Future Business Journal

RESEARCH Open Access

Exploring the General Data Protection Regulation (GDPR) compliance in cloud services: insights from Swedish public organizations on privacy compliance

Awatef Issaoui[1], Jenny Örtensjö[1] and M. Sirajul Islam[1,2*]

Abstract

The adoption of cloud services offers manifold advantages to public organizations; however, ensuring data privacy during data transfers has become increasingly complex since the inception of the General Data Protection Regulation (GDPR). This study investigates privacy concerns experienced by public organizations in Sweden, focusing on GDPR compliance. A qualitative interpretative approach was adopted, involving semi-structured interviews with seven employees from five public organizations in Sweden. Additionally, secondary data were gathered through an extensive literature review. The collected data were analyzed and classified using the seven privacy threat categories outlined in the LINDDUN framework. The key findings reveal several significant privacy issues when utilizing public cloud services, including unauthorized access, loss of confidentiality, lack of awareness, lack of trust, legal uncertainties, regulatory challenges, and loss of control. The study underscores the importance of implementing measures such as anonymization, pseudonymization, encryption, contractual agreements, and well-defined routines to ensure GDPR compliance. The findings emphasize the importance of implementing measures such as anonymization, pseudonymization, encryption, contractual agreements, and well-defined routines to ensure GDPR compliance. Furthermore, this research highlights the critical aspect of digital sovereignty in addressing privacy challenges associated with public cloud service adoption by public organizations in Sweden.

Keywords Public cloud, GDPR, Public organizations, LINDDUN, Information privacy, Sweden

Introduction

Technological development has enabled the growth of cloud services. The National Institute of Standards and Technology (NIST) defines cloud services 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" [22], p. 2]. Five cloud deployment models have been identified that establish how cloud services can be set up [3]. These models are public, hybrid, community, private, and virtual clouds. Each cloud deployment model has its own cost and level of information security. Before choosing one of them, evaluating each cloud model in terms of information security has become necessary [12]. In Sweden's public sector, there is an interest in using public cloud services delivered by international private companies [13]. In light of this, our study mainly focuses on privacy issues and solutions related to the use of public cloud services provided by international private companies.

*Correspondence:
M. Sirajul Islam
sirajul.islam@oru.se
[1] Örebro University School of Business, Örebro, Sweden
[2] Alfaisal University, Riyadh, Kingdom of Saudi Arabia

The European Union's General Data Protection Regulation (GDPR) was implemented to ensure the privacy rights of European citizens. It has created obligations for all organizations that are required to adopt stricter security controls, standards, and processes to ensure compliance [20]. At the same time, the protection of privacy needs to be of consideration when transferring data outside of the EEA (European Economic Area) [2]. Maintaining the data and privacy protection required by current legislation when using cloud services is a new challenge, and it will likely receive much attention in the near future [10]. Several studies have already investigated the use of cloud services and the impact of the GDPR [7, 9, 18, 20, 30]. Despite these efforts, privacy issues surrounding cloud services and GDPR compliance remain a subject that needs further research [20, 30]. In essence, previous studies on cloud services and GDPR have predominantly centered on the EU and its relationship with the United States (US). However, there is restricted research that specifically investigates privacy issues and solutions among public organizations.

The government's vision for Sweden is to be the best in the world at using digital technologies and put an emphasis on protecting both integrity and security [24]. The public sector recognizes the advantages of cloud services and aims to capitalize on their benefits [15]. Consequently, cloud services have gained widespread adoption among Swedish authorities, with growing interest in adopting public cloud services provided by private companies [13]. However, cloud services have enhanced legal and ethical obligations to keep sensitive government data secure; moreover, national security laws and sovereignty concerns complicate this decision [15]. When It-driftsutredningen [17] presented its report, some public organizations in Sweden were still uncertain about legal conditions when outsourcing data to a private company.

Even though a few studies have already addressed cloud services, GDPR, and public organizations, a clear research gap can be seen in studying privacy issues among public organizations based on a Swedish perspective. As such, our study aims to contribute to this area of knowledge and understanding. This paper attempts to address the research gap with the aim of uncovering some of the privacy issues and the solutions associated with public cloud services among public organizations in Sweden, following the GDPR regulation. We, therefore, investigate the following two research questions in this study: What are the privacy issues related to GDPR that the public organizations of Sweden face when using public cloud services? And how do public organizations address those issues?

