everyday support and operations. That's the first scenario. Second scenario is if we have, uh, business continuity, a tsunami hits island and Amsterdam, or at once a nuclear bomb hits Frankfurt, what do we do?

We need to make sure our service is available. Now, we've given commitment. We are certified on this as a separate ISO standard for doing business continuity. If we have business continuity, all help break loose in Ireland, we have ways of making sure the service available inside.

So it'll move to Frankfurt, it'll move to the UK, which is still a safe third country. We have so much capacity in the business. Continuity is not a problem. And even, even if it, let's say, I think we have more pressing problems than privacy.

Farhan: Is it called availability pairs?

Ole: Um, well, no availability pairs are already, I mean that's, this is Microsoft business consumer.

So this is what we do as a processers to be able to say to people, even if there's a huge crisis, a natural catastrophe, we will make sure your business can continue, you will still have availability, but the customer themselves can architect their solution using availability zones saying, we want to make sure that we don't only use the Dans data centers, we want to have a live backup, a hot backup in Melbourne where Microsoft data centers, so they mirror their solution in a data center region close by.

but we do it saying, look, if both Copenhagen and member are down, we will make sure that we move everything to Berlin, Frankfurt, Amsterdam, whatever. So yeah, the customer has some architectural, uh, tools they can use. But this is, uh, a top. So next, uh, potential is what we call law enforcement, um, or National Security Orders.

And again, globally, also dangerous authorities, German, Australia, all authorities have intelligent services and law enforcement who continuously ask us. Now we, the last, the first six months of, uh, 2022. I can't remember the exact number, but actually I think it's the, almost the same as the executive order I mentioned before, I think we got a hundred and, uh, 225,186 request.

Ment and National security Audits. Mm-hmm. . You want to guess how many were for consumers and how many were for commercial? What's the commission? No. . Yeah. Cause And 21 over here? Mm-hmm. over here. 25,000 and, hmm. 65.

You want to know how many of these actually ended up in us handing on the data to authorities? 5, 3 0. That's so we give out transparency report. When I say zero, that was just the first six months. The six months before that, that number was three.

Hac: But are you even allowed to, yeah. You allowed to say no?

Ole: We fought back in 2010 to 12. We fought hard to be able to disclose these numbers. Now you're probably gonna say gag orders. What about gag orders or confidentiality? Because we are getting those also from D authorities. It's, it's in all uh, uh, judicial systems in Western Europe that, uh, intelligence and police can of course hand you a gang on saying you can inform order that you are investigating sense or anybody it makes sense or anybody.

Yeah. Uh, absolutely makes sense. We thought to be able to include those G orders in our reports and back in 2012 we won. They told us, sure, so this is including gag orders, so 200 of those 20,000 of those could have gag orders on, but we can still say we got that annual request. We just can't tell the individual the si the last six months of 2021.

There were three, we most likely couldn't tell three cuz it was a front for terrorism or whatever. And of course, We want to serve the police and intelligence agencies. If it's a proven terrorist orientation or a human trafficking organization, we don't see that as a violation of gdpr. Just recall, GDPR also says, well, national security.

Yeah. Criminal intent. You can't claim, you can't look into my data yet. Cause you're a criminal. I mean, we don't have an absolute right to privacy. If we could, I wouldn't pay taxes. Uh, so of course we can limit the privacy if it's criminal intent, if it's terrorism, if it's important, crime or violent crime.

And we will continue to do that and no authority would say you shouldn't do that. Microsoft. Mm-hmm. , of course we should co-op who's, uh, not co-op. Uh, well, any organization here who has personal data are getting these requests. Co-op, definitely. Cuz co-op has payment insurance. Mm-hmm. So if they are, uh, Having me unders scrutiny.

They know my Visa card number, they know my Dan card number. Of course, they want to know where have I been. They'll go to court and say, has this credit card been used in your business?

And they'll find out and they can then pinpoint, yeah, we'll spend in all these stores at this time. Of course they do. They should be able to

Hac: Or selling?

Ole: I'm sorry?

Hac: Selling.

Ole: Oh, selling. Yeah. Selling.

Yeah. I mean any a bank, uh, uh, cinemas, I mean, any business that has any personal identifiable information can be served. Such orders, warrants, uh, court orders. And of course we should have, but there are no back doors. There are no looking.

But I just want to say when it comes to law enforcement and national security laws, because they're gaggles Yeah. We can circumvent customer.

Hac: Okay.

Ole: Because if we couldn't, customers would inform the person that we can inform. So we can go behind it, but this is certified, it's audited by a third party. So we have Deloitte Kpmd going through our operations saying, well, yeah, for all this day to day business, absolutely custom outlook stops every access until the customer has accepted. Now law enforcement, separate matter.

Hac: Uh, going back to my question.

Hac: Yeah. So can, can Microsoft see the, the content of the lockbox in clear text, or does there need to be some kind of, uh, consumer, uh, influence on this?

Ole: Um, the customer lockbox is something we create. Yeah. So we can see that. But until the customer accepts the customer lockbox request, nobody from Microsoft goes above this layer. We can only get access to customer data if the customer has accepted.

Hac: Okay. But so you can see it, I mean, you can access it in theory without the consumer's consent.

Ole: Yeah, for law enforcement and national security.

Hac: I got that. Thank you.

David: So what's the fourth scenario for data transfer?

Ole: You remember? Good, because these, these are potential, we know one that is actually taking place every day. And that's back to, uh, databases, log data, log data. Now this is not your concept, this is all lot. On his IP address, it took four milliseconds. He used this feature. That's all that we are using for invoicing, capacity planning, security.

David: It's also for your own services.

Ole: Exactly. Now, just for security, we process, hold on. 43 billion, not million, I'm sorry. 43 trillion. So not million. Not billion. Trillion, billion på dansk. So security signals daily. So is anybody looking at security signals? Sure. We're letting the machines analyze that.

Looking for patterns. Looking to, okay, so there's a side attack happening in Tokyo at the moment. They're using this tool. We might want to have more resilience in New York or in Amsterdam, cuz it might spread into the rest of it. This is one of the primary reasons except for cost. Cause it is cheaper, but this is one of the primary reasons customers are even looking at top.

Because having resilience against modern cybersecurity threats, it's a humongous task. And we have a global organization with more than eight and a half thousand security professionals who does nothing but trying to keep the platform secure.

Farhan: Is it security Soc Actually?

Ole: I'm sorry?

Farhan: Is it SOC?

So that's one thing. Yeah. We uh, we actually call it Defense Operation Center. Um, but it is a security operation center. We have one call, a cyber defense operations center that sits in Redman outside of Seattle. Um, they get, uh, from, there are like 13 swimming services, all these services. They get all the signals even from them. They do the analysis and then they post out to people like me. Uh, and I keep the incentive for cybersecurity and them on informed, they have the feed on all the vulnerabilities. We see all those threats we see. So, yeah, this happens on a database. When I say that most of it is pseudonymized.

David:generalized?

Ole: Aggregated, For these real data. It. Okay. We were asked by the Dutch, uh, ministry of Justice to be data controls and said, we can do that. So we adhere to GDPR terms about, uh, data minimization, only the data that you actually need to ship and collect anything more should process, blah, blah, blah. Uh, data retention, and of course, uh, security policies, so all that blah, blah, blah. There's so much that we have to be able to document that we have to document.

David: As a cloud service provider, what would you say are your biggest challenges?

Ole: Biggest challenges, um,

David: Complying to GDPR?

Ole: No, it's not. In all honesty. No, we took the stands seven years ago. We want to be GDPR compliant. We want to be globally cuz there's a global mandate in gdpr. So it doesn't matter if you buy our services in South Africa, in the us, in Argentina, in Denmark, or it's the same service. It's all GDPR complied.

It's all run as if it was in the year. Okay. But that's us and the service being complied once our customers start using it, if they don't. Do their due diligence. They don't do their risk assessments. They don't do their What is suitable? What is proportional. They can be in compliant with first, second name, use our, so we have what we call a shared responsibility model, meaning, yeah, we'll take care of all the basics.

Depending on what service you use. If use M 365, we have everything up until ID management. So ID management, we don't want to, it's, it's your customers, I'm sorry, it's your employees or customers that you want to have on the tenant. You rent it from us. So you manage IDs, we'll give you all the tools.

We'll have multifactor authentication, whatever you need. They're all there. But you need to configure this customer. You would need to make sure they are the right security groups. The right, I mean, you need to decide, do you want multi fact authentication? Do you want, uh, um, do you want ransomware scanning?

Do you want fishing scanning? Do you want to endpoint protection? Do you want that? I mean, services are there, but you need to configure and risk assessment. We provide you the tools, all the basics. We'll make sure the data center runs we'll, make sure the hardware runs on the services run are always patched, updated, secure.

Your network is secure. We will take care of all of that, but you can never outsource the last bit. So our biggest, if, if I were to choose just one thing, it's the combination. Still manage to get two things. The combination of perception. So is this the problem some people think it is, is the NSA actually having access to my data if I'm in a us?

They don't, we have all the reports, we have all the external legal lawyers saying that's not ones being used for. We now have the executive order comings of the and all that. But there's still a perception and it's partly media created. We all seen the snow and papers, we all seen the movies, we all see spy novels and all that.

And, and I get it. But for commercial services I would definitely be totally okay and saying, look, it's not being used. And I would again say it's even more secure in the hands of a provider like Microsoft, cuz again, the intelligence services, they don't want to go through us. They know how hard it is.

They know they're gonna be met by 140 lawyers who are gonna challenge them every step of the way. They have easy access through old spy methods to going through smaller, um, company. So perception. Okay. And then maturity. Cuz in all honesty, we started with the Chromebook case a ton. Customers simply haven't done their homework.