Theoretical background

General Data Protection Regulation GDPR (GDPR)

On May 25, 2018, the General Data Protection Regulation GDPR (GDPR) entered into force and became directly applicable in all EU Member States [11]. The aim was to strengthen data protection across Europe to address privacy challenges when using new technologies [20]. The GDPR is based on seven principles that define how personal data will be processed; each of the principles is presented in Article 5 of the GDPR [11]. Article 4 of the GDPR [11] introduces three entities that process personal data: the data subject (the person whose data are collected), the data controller (who collects and uses personal data), and the data processor (who processes data on behalf of the data controller). Additionally, Article 4 of the GDPR [11] designates a supervisory authority responsible for overseeing the process and imposing administrative fees in accordance with Article 83 of the GDPR. In this study, we assess that the data controller is a public organization, and the processor is the CSP (cloud service provider). To ensure the guaranteed level of protection of personal data, Article 44 of the GDPR [11] states that the transfer of personal data to a third country shall occur if the conditions in Chapter 5 have been complied with by both the controller and the processor. Various privacy agreements, such as the privacy shield, have been established to ensure adequate data transfer between the EU and the US.

LINDDUN framework

Threat modeling is the process of identifying privacy or security issues within a system [8]. Different threat modeling frameworks have been identified in the literature, with one example being STRIDE, developed by Microsoft to identify security threats [8]. STRIDE stands for spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. However, STRIDE does not cover privacy threats. To address this gap, Deng et al. [8] created LINDDUN, a framework based on STRIDE that is specifically used to identify and mitigate privacy threats. LINDDUN aims to analyze privacy threats during system development and can also be applied to existing systems to identify privacy threats [34]. LINDDUN consists of seven privacy threat categories represented by the acronym. Each of these seven categories is associated with a private property that the corresponding threat violates [8]. The LINDDUN methodology has gained widespread acceptance within the literature.

Robles-Gonzales et al. [27] focused on the first two steps in the problem space to achieve a reliable privacy threat analysis. Reisinger et al. [26] used LINDDUN and STRIDE in conjunction to conduct a security and privacy

analysis for the use of unified communications. Crepax et al. [5] employed LINDDUN with the risk management methodology of the EU project PDP4E and linked it with the General Data Protection Regulation (GDPR). In contrast to previous research, this study exclusively uses LINDDUN to categorize the privacy issues and solutions identified from the empirical data. Nevertheless, this study draws upon the work conducted by Crepax et al. [5] as a guideline and reference to connect the LINDDUN framework with the GDPR. According to the authors, they can be "…aligned to each other to bridge the existing gap between legal and technical practices" (Crepax et al. [5], p. 27]).

Methodology and data

This study follows an interpretative qualitative approach since its aim is to understand individual and organizational meanings [6, 25]. This approach enabled the researchers to gain insight into the use of public cloud services among public organizations in Sweden. A literature review was conducted as a guideline to identify the research methodology: LINDDUN, and to discuss the findings presented in this study. It also allowed the researchers to be aware of existing work in the field of cloud services.

Interviews and selection of respondents

The researchers conducted an interview study to explore privacy issues and solutions related to public cloud services among public organizations. To find respondents, they contacted public organizations in Sweden between mid-February and March 2022. The contact information was gathered from their websites and via LinkedIn. An invitation email was sent to multiple public organizations in Sweden, explaining the purpose of the study. The researchers used purposive sampling, selecting respondents who were more relevant to the study's purpose [25]. They specifically sought respondents who had insight into cloud services and significant experience with privacy issues. Seven respondents from five different public organizations participated in the study (see Table 1). One respondent was interviewed from each organization, except for a public university, where two interviews were conducted with three participants: one individual and one group interview. Each organization offered a relevant context because they had extensive experience in using public cloud services and implementing the GDPR, providing rich and detailed knowledge of common issues and solutions.

The perspective of public organizations in Sweden was sought since they must adhere to the laws and have a similar view on using public cloud services delivered by international companies. An interview guide was developed with questions centered around public cloud services and the GDPR, formulated based on the categories of the LINDDUN methodology. The semi-structured interviews lasted approximately one hour each and were recorded and transcribed. The interviews were conducted over Zoom, Skype, or Teams, allowing for face-to-face interactions instead of phone interviews. Before the interviews, each respondent received a list of topics to think about their views, helping to establish credibility as serious researchers. The researchers stopped conducting interviews when data saturation was reached.