Mm-hmm. , they don't understand risk. They don't, they've never assessed it. They've never taken a position on, okay. The shared responsibility model means they're actually stuff I need to go assess, So majority, So you who mentions EU data boundary? EU data boundary, uh hmm. How can I say this? Um, I think I'm called the grandfather of EU. I mentioned that this the need eight, nine years ago and it was ignored cuz too expensive. Why should we do that? I've cost my company north of a billion dollars cuz it's quite expensive.

But I staying tall and say, see what I said May last year we announced we are building EU data market. The reason for that is all these data transfers with all the misperceptions and all that stuff. Now we know everything we do is lawful. We know it's well protected. We nobody can point to a single instance of any security instances based on the way we run up.

Not one I can point to. Just in the last year, I can point to 20 security instances where Danish public service have mismanaged and data has been breached to third party. Right? That's day to day has. The Danish uh, government lawyers, li did, they started in December, 2020 of 600 systems in the public sector.

Found out that 24% of those had not been patched in a year and an additional 17%, they didn't know if it was patched . So the number one thing you need to do on every system is keep patching. There are vulnerabilities, there are newer attack services. So 41% of those 600 systems in the government had not been patched or was unknown to be passed in 12 years.

That's a risk. Mm-hmm. . So we know how hard it is for our customers to do all this. We also know that if they're using cloud services, we will take care of that problem. That's our business. And we can't, I mean, our business will die if we don't. Not that errors can't happen in the cloud, but we are part of professional, we've been doing this for many years, so we decided let's, we can't eliminate data transfers.

This, especially security will always happen in the us. That's where the primary resources are. That's where all our, our whole capacities is built. Plus, if we were to have the EU as a black spot, meaning we know everything about what goes on in our network and our customers outside EU, it's to nobody's benefit.

If we did a similar setup in the EU, only for the EU, we would ignore the fact that cyber criminals, nation state attack us the internet. They don't care about EU boundaries. They don't care if you sit in Hamburg, in Sur or in Beijing. You will be attacked. So we. And the, luckily the politicians and everybody else agrees with us.

Of course, security segment needs to be global. We can't split things because lawyers look at something, but we still decided, okay, let's minimize. We can't eliminate, but let's minimize data transfer scenarios. So, EU data boundary, uh, we are gonna be done with the first bit by January 1st. We're gonna announce on November 30th, we're gonna announce exactly what we implement.

Okay? But by January 1st, 23, we will have 24 7, 365 EU/EEA-based operations and support, also support

Hac: For every services?

Ole: And that's the second part. All services.

Ole: As it is not currently.

Ole: Well, so we're looking for store and process. So today we have this, we don't have support within eu. We do have, but it's 24 7. So it's followed the sun for a subset about a third. All the services that people use. I mean, we have more than 300 services. Some of them are used a lot. It's about 80 to 90 services. That's what we call a core services. Already today, we store and process that in the EU for core services. By January 1st, it will be all services.

Even the services are the anybody uses. Okay. So it's about 300 services that will be available within the EU today. Some of the more obscure services. You need to deploy them in the us, use them in the eu, but it's in, the server is placed in the US by January 1st. Those will be in the US one. Okay.

Ton of extra capacity being built in the, in the eu. But this is totally new. So our support organization is gonna be available 24 7 365 inside the, and that's where the lawyers then ask, well, are there exceptions? Of course there's, there's always exceptions. Mm-hmm. level four support, what we call, okay.

Something is very critical. The only person we have is Anna. She is the one who built the system. The era we've found now so critical. Only Anna can fix it. She sits in, she could sit in Lyngby. We have a ton of developers located, but she could also sit in the us. We have nobody else who can do it. . She needs to remote access any EU tenant to fix it.

It's so rare, but it could happen. Again, customer lockbox is gonna be replaced. So you will be requested. And again, I've had customers for many years running our services, never had a customer lockbox request. Cause we can manage, operate our services and even support our services without having any access to customer data.

But it could happen. So we have to list it as an exception. Mm-hmm. . But that's gonna be announced on, uh, November 30th. More details. This is all I am allowed to tell you right now.

Hac: That's fine. I think there is, you see a link to it in Yeah.

Charity: Um, just before you go these two. So what's your take on this and how is it going to affect.

Ole: It's gonna affect, I expect it's going to affect, uh, in many ways. First and foremost, it will be, Microsoft will probably be some opportunities too as well. Cause we run critical systems for government services and for utilities companies, um, merit team, organizations, all that. So for the first time, Microsoft will probably be subject to this tool.

That's, we, we not subject to this one, but we most likely will be in this tool. We, I actually just met with the authorities yesterday about this. We are ready. Tell us what you need. We'll absolutely make sure that we, we don't foresee any issues with that cuz the security requirements in this tool is, uh, we believe, I wouldn't say basic, they're straight, but we have it all.

There are no new requirements that we know of. That we couldn't live up to. The new thing is the incident management. If there's an incident, you then are now required to report it within a time limit. And if you don't, you will be subject to fines Up to 2% of your global journal GDP bars up to 4%. This is up to 2%.

We don't see any issues with this. We we're definitely capable. We already do incident management, uh, in the best possible way. If we are public critical infrastructure, we of course have to be, uh, involved in the planning of critical infrastructure security in the in demand. We are not today, we are, when there are incidents like the covid, we were asked to participate, but now we'll be on an ongoing data basis, especially cause we have these three data data centers coming up, um, in the next couple years.

But, uh, this NIS2 was definitely apo. The only issues we see with this two is the Danish implementation, and we are very open about that. Uh, have you heard about the Sektor Ansvars Princip? Like it's, um, it was implemented and then does eight, six or eight, I think it's eight under the NIS1 directive.

They divide everything into, so there's energy, water, sea harvest, and all that. Transportation, finance, and that's it. Each of these sectors or industries have what they call a decentralized intelligence system, meaning it's a, so they monitor everything that goes on within water, water companies or in sea transportation, finance, and they have to report back to the Center for Cyber Security, who is then responsible for, for the national.

Now under NIS2, the amount of companies that are gonna be covered by these two are required to participate is gonna increase quite a bit. Um, we believe the Sektor Ansvars Princip where you report to a digs for that particular industry is too limited. We would want it to be a central place cuz if an incident happens in transportation, who says it's only transportation that should be aware of that, it could easily spill into finance or vice versa.

So we need somebody central, that's our belief. One place to hand over the incident information and so they can learn from each other. Um, We're not alone on this. A ton of, uh, I mean dangerous industry association, the, uh, dangerous Business Associa Association. A ton of organizations are all saying the same thing.

We know why we did the eight sectors of the eight industries. We need something central, cuz that's the final critique. And this talks good in that respect as well, cuz it's very clear from NIS2 that we need to, uh, then, uh, um, analyze what's going on and let that knowledge, the best practice, um, filter in to all the organizations, which doesn't happen today.

You give in information about how you're being attacked, how you've been bridged, and that's it. No learnings, no key best practices, and then fills it back into the rest of the industry. And we believe that's the only, only thing really missing. Some authority could be the business authority, could be the center for cybersecurity, could be somebody else, but somebody needs to come back to the market saying, okay, we've seen these five instances.

The key issue are these three things you need to go fix. And in all honesty, we know what they are cuz we see it every day. It's not just in critical infrastructure, it's in everybody. Um, it's patching, lack of patching, it's lack of control, of privilege, access being administrators, and it's a matter of not having multifactor authentication. Horrible. These are so low. Let me, yeah. Three low level things. Sorry. Yes. Um,

Farhan: We are almost at the end, so we just have five more minutes. So we would like to have this opportunity to have your insights on like how with students, uh, should look into this career goal. As cloud practitioners or cloud engineers, and what is, what is mostly suited for us, whether it's Izzy 500 or C 200,

Hac: And where can we file our job, uh,

Ole: On our job site, it's the only way into Microsoft. It's on our job site. Um, let's say that first, that's easy on Microsoft job or careers, Microsoft DK slash careers or jobs. Um, we list all the available positions. And when you apply to Microsoft, you have to have a specific position in mind. Doesn't mean it has to be that, but that's your way in. Then you'll be assessed.

You'll probably have a test and you'll have a conversation. And if the, the screening person believes, well, actually I think you might better be suited over here. They'll make that happen. We have a ton of applicants. Of course we do. We also have a ton of open positions. So there's uh, especially if you are free to move, It doesn't have to be Copenhagen, but that's the only office we have.

So that's your way in. Um, then, uh, what you're talking about, what certifications, what courses, why don't I send you a list?

Farhan: Like there are a lot.

Ole: I know there are a lot. Um, it, it really depends on, uh, on what you feel for, if you want to be, if it's based on security or if it's based on administering or if it's based on building. Um, there are different paths. I've actually just sent a list to one of our partners who asked the same thing, so I'll resent that and then sent it to you. Uh, but I would say the, the, the one thing missing out there in our community, I mean we have 3,800 partners in demo, um, is partners. Who understand the architecture of cloud.

What are the services? How can you combine them into, uh, with the flavor of saying, well, I know the technology, but this is how you do a risk assessment. This is how you do it. Security and privacy review of the architecture. These are the tenants you need to be able to tick before we can actually use the cloud service.

We don't have those partners. The most, most of our partners are focused on either or. Okay. Um, most are so skilled in building architectures. They can use all the services, but they are not concerned about security or privacy at all. Some are only focused on security and they're great at that. They don't really understand all the pieces of the client.

Um, and very few, and these are primarily the bigger ones of PWC, kbmg, Accenture, David team implement those advisories. Uh, they know everything about compliance, but they have no idea. About what cloud is. Okay? Some of them had great no knowledge about security. Pwc instance, KPMG know ton about security.

Conceptually implementing it, knowing that technology and all the parts hardly in, we see some of these partners like D team, they were huge in public sector 10 years ago and they, they could do everything except technology. They recently just purchased somebody called Cloud who only knows technology. So we see some of these advices having figured out we need both flavors and building that capacity.