Data analysis

In qualitative research, data are considered descriptive as they take the form of words rather than numbers. Quotations from the empirical data are used in the results to illustrate the presentation [4]. The researchers developed different categories based on concepts drawn from the LINDDUN methodology. Visual tables [25] were employed to categorize the findings. The use of tables allowed them to rearrange different segments and modify the categories during the analysis process [25]. The researchers read through the empirical data multiple times and categorized the findings according to the LINDDUN privacy threat categories.

Table 1 List of respondents

Level of position	Respondent	Organization	Time (min)
High level in the department of information security	R1	Transport Administration	50
	R2	Social Insurance Agency	60
	R3	Swedish employment service	45
	R4	A Public University	57
	R5	Tax Authority	52
	R 6	A Public University	58
	R 7	(Group interview)	

Result

This section presents the findings from the interviews, and the analyses are based on the LINDDUN framework presented in Sect. "Theoretical background". Additionally, this section provides information about the roles and organizations that were interviewed for this study (see Table 1).

Linkability

From a legal perspective, the failure to hide a link between information could lead to unexpected personal data processing [5]. Both R2 and R3 addressed the issue of the cloud service providers (CSPs) potentially sharing information with a third party. Two potential solutions have been identified to mitigate this issue. The first solution, addressed by R3, involves keeping the collected information at their own premises, thereby reducing dependency on the market and available CSPs. This approach was also mentioned by R5, who highlighted the need for more on-premises solutions.

The second solution is to establish contractual agreements with the CSPs to ensure that information stored with them is not misused or shared with a third party. This solution was emphasized by R1, R3, R4, and R5. Furthermore, R3 provided additional insights into the contracts and addressed the issue of establishing contracts with US-based CSPs, elaborating in the following way:

> *Well, we would like, for instance, Microsoft to sign a contract with us where they promise not to reveal our information to a third party. But they are refusing even that. So, then we could have a challenge when it comes to how they treat the information within Microsoft. (R3)*

Against this background, the respondent decided to exclusively use suppliers based in the EU and to mandate that all stored information is kept within the EU. When compared to US-based CSPs, European CSPs provide a promise within the contracts not to disclose their information and assure that they will not utilize suppliers outside the EU. However, there remains a potential concern regarding trust issues, as a CSP could potentially deceive the organization. R5 further elaborated on this trust issue, highlighting that CSPs can employ various deceptive practices, and it may be challenging to find concrete evidence to verify such actions. They elaborated in the following way:

> *So usually, we have to go through the paper trail and say, "This is the procurement; you have to provide this information and have a contract where you say you'll do certain things. If that idea wouldn't be true, it is a breach of contract, and we will fine you." (R5)*

Regardless, establishing good contracts and building strong relationships with the CSPs and their providers were also emphasized by R1. Ultimately, it is not appropriate to provide a significant amount of information to a business partner that cannot be trusted. In the same context, R2 also pointed out that if vendors cannot be trusted, they should be replaced.

To summarize, two significant privacy issues identified are related to CSPs potentially sharing information and trust issues with the CSPs. These issues can potentially violate all GDPR principles if the data controller is unaware of how data are processed [5]. Particularly, the principle of Lawfulness may be compromised if there is no legal ground for processing [5, 11]. Therefore, to avoid misuse of information and trust issues with CSPs, the respondents suggested some solutions, such as establishing contractual agreements and the need to rely more on on-premises solutions, as well as exclusively using EU-based CSPs. Implementing these solutions would contribute to compliance with the principle of Accountability.

Identifiability

Identifiability refers to the ability to identify to whom the information belongs [34]. In terms of identifiability, R2 and R5 mentioned an incident that occurred in 2017 at the Transport Agency. R5 explained that it was discovered that unauthorized individuals had access to their driver's license register. However, there was no concrete evidence of anyone having infiltrated their system. This incident was identified as a potential issue by the respondent and elaborated upon in the following way:

> *But then we have folkbokföring, the register of every Swedish citizen. That register is at the tax authority, and if that register is gone, then Sweden has no idea who is a Swedish citizen or not. If that risk is compromised, it is very, very bad. (R5)*

The above statement highlights the consequences of compromising the system at a public organization. To avoid such situations, R5 emphasized the importance of having control over the information and the system. However, they also pointed out that achieving absolute full control can be challenging. Similarly, R6 mentioned the difficulty of implementing double confirmation processes, such as using email, passwords, and pin codes. Some employees may try to avoid double confirmation due to a lack of awareness about its importance.

However, R3 confirmed that there are instances where employees act securely. For example, banks advise older users against using electronic ID when someone initiates

contact to prevent fraud. While this is a good practice, it can be problematic to contact and identify the correct person. In such cases, Swedish citizens have increased awareness. R4 also elaborated on this issue in the following way:

> *So sometimes, I think that the personal needs and the personal development for services are much faster than the organization changes. (R4)*

The above statement suggests that organizational development can sometimes lag behind personal needs. Users may be more willing to adapt their behavior when it comes to protecting their personal information.

R2 provided another example related to identifiability. The respondent mentioned that all the information a university stores about its students becomes more critical if a university student later becomes the prime minister of Sweden. However, R6 and R7 mentioned that this is not the case, and the only way a person's status can change is if they receive a secrecy mark. Nevertheless, the information may still be available at different locations. They elaborated on this issue in the following way:

> *... like if you work at Åklagarmyndigheten, then your full name, address, and telephone number will not be accessible. But if you look this person up from where they studied, the information that the university has will still be available. You can, if nothing else, if you haven't thought about all the connections where you have stored data previously, find that information accessible at different locations. (R7)*

The statement above highlights that even if the classification of information changes, it may still be accessible from different locations. R5 also pointed out that this is not solely a cloud issue, but it can potentially have some impact. This suggests that the handling of sensitive information and its accessibility can be influenced by various factors beyond just the use of cloud services.

Non-repudiation

Crepax et al. [5] linked non-repudiation with the principles of integrity and confidentiality. Failure to maintain non-repudiation could result in the loss of control over personal data and increase the risk of unauthorized access. In such incidents, the data controller will likely be held accountable [5]. All respondents expressed concerns about the US and its surveillance laws, such as Executive Order 12 333. This law allows the US government to access data from US companies without any notice. This issue was identified by R4 and R6. If US public cloud services are used, R1 suggested implementing measures from the GDPR, such as encryption. However, both R1 and R2 agreed that encryption might not be as useful as expected, and they elaborated on this issue in the following way:

> *I don't think that this is a valuable strategy because if you encrypt the information in a way that the cloud service providers cannot access it, you lose a lot of value from the cloud services. (R1)*

Against this background, there is a conflict among the respondents regarding the effectiveness of encryption. R6 argued that all data stored in a US cloud should be either encrypted or pseudonymized, with the encryption keys kept within the EU. However, R2 confirmed that the US collects data in advance even if it cannot decrypt it. This creates uncertainties about the US government's future ability to collect and access data. The previously mentioned issue is not the only risk related to non-repudiation. The surveillance law enables the US government to force suppliers to cease operations abruptly. R2, R3, and R5 confirmed this. In a worst-case scenario, this could also happen to Sweden. R5 elaborated on this matter in the following way:

> *And to gather as much data about the whole Swedish society into one country's cloud services maybe is not a good idea. You lose sovereignty in that sense, or a lot of our systems could break because we don't have access to them, or we don't have access to our data when we need to have access to it. (R5)*

Based on the above statement, we can conclude that establishing cloud solutions in Sweden is of utmost importance. The potential impact on Swedish society could be significant if access to information or systems is denied when needed. However, it is also acknowledged that international private companies are developing effective solutions. Therefore, R2 emphasizes the importance of collaborations between the public sector and private companies. They elaborated on this aspect in the following way:

> *I mean, we have placed people on the moon. Skype was created here in Stockholm. We have a king, we have Ericsson, we have Spotify. I mean, if you look at the Jaas Gripen, the aeroplane is a flying computer center. Amazing! Then to say, "Well, for us to be able to send emails, we need American solutions." That is crazy! (R2)*

Based on the above information, we can conclude that maintaining digital sovereignty has become a crucial issue. The respondent emphasized the need for the Swedish government to provide clarity on what is required to uphold digital sovereignty. This is essential to ensure that all services continue to function effectively during a crisis or a war, safeguarding the country's digital infrastructure

and independence. By addressing these concerns and establishing clear guidelines, Sweden can better protect its digital assets and maintain its ability to operate critical services even in challenging circumstances.