Uh, so you have to decide for yourself if you're technical architect, if you are a security architect, or if you are primarily into the one who knows technology, but knows what compliance is all about. How do I do risk of. Assessments, how do I do transfer impact assessments? How do I do uh, data protection, uh, impact assessments, all the GDPR terms. If you know at least two of these, you're in good shape.

Hac: Thank you.

Charity: Sometimes, um, work with students on projects?

Ole: We, uh, I did when I was uh, head of development, we, uh, we brought in students to work. Um, I don't now, I decided when I took on this position, I decided no budget, no people, no, uh, um, no, um, product ownership or custom ownership. The only customer I own is the military intelligence and the police intelligence services. Those are the only ones I own. Cuz I don't sell, I only advise.

And, uh, so I don't, but we do. Absolutely, we do. Um, Our development and our consulting, uh, have some, I don't know how many, but they do have student workers, uh, working on projects as well.

We have a trainee program that's also on the career site. Um, can't remember. It's just been renamed. They rename it. I mean, one thing, Microsoft does a lot rebranding, and renaming, it's horrible. Um, it's a mismatch, but, um, it's on the career side. It's a trainee program aimed at gaining full-time employment.

Afterwards, uh, when I was head of development, I have had four, maybe four, going through the trainee program, ending up in consultancy or in development.

Appendix D

Prepared questions for Allan Frank

Introduction and the Danish DPA's role:

- What is your background and position here in the DPA?
- What is DPA's area of focus - Is that the GDPR and/or national laws?
- When does the national DPA investigate a case?
  - In case of a complaint?
  - In case of suspicion of GDPR breach?
- Who makes the decisions? - And is there any kind of court request involved?
- How much does the Danish DPA compare to other EU DPAs? - Is it more strict? Considering the French DPA's recent decision to ban Workspace.

Foreign legislation

- What is the DPA / your view on the surveillance laws in the US?
- Which surveillance law do you think is more concerning and why?
  - CLOUD Act?
  - FISA 702?
- We have talked with Ole Kjeldsen the CISO of Microsoft DK, we discussed the impact of FISA 702 on their company. He says that Microsoft is able to fight the requests of the US agencies.
- What are your views on the upcoming Privacy Shield 2.0, and its ability to help conform to GDPR?

Outsourcing/leasing datacenters *Given the newly canceled custom contract with Germany, which granted the German people control over Microsoft German citizen data.*

- What is DPA's view on how much control countries should have over their own data?
- Microsoft has been renting Microsoft facilities to local trustees. - Do you think this is a good methodology?

Chromebook-case *Set the scene*

- Tell us about the dialogue between you and the municipality. (KL, other Municipalities)
  - What did it lead to?

  - What kind of documentation did you ask for?
  - Was the requested documentation different between each verdict?

- Given that half of the primary schools in Denmark are using Chromebook - Do the other municipalities in Denmark have to self-adjust according to DPA's decision on Elsinore?
  - Or do you investigate and decide for every case?
- Who are the victims? Which children does this Chromebook case concern? Can you give an age range?
- Buying and using these Chromebooks in the schools, was there any form of consent given by anybody, student, parent, school, etc., considering the student data being processed or possibly transferred to the US or other IT-support countries?
- How did you assess the case? Was it based on your own assessment or on Elsinore's one?
- Our goal is to understand and analyze the Chromebook case in order to propose relevant solutions. In that light, we have highlighted 4 problems within this case. We would like your opinion on those *(list the four problems)*.

Alternative solutions

- Do you see Google self-adjusting in order to comply with the GDPR in the future? Or more precisely for the use of Google products in elementary schools.
- What is your personal view on the way forward? A European / sovereign Cloud? Data Confinement?
- Is there any product which complies with GDPR in Denmark/EU which can replace Google Workspace for students? Are there credible open source alternatives? If yes, do you think they can live up to the tech giants' service quality?

Appendix E

Allan Frank interview

Hac: So thank you for meeting with us. Uh, we have, uh, different topics for, uh, for questions. We have one, which is more an intro. Then we'll go into some foreign, uh, legislation. Yeah. And then something, uh, about Microsoft. And then we will, um, we will, uh, end with the case of Chromebook.

Allan: Yeah, of course. And, uh, I you just, you just hit it. Go away. Yes. Give it, give it your best shot.

Hac: So first, uh, what is your background and position, uh, here at DPA?

Allan: Yeah, my background originally, I'm a master of science in physics, atomic physics and mathematics originally. Uh, but, uh, then I've reverted to being a, a lawyer, so I have a degree in n law as well. Uh, and that, that combination has kept me in breadth, so to speak, for [00:01:00] a very, very long time. So I, I've been working in the, the crosshair between law and legislation and, uh, technical issues around it and it-usage the, the last 30 years, something like that, in different parts of the Danish governmental system primarily, but also in, in, uh, private companies as well. Mm-hmm. And, In the DPA I hold the position as a ICT security specialist and lawyer.

Hac: Okay, let's go to next for the next question. So, um, the DPA, which is the Datatilsynet, you know Yeah. But we call it the DPA here.

Allan: Yeah. Data protection Agency.

Hac: Yes, exactly. Yeah. Uh, so what are the focus, what are the area of focus of the DPA? Uh, is that the mostly the GDPR or also the, the national laws or some of the laws of the national laws.

Allan: Primarily the DPA is, uh, yeah. We, we are in control of the citizens data protection. So, so, so it's more or less GDPR wise, but it could be national law as well as TV-overvågningsloven (national TV-surveilancelaw) or similar laws, which holds issues around the protection of, of human rights within personal information. So, so, so everything that revolves around personal information is our subject, so to speak. And we are by law, the, the, the authority that are the competent authority to, to, to, to handle all cases around personal information.

Hac: Okay. Uh, so when the national DPA, uh, chooses to investigate a case, does that typically derive from a complaint or is the breach of loss of your observation?[00:03:00] When does that happen?

Allan: Yeah, it, it's a, it's a very broad, uh, topic because every week we get around 350, around, so, uh, breaches in the personal data, uh, protection in general so, so we have 350 cases where the companies themselves, the data controllers themselves to us. Uh, while the GDPR article 34 has to, to, uh, 33 has to, to, to give us a notice when they have a breach. And, and we got around 350 of those every week. We have around 3000 complaints a year. So that's probably 30, 30 or something a week, something like that. And, and we have a lot of own cases where we either hear it in the background or in the [00:04:00] press or something like that, or, uh, via a whistleblower, uh, advertisement, something like that, that we, that there is a problem. And then we start a case of our own device. So we have around those 400 cases a week, and from them, we choose the ones where the rights of the human beings are, or the individuals, which data being processed are at the highest risk. So, so that's the way we work. So from those, let's say 400 cases, just to give a number, we, we derive that to, to a smaller number where we actually go in depth with the investigation.

Hac: Mm-hmm. Okay. So you, you say there are cases where you actually don't, eh, look into,

Allan: So probably, probably most of the cases that we, we get in, we don't look, uh, hard into because either, [00:05:00] uh, infringement is so small, uh, that the investigation would take so much resources from us that we wouldn't be able to solve some of the, the higher topics. Or maybe we got 12 breaches, which are the same case. So to speak. So by handling that one case, we handle 12 other cases. So that's the way we look at it. But, but in that way, we try to cover every aspect where there is a high risk or, or a higher risk of for data subjects. So, if that should be the case, then we will investigate. So it's only minor infringement because for instance, my email address at Datatilsynet(DPA) is a personal information. But if that got lost, some somehow was sent to a person, which should [00:06:00] not have my email address at Datatilsynet, it's a minor infringement because they could look it up if they wanted to at Datatilsynet homepage. So, so, so there is a lot of those as well.

Hac: It's funny you should say this, that, uh, somebody has to make the decisions of. Uh, how to pursue these cases. So who, uh, makes these decisions and when those decisions are made, in the process, does, uh, is there any kind of court, uh, involved in this when you are pursuing?

Allan: Yeah, it is so that, that we make a decision in every case, every, complaint is handled. Even though your case is not investigated in itself, you get a decision. And that decision, the data subject then can take to a, to a Danish court because it is so that the Danish data protection authority, uh, will be [00:07:00] competent to handle every case around this and do that as a first case level, so to speak. So no courts are involved. It's the DPA themselves that handle that. And, and, and, and if their decision should be questioned or you want to complain about that, then you go to the court. Okay, so the court is a secondary measure. And, and so it is under the Danish, uh, Grundlov(Danish Constitution), under that article 63 that you can always go to the Danish court to get a, a verdict.

Hac: Okay. And in, in, uh, in terms of who, uh, are able to make decisions, whether something should be, uh, labeled..

Allan: Datasilsynet themselves are, are entitled to make those decisions because the GDPR itself stipulates that that's one of the jobs that, uh, DPA has to do.

Hac: We were thinking within Datatilsynet sales

Allan: Then we have a, a [00:08:00] decentral way of, of working where the case handlers have, uh, some responsibilities and can decide in some cases and, and there are supervision up until we have a director in, in the, the last end taking the, the formal decision if, if it should, if it should be but normally she is not involved in the day-to-day running of, of one case or another. But, but that's handled by, yeah, the case worker themselves and their superior officers, something like that.

Hac: Mm-hmm. Okay. So generally, um, uh, how do you think that the Danish DPA compares to, um, international or European, other DPAs? Um, do you think it's, do you think it's more strict? Let me give an example, come some contexts. Uh, the French DPA recently banned, uh, Microsoft 365 as well [00:09:00] as, uh, Google Workspace in there.