Detectability

Someone can connect information without having direct access to it. For example, by knowing that an individual has a health record in a rehab facility, one can deduce that they have an addiction [33]. To avoid detectability, R4 confirmed that sharing information has become more challenging, and certain processes are no longer allowed under the GDPR. For instance, emailing and asking questions about a specific diary request may not be permissible. The respondent believes that as a result, much useful information has been lost, and they elaborated on this issue in the following way:

> *I think that those types of issues are not IT-related, but they have quite a big impact on some kind of situation. (R4)*

Based on the above statement, not all the issues identified in this study are directly related to the use of public cloud services, but they can potentially have some impact on data privacy and security. Furthermore, R2 mentioned an issue concerning US CSPs potentially selling information to third parties, who might then offer services to users based on that data. This practice is not allowed according to the GDPR, as confirmed by R4. To prevent CSPs from detecting sensitive information, R3 explained that measures such as performing due diligence and controlling their suppliers are implemented. These steps are essential to ensure that the data is adequately protected and that the privacy of users is maintained. R3 elaborated on this approach in the following way:

> *... and that is allowed according to our contracts. But, of course, you have to be very careful and very well aware when you do that. So, at the end of the day, we don't know, we don't have full control. (R3)*

Regardless, it is challenging to control everything. For instance, R2 explained that their staff uses the Stockholm metro, where the camera surveillance is controlled by the Chinese government. This situation raises concerns about data privacy and surveillance, and R2 elaborated on this issue as follows:

> *So it is hard to do everything, but we are doing everything we can in the environment we control. However, it has made it almost impossible to use public cloud solutions if they are connected to a third country. (R2)*

This statement emphasizes the challenges of controlling how information is treated when it is stored outside Europe. This highlights the importance of using a public cloud solution within the EU and Sweden to ensure greater control over data privacy and security. By choosing cloud services within the EU, organizations can adhere to stricter data protection regulations and have more confidence in how their data are handled and secured, reducing the risks associated with data being stored in jurisdictions with potentially different data protection standards.

Disclosure of information

Exposure of personal information to unauthorized users, which is not supposed to be shared, is indeed a critical issue [8]. To ensure confidentiality, R1 explained that their organization conducts information classification whenever a new system is created or new services are employed. R2 also stressed the importance of information classification, as information can become more sensitive over time, leading to potential issues if not handled properly. The respondent also acknowledged that this issue could arise because certain information, such as one's address or social security number, is classified as public in Sweden. R5 recognized that issues can arise, but the release of information must align with the laws and regulations. If certain information should be kept secret, there must be legal proof to justify it. In addition to this, R3 also stated that:

> *Our interpretation is that we have one law in Sweden that regulates the publicity and the confidentiality of information, and that law only exists in Sweden; it's not harmonized within the European community. So, information that is under confidentiality can't leave Sweden because it would leave the legislative area of Sweden. (R3)*

To avoid exposing personal information, it is essential for public organizations to prioritize safeguarding all the information they collect. As they hold a monopoly on their services, there is a special demand for robust information security. R2, R3, and R4 all recognized the significance of this aspect and elaborated on it in the following way:

> *We are an important part of Swedish society. We cannot afford to look bad in the eyes of the members of society or companies in Sweden. (R5)*

Against this background, all of the respondents expressed concerns about the surveillance laws in the US. They highlighted that the US government can access data from US companies without any notice, regardless

of where these companies store personal information. Both R4 and R5 confirmed this, emphasizing the potential implications of such laws. In case of such access by the government, R4 explained that it might not count as a breach, as the data is being accessed by authorities, and for this reason, services like Microsoft 365 can still be used.

Furthermore, R1 addressed the fact that larger organizations with bigger budgets can prioritize information security and digital sovereignty more effectively. However, the lack of resources among smaller organizations is a significant issue, as emphasized by R4 and R7. Ensuring a secure infrastructure requires considerable resources. One potential solution discussed by the respondents would be to develop a secure data center in Sweden. While initiatives in Europe and Sweden were mentioned during the interviews, creating something on par with the international standard could be expensive. This highlights the challenges faced by organizations in maintaining high levels of information security and data sovereignty in a cost-effective manner.

Content unawareness

Users should be aware of their data, and organizations should only seek and use the minimum necessary information to perform the related function [8]. However, one of the main challenges is the unawareness of users about their online behavior [34]. An issue highlighted by both R4 and R5 is the concern about the amount of information supplied by users. The more information provided, the higher the risk that it can be misused by unauthorized individuals. R4 also mentioned that information shared on platforms like Facebook can be used to make assumptions about users' behavior. Therefore, being more aware of where information is located and how it can be accessed is crucial, as emphasized by R5. This underlines the importance of educating users about responsible data sharing and online behavior to enhance their awareness and protect their privacy.