Allan: I think actually it was not the CNLIL (Commission nationale de l'informatique et des libertés),the French DPA that did that. It was their Ministry of Internal Affairs or something like that. Okay. That made a decision, uh, that they would not use, uh, Microsoft 365. And it's right that both the CNIL and now the German DPA or German DPAs, because there are more than one down there, uh, they have, they have, uh, stipulated that, uh, under certain circumstances that kind of software cannot be used. And that is totally in agreement with the Danish Cloud Administration. What we have said in our, we have made a guideline around cloud, cloud computing, for instance. They're just quoting the same things that we already said. But you have to remember the, the GDPR itself, and that's why I know it's not CNIL because we don't, [00:10:00] we don't ban products. We ban processing, uh, the way of processing things. Mm-hmm, so we don't ban Microsoft, we don't ban Google. We, we ban the way that the controllers are doing that processing, because that's our job. Mm. Uh, everybody, every, every firm should be able to come with their flavor of how they want to do things and, and we are just looking into how it's done at the controller level.

Hac: Yeah, so you say CNIL or something is that the French?

Allan: Yeah, the French that the French DPA. Okay. And, and, and, and I didn't answer your question. I think that the Danish DPA, uh, is very in, in the, in the European family. We are hold very high in the esteem because we are very free. We are very good to express ourselves. We have a high degree of digitalization because yeah, Denmark has been on the forefront of this for many, many years. And some of the problems that we are [00:11:00] having here in Denmark, all the things that we are occurring, then they will occur in France in three or five years and, and things like that. So we are very much on the forefront on this with some other European countries as it could be Holland, for instance. Mm-hmm. , which are more or less on the same page as we are in, in digitalization. So, so, so I, I think that we have a very high esteem, making very good law decisions and having, uh, a very good way of communicating our decisions to the public. And we are the DPA in Europe that has most, the most published decisions by, by far. So, so they are, they are quite happy with us because normally when they get a case, they can take a Danish decision and then they can transcript, uh, what we did. And, and, and that's, That's very good. [00:12:00] So, so that we are holding very high esteem and toughness wise, if you are assessing toughness, it is more or less to, it's important to say that we do the, the things that are necessary to get the Danish controllers, the ones that we are responsible for, to, to, to adhere to the rules, to, to follow the rules. And in France, uh, people, I don't know, it's a cultural thing. They do not always hear what, uh, the, the authorities are telling them. So they have to be a lot stricter. They have to use a, uh, a bigger stick to make people do what they want. And, and that's one of the things you have to look into when you are, if you're not just looking on, on the measurement of fines and things like that and, and we have been very successful in getting our controllers to do what we are telling them without giving them a very high [00:13:00] fine. For instance, an example that can show that the Danish controllers are much more compatible with the GDPR is that we, we get around 350 of those breaches, data breaches to us every week, and in France, they have not had more than 700 over the four years that the GDPR has been running. So a, a French person would never, uh, incriminate themselves to the, to a, a governmental body. But in, but in, but in Denmark, we, we have a long-standing tradition also in taxes and things like that to make a self-assessment. So, so we are much more, we believe normally that our society, our state, don't want to hurt us or do anything illegal against us or. And the French has a different, uh, tradition in that aspect. So, so you have to see the fines and the way of acting in that context as [00:14:00] well. Mm-hmm.

Hac: He's, he's French(pointing at co-interviewer, David).

Allan: He's French, but he's nodding. I can see that.

Hac: So, so you, you might say that, uh, Denmark has in a sense, a higher standard.

Allan: We, we, we have now we have a different standard. I would rather say, because the French standard is good in France and, and matches the, the, the, yeah. The way the, the French are thinking, so to speak. And, and we have to have every, even though the GDPR is supposed to be the same rules in every country, we have to have different flavor levels that does it proportionally right in our country and in Denmark, we don't, we don't have the need for as big a stick as they have in France. So, so, so you have to, you have to take that into account as well. And, and I think that the legal work done in Denmark is in a very high status, also in the EDPB(European Data Protection Board), and we have a lot of, what do you call it? Mm-hmm. in English, you call it cloud. We have a lot of, of [00:15:00] agreeability amongst our colleagues because we always Yeah. Go very deep in the discussions.

Hac: Okay. The next, uh, topic is, uh, foreign legislation. Yeah. So, uh, what are the DPA view, or your view for that matter on, uh, the general, uh, laws, surveillance laws of the US?

Allan: Yeah. I, I think we, we have to say in general that a lot of the laws in the US are exactly the same as the one that we, we have in Europe. Uh, and the problem being, uh, not spec specifically us, but every third country not being the EU. There is, uh, a set of rules within the GDPR that says that if you are going to, uh, export data outside the EU, you have to adhere to some special rules. And those special rules, uh, [00:16:00] demands that the surveillance is done in a special way. It should be proportional. You should know what, what is you have to adhere to in the law. It should be able to read and some page, ah, okay, if I do this and this and that, the, the, the community or the, the state is coming after me. So, so there is a, and I, and I should also have the right to go before a judge and get my case proven or tested and things like that. And all those issues, uh, more or less is the problem with American, Chinese, Russian, and, and a lot of other state laws and, and they are all in themselves, uh, problems in this matter because they normally, normally secret services, they like to, to operate in secret because that's their nature, so to speak. And, and one, have to admit that the [00:17:00] rules in Chapter 5 in GDPR, the, the rules about foreign transfers, uh, is a little bit of a double standard because within the GDPR, uh, the community, the, the way that law, uh, the secret law enforcement is done is exempt from the GDPR. So in Denmark, Politiets Efterretningstjeneste(PET). Forsvarets Efterretningstjeneste(FE), they are, they are not, they don't do not have to abide by the GDPR. And now we are telling the US to adhere by a standard that even our own secret services, Shouldn't adhere to, uh, and, and, and, and that therefore there is that difference. And, and we have to look into this in, in that context. But here in Europe we should be protected by the EU charter and things like that. And that, that we cannot invoke in the US or China anywhere else. And that's [00:18:00] probably the biggest difference because law wise, they are more or less the same. We have more or less the same types of rules. The US, China, and the big countries normally tend to have a little bit stricter rules for foreigners. While in Denmark we have the same rules adhering to everybody. Mm-hmm. . So, so, so that's probably one of the flavor issues that, that there will be. And. Big countries, like especially us, which is a, which which is a problem, don't allow foreign citizens to sue the American state unless the Americans, you were in the US when you were issued with a subpoena or things like that, then you of course can sue them. But if you, if you're staying here in Europe and, and they, they want to do something with your data or your information, uh, you can't, you can't object to that. You have no, no [00:19:00] way of objecting.

Hac: You have to have a representative in the United States.

Allan: Yeah. Either, either that, and they can only do it by proxy. They cannot, uh, exercise the full set of rights that the GDPR gives to the, the individual. And, and that is in basically, or in, in, in very broad terms, the, the problem about foreign legislation. , uh, in transfer situations.

Hac: So you mentioned the PET or the military intelligence, even with those in mind, don't you think that the American surveillance has been, and as well as, uh, the current laws, don't you think it's more, uh, in a, in a much more, uh, severe sense, uh, comparing to considering their technological kind of capabilities? For example, for example, uh, what FISA 702 702 with the NSA were allowed to do, what they did do?

Allan: Uh, I, I think, [00:20:00] I think that you will be very naive to think that the Danish government is not doing the same. So, so, so, so the, the, the problem is the investigation and, and the keen eye that Snowden and others have, have turned to, to American legislation is, the foreign legislation, uh, the Snowden things and things like that, they have, they have shown us that the US has this problem. But if somebody like Snowden within Denmark, we had a whistleblower like that, we would probably see some of the same problems with the Danish legislation and the way that we are doing it in Denmark. And we have to acknowledge that Denmark is, has for a long time, been a part of an international network collecting [00:21:00] information for, for these foreign services. So, so we are not too good either. Okay. So, so, so, so I think it would be naive to say that the US should be worse. It's, it's, I think it's like making a degree of something bad - it's bad or bad, something like that. And I think that every kind of surveillance. Which are done in a bulk kind of fashion and in a way that everybody is getting their, their data censored in some way should be banned also, uh, because that's a, a standard that we don't want. And the GDPR tends to work with that subject and try to, to tell also the, the, the national European National Services of secrecy of the one of one, kind of the other, that they should not do it in a bulk way of fashion. And, and there are rules within the charter that, that, that does that, that says that, [00:22:00] okay, they should not do that for their own citizens because this is the schism. If foreign citizens, we can do everything upon our own citizens. We have to be careful about. And, and that's probably the same problem in the us. But of course the concentration of information is much bigger in the US because many of the big vendors and, and a lot of data is getting concentrated over there. So the issue is bigger of course, but the foundational problems are the same. And the legal, legal access is more or less the same. So, so, so yeah, you are right, because if they are bigger, they have the capabilities. But in Denmark, they could do the same. In Germany, they could, in Germany, they could not do the same because they have a legislation that is much harder on the, the, yeah National security [00:23:00] agencies, because they have a history of both in East Germany and, and yeah, if you go to the, before the second World War, um, with the nazists, that was a problem. So, so they have a very strict set of rules adhering to the Secret police, Inger and in Germany.

Hac: So, uh, more about that. Yeah. When it comes to these laws. Yeah. Uh, which of these laws you mentioned FISA 702 and you mentioned Cloud Act, those are exactly the ones we were, um, thinking about specifically. So why so specifically those but feel freely to mention others if, if, if necessary, which one, uh, are most concerning and why?

Allan: Um, the problem is that the concern about FISA 702 is, is occurring when you have information at an American electronic service provider and custody of one of those. Then FISA 702 applies [00:24:00] under some circumstances, and those circumstances give a wide range of opportunities for the American state to address and get that kind of information if they can identify it. and, and to us the problem with FISA 702 primarily is that a lot of the, you can, you, you can't say if you read the text in FISA 702, okay, this looks okay, you have a good description. But then again, there is a mention of, of the way they should get information and all that is blacked out in the, the underlying material. So it's not, it, let's say there was 25 pages describing how to get information and 17 of them. Well just, uh, black spots where it was painted over because it was, uh, it was, uh, under, under secrecy. So, so you can't say what they're do, you can't see what they're doing. It's not [00:25:00] clear to me as a subject what they're doing. And that's a very, the, it's, it's called the rule of law. And, and in Denmark and other European countries, you have to know which rules you are under. It should be clear to you what you have to adhere to, but that, that you don't know here. So that's a big problem with the FISA 702, the Cloud Act is a little different. The problem there is the extraterritorial issue because they can use the Cloud Act to invoke on even in, uh, companies that are situated in Europe and under European law and should operate under European law to divulge information, uh, under American law, which could, or, s0ometimes could, are compatible with European law, but sometimes are incompatible with European law. And, and it is so that for a data processor, one processing data on behalf of the [00:26:00] controller, uh, it could only happen, you can only give away data if your controller tells you. So it is stipulated within European law or within national EU law. And so, so, so if American law should not be in compliance with EU law or national law, Danish law, for instance, then they have a problem because then we have a situation where they can't get the data, but there are rules in the US, the US cloud Cloud Act says that they can do it and force their arm on the, on the company in Europe and get the information anyway. And that's a problem because that will happen in the dark, so to speak, for the data controller. and, and that's the, the different problem. So it's like, uh, comparing a plate to apples to oranges or something like that. It is, it's, it both are bad, so to speak.

Hac: We have had the understanding that the FISA 702 was actually [00:27:00] this no-border, uh, US based countries, uh, US based companies, sorry. Mm-hmm. , uh, which were, um, getting requests from the agencies in the US mm-hmm. about data. Yeah. But you say it's, this is about Cloud Act actually.

Allan: Yeah, cloud Act is the, FISA 702 is the one they are using within the US if, if it's, uh, American electronic service provider and, and falls within the scope of the FISA 702. And, and there is some elements of export territorial issues, but only towards American companies because the other one is a European company. Established under EU law, but owned their, their shares are owned by the American Mother Company. And in those cases it would more, most, uh, certain be the Cloud Act that they would be using to access data there.

Hac: Okay. Uh, it was nice to clear that [00:28:00] out. We actually talked with Ole Kjeldsen. Yeah, yeah, yeah. We had an interview with him. Yes. Uh, and we actually discussed this, uh, this impact of FISA 702 or maybe even Cloud Act that he did not mention that,

Allan: Yeah. But it's okay.

Hac: He actually said that, uh, they were able to fight these, um, requests that American agencies

Allan: Right. To a certain degree anyway. .

Hac: Yeah. To a certain degree. He excluded criminality, of course, terrorism and so on. But he mentioned there are periods actually where they take the US agencies in court. And actually fight them.

Allan: um, they, they, they, they do it by, they are being my proxy. It was my data being possessed. They are being my proxy. Mm-hmm. Yeah. And, and they, uh, of course they do. And, and they should do so because they have a contractual obligation to do so because they say so in their, in the agreement with the data controllers that they will do it. So [00:29:00] that's a contractual thing that they have to do it. And, but they, they can't guarantee that there will not be cases where even though they fight it, that there will be a case where they would be obliged under

American law to divulge the data to the NSA or whatever, uh, but not falling into the three categories that I mentioned before. So, so, and that can be any, anywhere between zero to three cases, uh, year or zero to 10 cases a year, something like that. But, but it will happen. And the problem in the GDPR being that the chapter five is a legality issue. You have, you have any, it states that any, any transfer of information should adhere to all the rules in chapter five and should adhere to the whole of the GDPR. [00:30:00] And, and the problem is that any is not any minus six. It is everybody. So that's the general problem. Because you can't say that you, you have a, it's the same as Article 6, which is the legal right to, to do something. You can't say that. Okay. 99.9% of the cases I have a legal basis for processing data. Uh, that doesn't make the one point, uh, 0.01% legal. So, so it's that way you have to look at it.

Hac: So we were specifically talking about with Ole about their commercial line of products. Yeah. So not so much about the, the private section. We were looking at,

Allan: The public sector?

Hac: not only that, but also bigger companies in the market, which you are using, utilizing their product, and he was saying he was very proud of this, actually this case. And in zero cases this year, only three this year, and we fought them hundred cases, [00:31:00] so on. So before we actually talked with him, we got the, at, uh, the um, uh, uh, the picture of it's non-fightable. Hmm. Uh, so Microsoft like opened this window for us.

Allan: And I think that every, every of the great, great, uh, cloud providers, uh, they, they do this on a regular basis because that's the way they do business in Europe. They can only do business in Europe if they can convince that customer that that put up a, a real fight. So I, I think that all of them are, are trying, and it, it's probably more, uh, the likes of Google and, and Microsoft that has this problem. Uh, Amazon web services probably more deliver, uh, yeah, the capability is within the, the server range and things like that. And not so much an information provider like the others. Mm-hmm. , because it's, it. [00:32:00] they have a, a small sliver of services that falls within that category, but normally it's server capacity and things like that you buy from Amazon, normally.

Hac: But, uh, if they own the servers, uh, Amazon they might still be a abide to the agencies in the US.

Allan: Yeah. And, and, and, and I think they, they will, they will put up the same fight. I think they do more or less the same, all of them. And Ole can be proud because as a Microsoft are doing a good job and Google are doing, doing a good job. And, and we are not questioning that. No, but we are only saying that yeah, you, it's okay that you're, going, going on and doing a good job, but the good job shouldn't be necessary because, because it should be ruled out that the Americans could address this at all.

Hac: We will actually come into Microsoft. But before that, we have one last, uh, legislation, Um, [00:33:00] topic question, which is, uh, this new Privacy Shield 2.0. This upgraded version, do you, tell me about the, what do you think about these abilities to help, uh, people conform to GDPR?

Allan: Yeah, of course. As the, the problem right now is that when the Schrems2 verdict came out, the rock was pulled under, uh, a lot of people doing a legal thing because the EU commission has, has made a decision. And, and, and that decision was that US was a, a safe place to put your data and that was the EU commission. And, and when the EU Commission has done that, every controller can can go on as if it was the case. They don't have to put up any questions or ask any questions about that, they can, they can just go on with their business and have been doing so legally. And the rock was pulled out under that [00:34:00] with the Schrems2 verdict and now they, they all the problems so to speak, was spilled open. And, and, and, and that could be the same problem when the Privacy Shield 2.0 gets into effect. Because if the EU commission, once again makes the wrong decision as if the courts overturn the, the EU, uh, commission's decision of making the US once again a safe place to put data then we have the same problem again in two years or something like that after Schrems3. So, so I think I the commission would be very wise to listen to the, the DPAs and others that are concerned about the way things are, are being done under, uh, yeah, the data protection framework that is stipulated right now.

Hac: You mentioned Schrems3.

Allan: Yes.

Hac: Which is a [00:35:00] non-existing thing.

Allan: Yes.

Hac: Tell me why it could, would or should exist.

Allan: Yeah. I'm not, uh, I'm not my brother's keeåer as they say, and the Bible, so I don't know what Maximilian Schrems would do when, if it, there is a EU commission decision to make a Privacy Shield 2.0. But, uh, he has openly said that he would fight that if it was based on the things that we know right now, and that I'm just telling you that, that that's his own words in this. So, So that will probably be, uh, Schrems3 case then. But then again, we have to see if the EU court of of justice will come to another decision than they did under the Schrems1 and Schrems2 ruling,

Hac: We have heard from Maximilian Schrems, not directly, but he also says almost the same thing. He says that, [00:36:00] um, that the, the fundamental problem, uh, are not solved, is not solved by privacy shield. So he actually kind of also expects there is this Schrems3, because he seems to say that, uh, either the EU commission or the United States in, you know, when only considering that relationship is that one has to bend; One has to give in.

Allan: Yeah. Yeah.

Hac: And none of them are. Do you think that's true?

Allan: Yeah. That, that is probably true because. The, it, it goes back to one of the things that we talked about earlier, that we are trying to protect our own citizens against a foreign government. And, and that works the other way around as well. The US have to protect their own citizens or their companies against us. So, so that is, uh, that's like, that's an arm twisting battle, that one. And, and I don't think that there is one golden [00:37:00] solution on, on this other than both parties have to give in some way to, to make a fundamental sound, uh, decision. And I don't know what the right answer to that is, because that's a political answer.

Hac: Okay, now we will talk a bit about, uh, data. Yeah. Um, in the sense of Microsoft.

Allan: Yeah.

Hac: Uh, so you know that the Microsoft had made some trustee models deals, uh, with some countries specifically, uh, Germany. Yeah. Um, so they gave them in control of their, their Microsoft citizens data. Uh, how much, uh, does, what is the view of DPAs or yours, uh, view on how much one should have control over their own data?

Allan: What, what we tend to see under the GDPR, or should see under [00:38:00] the GDPR is that it is called the data controller for a reason. It's because the data, the data controller should be in control of all the processing being done with the citizens data or the, the, the data subjects data, if you want to call them that instead. And being in control is knowing what you're doing with the data at every stage of the processing being done. And that has been the problem with some of the big vendors, not Microsoft as such, but other vendors as well. We are just bought in to a service and, and, and says, okay, this solves my business problem. But we have not, we have not walked that step further and, and been in control of what is happening in that black box over there. A lot of processing is going on in there, but I'm only interested in the results as, as a controller. But the GDPR tells you that you have to be in control with all the [00:39:00] processing being done, even though you only care for the results, so to speak. So, so, so that's the, that's the, the model that we are trying to, to persuade people to look at it at instead, because, by being in control, knowing what you are doing, knowing what your processes are doing with your data, and you will be able to make sounder and the, the right decision GDPR wise. So, so we are just trying to teach the data controllers to be in control of the data processing. So, so, so, so that's the way you have to, to look at it instead, because we have just, yesteryear or the year before that we just bought the service because it solved our business problem. We didn't look at what the service did with the data.

Hac: Mm-hmm, so you might say they have been renting Microsoft facilities out too. Mm-hmm. , uh, do you think it's a good methodology when you say, [00:40:00] uh, the data controller has to be in control in some way of the processing and so on?

Allan: but, uh, but the, I, I, I, neither the GDPR nor the Danish Data Protection Agency. Will tell you that one solution of the, the, it could lay as well in the US for all the GDPR cares because it's one of the, the, the prerequisites of the GDPR is that data is transferrable, will live in a global world where data should and could and we be processed other places than in our own seller. So it's a, a fallacy to think that we only can do it within Europe or within. And, and the GDPR itself stipulates that. It only stipulates that you have to, you have to be in control. And the further you put away your processing from yourself as a controller, the more control you have to, to act, [00:41:00] uh, to have, you have to have a, a large binoculars to look at the, the controllers way out there. And, and, and that's the, the only problem in. Yeah. In, in selling out on your, your data controlling in that sense, it's that you have to make the control in another fashion, you have, you have to have a longer arm or longer cleaner eyes to see what they are doing out there. So the further away from you, you dilute your processing, the more control you have to more audit, it's the more, uh, other ways of, of looking into what is happening out there you have to have on a distance. And that's, that's the, the problem. We have only been looking at the, the near cost. What does it cost to buy the service, but all this extra, and that might be cheaper in a cloud solution, but all this auditing that is necessary to be [00:42:00] in control, to still be in control and have a contract that you can use as a control, as a control mechanism.

Hac: m-hmm.

Allan: And that is the general problem with the services that we have been buying into over time.

Hac: Okay. Uh, let's move on to the interesting part, uh, the more interesting part for us anyway, uh, which is about the case of the Chromebook. Yeah. Yeah. So, um, just shortly about the whole case. There is this parent who, uh, who complained to the, the DPA and said we didn't give consent. And then he figured, uh, then we found out that they were actually, uh, transferring information, um, uh, unlawfully to the States United.

Allan: Amongst other things, yeah.

Hac: And, uh, so then there has been since the start of 2020, there has been some dialogue between, um, uh, the [00:43:00] DPA and then he Elsinore municipality.

Allan: yeah. 2018, 2019 around there. It started arounds there

Hac: yeah. So in December 2019. But it seems like, uh, he, Elsinore also, uh, submitted a, um, a request so that so start off 2020

Allan: Yeah around there. Yeah.

Hac: Uh, so there has been some dialogues since then.

Allan: Um, tell us there's been 3 verdict as well. 4 verdict now. Uh, the problem being that we had this complaint for, from a parent in Elsinore municipality. And, and when, when we got into to that, the municipality themselves, quite frankly, stipulated that they have not made any risk assessment about this. Uh, in the concrete case where it was the, the use of YouTube accounts and, and the community of the municipality, they, they, they very quickly reverted on that and says, okay, it was a fault [00:44:00] that were access to, to YouTube. So they shut that down. But, in the consultation that we, we thought that, okay, you haven't made the risk assessment, you haven't any, uh, clue of what kind of processing you are doing. Then we thought, okay, we'll make this, uh, case of our own and, and go into the, so we had a very broad investigation on, on the municipality and other, there was around 50 municipalities using this kind of software. So, so, so we looked into the mold, but Elsinore was the one, the furthest ahead. So they were the one spearheading the, uh, yeah, the decisions. And, and the problem was that no risk assessment was done. No. If they had done a risk assessment, they would have, they should have. Found out that there was probably a high risk for the, the data subjects they should have made, [00:45:00] made a DPIA and they haven't. There was a lot of problems about the contractual situation with, with Google in this case because Google in their contract says, yeah, okay. We are using the data, some of the data, not the content data, but some of the meta-data generated, uh, by the children. Uh, it could be search statistics, it could be other things that we use them for different purposes of our own and within Danish law, so that as a controller, you can only give away your data to another controller if you have a legal basis. And the only legal basis that the municipality had was folkeskoleloven(primary school law), was it the Danish school law and maybe some communal laws about how municipality should act in general. and, and none of those places it stipulated that they were allowed to give away the children's information to Google, [00:46:00] even though we are not even talking advertisement or something like that. That would be a big no-no. But, uh, for one example, the way that Google makes their software better, if they use the children's data to that, that's not allowed either. And that's probably the two main problems is, hey, they should have done a risk assessment. They should have done a DPIA and by doing so, they have, they should have seen a lot of other problems and all the problems that comes after that they stem from not doing a risk assessment, not doing a DPIA and not thinking about, oh, in the, in the contract it says that we are giving away data to Google's own purposes. Ah, Then we have to have a legal basis for that. And they haven't assessed that either. And that's the main problem. Then there was this third country transfer thing as well, but that was a minor problem [00:47:00] on top of a lot of other fundamental problems. And we would rather have that they address the fundamental problems because by doing so, they would've solved the, the problem with the third country transfer as well, because that would have been flagged under the DPIA. Once again, we are trying to get our controllers, in this case Elsinore, to see in a broader light, what is the right steps in, in addressing and some kind of of processing. And that's how the way you should read our cloud guidance as well because in that we also try to stipulate how to think which, which steps to go through to make a legal, uh, processing in the end. So, so, so that's more or less the statutes of the Elsinore municipality case. And now it's a case where 50 municipalities in Denmark has [00:48:00] gone together and trying to, to get Google to change their contract under product in certain ways. So it can be used in a lawful manner.

Hac: Which Kommunernes Landsforening helps with.

Allan: Yes.

Hac: So more about this documentation. It seems like in the first verdict there was missing documentation, but the second verdict there was also, um, lack of quality in the, yeah. Eh, so tell us, um, you mentioned also transfer, so they were by the DPA flag, they should do a transfer impact assessment as well. Yeah. So, uh, tell us how the documentation like, uh, the expectation of the documentation and what was missing and what did they need it the second time and, and third time and so on.

Allan: Yeah. And the, the, the, the problem with documentation is that nowhere in the GDPR it says what kind of documentation is needed. So we have to, to address it the other way around, we have to see, okay, what [00:49:00] processing is being done? Which data is being processed, uh, by which means or how is it being processed? And by doing so, we can make a, a link of different processing, uh, scenarios. And, and each of these scenarios in different places have different risk issues. And those is risk issues is what your risk assessment should, uh, list. And, and if one of them is high, you should go on in the way that the, the Article 35 tells you to do it under a DPIA. And, and that's a, just a structured way of mitigating risk and. If you do it in that way, make can describe your processing, describe the data, how it's being processed by whom and by which machine and in which case then you have made the, some of the documentation. And if you're made a DPIA, you will tell the, the data protection agency. [00:50:00] Yeah. Okay. We solved this risk and we mitigated it by adding this measure and that measure and doing that. And then we signed off on this and we did that. And, and that is the documentation. And so the documentation should be self-explanatory under the processing being done and the way the processing is done and by whom and, and, and, and which risks there are in place in every, yeah. Every chain of that long chain there. So that's the way to, to do it. and if we cannot see the full picture, so to speak, that picture that I've just tried to paint to you here verbally, uh, that is, that is the problem because we have to be able to connect all the dots to see that you have not, you are not broken the chain and in some kind of way.

Hac: Can you see the full picture now? Is there any upcoming?

Allan: Unfortunately, [00:51:00] as it is right now, can't divulge, but they are working with a, a model where they are the last word that we had, we were very explicit in what we needed to, to see and just like, I gotta try to tell you here. And, and, and, and they have tried to, to meant their ways and, and come up with some new, but there was some issues which regarded Google's contract and the software as a, the way that it worked itself because there was some problematic ways in that as well. and, and that had to be re-coded and things like that. So it's, uh, quite a complex matter and we haven't reached a final verdict yet. Okay. And, and probably we will have to, to get some more information to do that.

Hac: Uh, so you mentioned there are other municipalities that actually use Chromebooks. Uh, in other words, half of the schools, elementary schools in Denmark [00:52:00] are actually using it

Allan: More or less.

Hac: More or less, yes. So giving that, uh, these other schools also using, um, uh, now that this case is in, in light does these other municipalities have to self-adjust?

Allan: That was one of the benefits of the Elsinore case. It was that we got the eye of all the other schools. All the other municipalities and them are doing it. So, so they have, they now we have instead of just one municipality, 98 parts of Denmark municipalities, we have half of them, which have done it this, the same way. So all of them are doing it like the verdict against Elsinore told it now every 50. And that's the way we like to work in, in the Data Protection Agency. By, by taking one case and, and seeing, okay, it is, it, [00:53:00] it tends to, to to be the similar problem for these 50 municipalities. Then let's get these 50 municipalities under the same kind of, of scrutiny. And we did that and, and now we are handling all 50 cases at once. Okay. Instead of handling one case at the time, one there, one there, one there. Now we have 50. So, so in that way, even though Elsinore was the hardest hit, so to speak. publicly, all 50 of them has been, has been issued with the same verdict as Elsinore. So there is a verdict against every of these 50 municipalities, but in essence it stems from the, all the investigation done in the Elsinore case.

Hac: Mm-hmm. So yeah, you don't investigate every case. They just, they are part of the conversation, but they they're not sending any documentation.

Allan: No, we have requested the same documentation [00:54:00] from them as we have requested for Elsinore, and we are told them, okay, instead of doing it 50 times, one of you doing your own, you're going, you can do it all together. And that's why Kommunernes Landsforening has in intervened in this and, and helping the municipalities as a whole. And, and, and that's the way it should be done. It it if you have the same kind of processing problems. Yeah. It's only, you don't have to reinvent the plate or the fork every time. So try to replicate what others does, has the same problems with doing.

Hac: Uh, let's talk a bit about the, the parents, the, the victims and how they play a role in..

Allan: The victims are the children.

Hac: Exactly.

Allan: And, and I, and I don't like the word "victims" because of course they, they are on the wrong end and, and it is their, uh, rights that have been, uh, miscued or violated, so to speak. But, [00:55:00] but I, I don't, I don't like to see them as victims in, in a classical way. But of course, their rights have been violated.

Hac: Mm-hmm. So, you know, buying these, uh, Chromebooks, uh, in the schools, uh, did anybody at all give any kind of, uh, consent to this? -the children, the parents in the age gaps of who are using them, who are using this as it, if I read, we've read it's from zero, zero class, but also from the second grade. Is this, is that up to the individual in municipality?

Allan: If you, if you read the first word we had against Elsinore municipality, we went quite deep in investigating in what, what kind, uh, municipality decide. And they can decide which make of model that you are going to use, which software you're going to use because it's part of the digital school and you have [00:56:00] to, to, to, to address a digital school. It, it doesn't say in the, in the folkeskolelov, how to make a digital school. So you can use a Apple computer, you can use a Microsoft computer, you can use a Chromebook, you can use any kind of hardware that you like and any kind of software that you like. And, and that's once again where we get to what I told you earlier, we don't ban Microsoft, we don't ban Google. We don't ban a company specifically. We banned the processing being done. And what we look into here was the processing being done by, with this tool, with these tools that they have chosen. It was, in this case, the Chromebook and the ChromeOS and Chrome web browser and yeah, workplace for Education.

Hac: So this was not necessarily only for Elsinore. This is across the whole, uh, whole.

Allan: Yeah. And, and I, I, I'd like to state and have stated publicly, but we probably have some of the same issues. [00:57:00] If your system is based on a Microsoft based platform as well, it could be a 365 or any, any of the other platforms so that there could be similar problems and those municipalities using, using other software and another way of doing it than the 50 ones that are using the Chrome version. Yeah, they should be looking into their own computing, but that has not been the issue of this case. This case was to, to that way of processing things and, and it could be the same or equivalent in, in other cases.

Hac: Okay. So there, there were these, uh, possible, uh, third party, uh, third country IT support scenarios.

Allan: Right.

Hac: That didn't make any difference in, compared to when asking for whether we should do this or should we take this extra step of, uh, uh, involving the parents or, [00:58:00] skipping some of the grades. Cause we have read that it's actually up to the, it's not that the fact that it's up to them, but the fact that, uh, different schools are using, have different policies. So some start at very early age using Chromebooks. Others don't. Uh, also they are different. Um, the packages of, uh, the editions of workspace, they're using different additions. So it seems like it's been up to themselves to actually,

Allan: yeah it has. Every municipality in Denmark can choose from, from themselves. And every school within one municipality have a lot, a wide range of different choices that they can do. It's up to the school themselves, but the municipality is as a whole, they are the ones responsible under the primary school law. So, so, so the problem is that we could have 50 different ways of doing things and, and we had maybe not 50, but 30 different ways of implementing because there's a lot of, [00:59:00] of configuration opportunities within the, the Chrome stack itself. And, but we, we, when we assessed this, we took the strictest way of configuring the system. And even though we did that, we still found problems. And that was the ones that we addressed. Because now we assume that every municipality and uses the strictest version of configuration. But on top of that, we have to do more to be certain that the GDPR is adhere to. So that's the way that we are looking into this and, and even though there was differences between the different municipalities, And we said, okay, we make one assumption. You all configure it in this way, which is the strictest, and then you fix the rest and then you, you are going to fix the rest. Unless you, unless you do that, you can't use it legally. [01:00:00]

Hac: Okay. Uh, so one last formal question. Yeah. And that is, um, for this case specifically, you did put some words to it already, but, uh, even then, uh, for this case, did you assess this yourself?

Allan: I was both the case worker and the controller. And of course I had a lot of help from my colleagues. And it's a very big case because 50 municipalities, different things. That's a, there's a lot of documentation in this case. 10,000 of pages worth, so, so, so it's a very. Very well-documented case. Mm. And so we, we have been the team, but I'm the one responsible and the one that has written the, the verdict.

Hac: Yeah. Did you make any assessments yourself? Uh, or was it only based on, only based on he earth, uh, own [01:01:00] assessments of the case. Did you like follow up and, uh, like do, did your own research?

Allan: Yeah, we did our own research, but in this case, we started out legal as a, it, it was more or less the legal way to do things. It was not technical. We didn't have a wire shark or something like that. Uh, because there was so many fundamental problems and so many problems in the, in the contract itself and the way that the whole processing was being done, that we, we thought that not necessary to address every point of it, but trying to say, okay, you have to start here. And if you do that, then you will get this part served and that part served, and then you can start thinking about what processing is being done. And the, one of the things that we said the to Elsinore and to the other 50 municipalities, was that they had to do this technical assessment because that's the way that GDPR functions. [01:02:00] It's the controller. Yeah. Why are the risk assessment, the DPIA and so on, and the documentation that has to do all this in advance. And that is the real problem in this case. A little like the cloud services that I told you, we just bought the service because it fix our business problem. And then we don't look into how it is done. And that is what this case has proven and, and what the Danish DPA has told the controllers. You, you have to, you have to go into how the processing is being done. Otherwise you're not accountable on GDPR.

Hac: We have very much understood there that there has been this pattern of a somewhat attitude from, uh, from the data controllers, uh, um, Uh, from view that they didn't take this in much serious. Even though you've did, you've, we've read a lot of, uh, quotes, uh, from [01:03:00] you saying that this is actually a very serious matter and even then, um, you also states that the more they should know the worse it is.

Allan: Yes, that is more or less, because normally in Denmark, we, we tend to go by the, the meaning that, okay, we have no choice when we go to our municipality, when we put our children in school or go to the, if we're going to the hospital and our, or having our tax done, there is only one agency that can do that. The tax agency, the schools in the municipalities or the hospital in the regions and, and where we don't have a choice, the level bar of what you have to know as the controller is much higher because I have no choice, I have to deliver my data to them to get my broken leg fixed and I have to go to the tax authority and, and if, if we are going to have that high kind of trust that I told you that was one of the reasons that in [01:04:00] Denmark we could use a smaller stake than in France, which has to have a bigger stake. It's because we trust our government and the way things are done and, and if we have to, to, to care about that trust and then we have to have this very high bar where, uh, our communities, our municipalities, our regions, and our state, different state agencies, they have to adhere to the rules that abide them. And that is what this is all about. Only do things that are legal.

Hac: So we actually, uh, obviously researched the case. We did our own assessment on all of it. Yeah. And we actually got to four issues with the whole crumble case. Mm-hmm. , and we would like to share them with you Of course, as thank you very much. Some of them are actually, you know, also your own points. Yeah, yeah. Uh, but we, we dumbed it down to four different [01:05:00] points and, um, So the first one is, the obvious one was the lack of any kind of assessment, specifically a lack of risk assessment for the first one. And then something else they did wrong, which is a bit different. Um, not totally different, but more precisely is the lack of control. Mm-hmm. of support scenarios, it support scenarios. Mm-hmm. some that was also, and, uh, this is from our point of view coming from this project. Uh, and then the third problem there that is, is that they assumed Google's agenda. Yeah. So what they did, what they're doing with their data mm-hmm. They, they did not investigate this. So again, both, all three of them so far are kind of assessment. . And then the third, fourth one, I'm sorry, , uh, is also one you mentioned. Mm-hmm. is that when it comes to, uh, primary law and that, uh, the question whether is there a lack of, um, lawfulness in sharing, uh, students information with the third party [01:06:00] students, um, outside the US Yeah. Outside EU and even to us.

Allan: Yeah. And, and, and I, I have to say to you that the problem by giving away data has been, would've been exactly the same if it was to a da, a Danish company. Let's assume that Google was a Danish company living in battle or something like that. It would've been the same problem. You have to have a legal basis to give it. And in Denmark, you can't give public data and data, get it publicly to a private company. That's not allowed unless it is stated in the law. Because in Denmark, the, the government and private, uh, private communist, they are. they are, they are not allowed to, to, to engage in that kind of way. So it's a very big no-no, it's a, it's what you learn at the first year in law school, something like

Hac: that. So there would be no difference in whether there's workspace was a Danish company?

Allan: No of course, for the third [01:07:00] country transfers that would've been a difference. But only that, the rest of it, all of the legality issues, all of the, the lack of, uh, risk assessment and things like that would've been exactly the same. Okay. So it's only the third country transfers That would, would've been different if it was a Danish company. Okay. So

Hac: you are referring to the, the third, uh, I'm sorry, the second point, which is support scenarios.

Allan: Yeah, the support scenarios. Okay. That would've been the only thing that would've been different, because if that has been, would've been done within the eu and that hasn't, that hadn't been a third country transfer. Mm-hmm. . So, so

Hac: these are not IT solution, uh, it related problems necessarily. These are problems which are not even cloud necessarily specific.

Allan: No. But, but, but some of them are. Anyway. I I would like to emphasize that a lot of this is going to, to Google's own fault because the software they have developed originally was designed to gather [01:08:00] people's information to sell us Yeah. White sneakers or brown shoes or something like that. So, so all their software originally was built that way. And when used in, in, uh, in unison in a, in a stack in the technology stack, they are still dripping out data everywhere because there are leaks everywhere in the code designed to, to benefit the Google model. And, and that's just the way they have to rearrange it all because they only rearrange the, the top layer. The, the Google education, the workspace for education layer. But if you use their browser, you, you still leak out information. Mm-hmm. If you use their, uh, operative system, you still leak out information and they have to pull plugs in all of those holes in the bucket to solve the problem.

Hac: So, uh, so lack of assessment control, uh, control [01:09:00] scenarios, uh, Google, assuming Google and lack of lawfulness. Yeah.

Allan: Do you see any, yeah. And, and, and lack of lawfulness is, uh, also around going into contracts that you don't understand. If you don't understand something, don't, don't, don't enter into a contract. So, so that's more or less the problem here. And that's the point of view from the DPA anyway. Yeah, there's, it's the point of the DPA, but. It's something you learn when you go to law school. You, you don't, you don't sign a contract where you don't understand what it's saying because then you just get Yeah. You have pro all kinds of problems. uh, we,

Hac: we do have some alternative solution questions, uh, which is more like, what do you think about opensource and stuff like that. But before, before that, uh, our solution, our concept that we are introducing is something called data confinement. Yeah. Uh, you know, those two words? Yeah. Yeah. But we put, we put them together and boom, we [01:10:00] are inventing the, the plate, um, where we actually say that to any kind of third, uh, you know, data transfer outside eu when it comes to gdp dpr, that we are actually, um, uh, that we are perceiving it. Yeah. Perceiving it as being three threefold problem. One, which is the, uh, the legal aspect, the technical aspect, and then the, um, the more or less managerial managing aspect. Mm-hmm. . So we are saying that these three aspects are, uh, in a sense like as, as like a cake of three, uh, parts where they all go together in how we can, um, uh, use data safely, not only like, uh, on a technical scale, but also on a, on our, on a personal scale that we feel like it's safety. Yeah. Um, so we've looked into the legal ones. Those are the ones that, the laws that [01:11:00] we are going to, that we are making the, that normal companies may don't have control over. Mm-hmm. managerial and technical aspects are something that we can, um, do something for ourselves. Yeah. So we think these three things combined, uh, does data confinement, uh, in eu.

Allan: that's something that we are, we, I think that's a very good thesis to, to work with, but you have to, to take into account that some of, of the technical issues will require that. A lot of the way we are doing service-based architecture today has to be re rewritten in a way where we don't use The problem is that we have gone from, from sector sectorial, data confinements, uh, in every sector in, in the society to having a, a more broadened 10 because the service based architecture have decentralized the data and put it out in the cloud and things like that. And, and we are [01:12:00] about just getting the data wire, our service interfaces when we have to use them. And that concentration of data out there is a potential problem because, uh, the controllership, when we have left it out in. , not just the cloud, but in any context to another process or things like that. And we, we, we, it's more difficult when it's out there. If somebody breaches our controls or our security measurements out there, they get the, a lot of information. When I just had my own sectorial data in my basement, it was limited to that when, if I got breached. But now, if Microsoft security module get breached, or Cisco security module get breached, you get a wide array of data and not just my sectorial data. And you have to take that into account and the way you, you, you think. things [01:13:00] because it's not only third country transfers, that's the problem. It's yeah, different kind of state actors trying to get to our data out there. So I think it's a very good, uh, issue for third country transfers, but we have to think a little further along to, to solve all the problems that we have.

We are not here for that No, no. We are not here for that. We already solved one problem at the time.

Hac: something you said which actually makes a difference for us is that, um, you said, um, abiding, the, uh, you know, if, if we do an SCC uh, that itself is not enough. No. Uh, you need some kind of extra encryption. Yeah. And, uh, those will probably be the two parts of this, uh, trifold. Um, where we both have no some, uh, privacy preserving techniques which is in technical part, but also in the legal part. So this [01:14:00] is about, um, all of them are equally, uh, not, not in every situation. It's not equally important, but every, uh, every part of it, uh, plays a, a, a big part of it. Mm-hmm. , and that, that's the, that's, uh, what we suggest. Yeah. Um,

Allan: think it sounds, sounds very, very plausible. The, the, the problem is that right now, the, the way we do computation, we only do computation on data that is decrypted as a, the computation being done in a computer somewhere. Even if, if it's our own computer will always be on data that is decrypted. And, and the weak point is, is that that part of the, the, the processing, because we can, we can encrypt and transport as easy as anything. We can encrypt when things are at rest at the heart desk and things like that. But in memory and, and in things like when, when computing and [01:15:00] things, we have to do it, uh, on decrypted data. And, and that is what where, uh, some of the newer technologies, like the nitro technology of, of AWS and things like that where we have a a chipset compartment, which is separated in every instance that you maybe can't decrypt. And if you try to decrypt it from that outside looking into the memory or into, you only get garbage from the outside. Yeah. And, and, and or multi-party computation could be one of the other, uh, things, and Yeah. Homomorphic encryption could be be one of the others. Once again, some of these technologies are not quite mature yet, unfortunately. And, and there is no valid basis in, in the, you can't buy it, so to speak. Nobody's selling it. [01:16:00] Okay. And that, and that's a real problem. You know Nitro is now, uh, a saleable product. Nitro and Nitro, yeah. Try to Google that there. It's nitro technology. It's AWS that has made a special chip set on their, their computers where everything is done in a way that is supposed to confine data within the, the memory and, and the, the, the chip processing where it is, it is of course, decrypted, but, uh, where the outside can't look in. You can't get your, your, there's no way you can get your pencils in and, and tab out the data while it is in clear text. Mm-hmm. You will only see garbage everywhere, I think, as encrypted data. Mm. Yeah.

Hac: Yeah. Uh, so yes or no questions. Uh, Google workspace in, in elementary schools in the near future, lawfully?

Allan: It's up to Google and the municipalities as my [01:17:00] answer to that.

Hac: European sovereign Cloud?

Allan: Yeah. That is a, that is probably a thing, but for the DPA or, and GDPR wise, there is no such requirement on the law. So, so I have to say it's not the law require requiring it, it is maybe the market. I don't know.

Hac: Ss there any kind of, uh, other product other than Google Workspace, open source, which can be used, uh, and uh, can live up to these tech giants service quality??

Allan: I have no clue to be honest, because there, there is, it is so, so diverse, uh, landscape out there. But of, I've always been a big fan of, of open source, uh, software as a general, but the problem is, if it's not commercial, commercial, viable [01:18:00] for the people making, uh, on, on open source then it won't be sold to anybody. And if it isn't sold to anybody, nobody else is going to buy. They'll always have to be someone who starts to use something before it gets an inertia that will make it, uh, a market product. And that's probably the problem with a lot of open source. But open source in itself is no solution. It could be as good or as bad as, uh, any other software.

Hac: Last question. Hmm, for real? Yeah. Do you see, uh, do you see the digitalization of schools using Chromebooks? Do you see whether it's Chromebook, whether it's Microsoft, do you see this changing at all?

Allan: I think we are going to have a digitized school because the politicians have chosen to have a digitalized school. And, uh, and if they have chosen that in the rightful manner as a [01:19:00] made of law that is legal in Denmark, then we have to abide by that as, as well as the schools have to abide by the GDPR.

Hac: Thank you for the interview.

Allan: Yeah you're always welcome .

Appendix F

Independent Certifications

Google offers a variation of Workspace for various sectors, including Workspace governments. This means Google must be inclined to uphold some expectations according to different sector standards, including GDPR. Google states that they are committed to providing security for its consumers to demonstrate compliance. This includes undergoing independent verification of their security, privacy, and compliance controls. Google Cloud services, including Google Workspace, offer the following audit reports and certificates;

System and Organization Controls (SOC) reports

SOC reports are based on the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) existing Trust Services Criteria (TSC). Having these SOC reports allow companies to demonstrate compliance and issue trustworthiness. The audits are requested by different companies in various sectors, including healthcare, finance, and cloud computing. The reports establish credibility for companies as well as stakeholders within a company. The audit includes an examination of security measures, the ability of availability services, matters of privacy, and controls related to cyber security.[95] Companies that offer such audits typically offer several audit options, these are SOC 1, SOC 2, SOC 3, and SOC for cyber security. Of these certifications, Google Cloud offers SOC 2 and SOC 3.[96]

International Organizations Standardization - ISO Standards

ISO is an independent and non-profit organization that develops and publishes international standards in most industries. Today they account for more than 20 thousand standards operating in 167 countries which covers everything from manufacturing products to healthcare. The standards essentially guide companies and organizations to operate optimal in their respective fields. Within a certain field, each ISO has one area of focus. ISO standard can be bought from the ISO organization or by enrolling with independent companies to guide comply the guidelines. Such procedures for obtaining such certifications typically start with some initial pre-assessment followed by audit sessions and end surveillance audits to ensure compliance continuity.

The ISO standards which are relevant for Google are standards that relate to topics such as information, electronic systems and cyber security.[97] Of those, Google says, regarding Google Workspace, they provide compliance for ISO 27001, 27017-18, 17701.[96]

ISO 27001 (ISM)

The 27001 standard refers to the code of practice of information security management (ISM). It is a standard that supports requirements for implementing, maintaining and improving an information security management system (ISMS). It addresses securing information, preserving CIA-triad, protecting against threats and attacks, etc. It essentially helps organizations protect their information through the implementation of their ISMS[98]

ISO 27017 (Cloud Security)

The 27017 standard refers to the code of practice for information security controls which is the extended version of ISO 27002. The standard has an enhanced focus on cloud security and cloud services. The additional controls are explicitly related to cloud computing.

ISO 27018 (Cloud Privacy)

The 27018 is the code of practice for operating with Personally Identifiable Information (PII). This standard provides an additional step toward customer confidence, specifically for organizations that handle sensitive personal information.

ISO 27701 (Privacy)

This standard, also known as the privacy information management system, and is built on ISO 27001, guides companies operating with personal PII. The standard is developed to help organizations comply with international privacy frameworks and laws. When organizations collect and process PII this guide outlines control and processes to manage data privacy and protect PII.