> *With opening information, you have Facebook accounts, email accounts, email addresses, and there is so much open information. You start again combining all of this, and so again, maybe it comes back to the suitability thing. Maybe some data doesn't belong to some services or some companies' hands because of this. (R5)*

Another issue addressed by R4 concerns the challenge of transferring knowledge to those who are using public cloud services. The respondent discussed how sometimes employees do not fully understand the reasons behind certain security measures or policies that have been implemented. One solution to address this issue is to identify the level of knowledge that employees possess and then implement strategies to increase their awareness and understanding of information security practices. R6 added that it does not matter how much information security is added if employees do not have the necessary awareness and understanding of these measures. This statement emphasizes the importance of not only implementing security measures but also ensuring that employees are well-informed and educated about them to effectively protect the organization's data and resources. Proper training and awareness programs can play a critical role in enhancing the overall security posture of the organization.

> *Because the person, I mean the human being, is the weakest link. It doesn't matter how much security we put on technical information. The human is always the weakest link. And we can handle information. (R6)*

The above statement highlights an important aspect related to information security education within the organization. One of the interview questions asked whether the IT department works to educate users on information security (IS). R4 explained that information security education is not done as much as they would like, and it can be challenging to manage information security across different departments within the organization. This response suggests that there may be a need for better coordination and efforts to enhance information security education throughout the organization. Strengthening information security awareness and training programs can help employees better understand the importance of safeguarding data and adopting secure practices in their daily work.

Policy and non-compliance

This threat occurs when the system is not compliant with applicable legislation and policies [5]. During the interviews, several regulatory challenges were identified within the organizations. For instance, R6 emphasizes that one large issue arising after GDPR is the ability to show GDPR compliance, and for that, much more documentation is needed than before. But at the same time, documentation is crucial to demonstrate that the collected data are protected. The importance of documentation was also addressed by R1. Another regulatory issue,

addressed by both R3 and R5, concerns booking airline tickets, which led them to change the process since there is no legal way of doing it. R5 also added that they have stopped using public cloud services and procured new services that are legal. In addition to this, the respondent elaborated in the following way:

> *We can't suddenly do our own analyses and say we think this is okay, even though we know the real judgment, and it isn't. (R5)*

As a public organization, they have to act according to the law, and unnecessary risks should not be taken. Both R2 and R5 confirmed this. Because of this, R1 noted that many public organizations are hesitant to use public cloud services. Those who still use US CSP have faced many challenges that need to be addressed to ensure compliance with the principles of the GDPR. One of the largest issues identified by R4 relates to not following these principles after the Schrems II judgment, and many have spent hours analyzing this ruling to fully understand what is allowed. The respondent elaborated in the following way:

> *"And no one seems to exactly state what actually is the final interpretation of the ruling." (R4)*

To avoid misinterpretation of Schrems II, the respondent suggested that someone should state how it can be interpreted and provide recommendations based on a Swedish perspective. As a result of Schrems II, the respondent felt that the full potential of cloud services has not yet been used as intended.

Discussion

This section presents the discussion based on the literature review and the empirical findings. Additionally, this section follows the LINDDUN framework presented in Sect. "Theoretical background".

Linkability

Linkability indicates that someone can link information [8]. Misuse of personal Linkability indicates that someone can link information [8]. The misuse of personal information could violate all the principles of the GDPR [5]. Given the importance of personal information and the implications of misusing information, Shastri et al. [30] concluded that this risk should be eliminated as soon as possible. Diker Vanberg [9] argues that one crucial aspect of the GDPR is to protect information against misuse. Our findings, therefore, show the importance of establishing contractual agreements with CSPs to avoid misuse. Both Rodriguez-Doncel et al. [28] and Jaatun et al. [18] highlight that this would increase accountability, meaning that information is trusted by the CSP from being collected until destroyed [18].

Identifiability

The ability to identify information can result in severe privacy violations if the data subjects assume that they are anonymous [33]. Anonymity is about hiding the link between pieces of information, for instance, information about a person in a database [34]. Our findings confirm the pre-existing findings by Domingo-Ferrer et al. [10] and Aslak Juliussen et al. [2] that anonymization or pseudonymization can enable sensitive information to be shared with an untrusted third party without disclosing information. However, if it is not done appropriately, the protection will be ineffective and may not be sufficient to ensure Identifiability [10, 31]. Therefore, this could be considered a violation of the GDPR due to not complying with the principles presented in Article 5 of the GDPR [11].

Our findings show that public information could be sensitive in the long run. Therefore, large volumes of information should be stored and safeguarded in a controlled environment. This finding has been confirmed by Tcherykh et al. (2019). Regardless, risks can still occur, and our findings show that employees sometimes find it challenging when a public organization implements new technological solutions. This has also been pointed out by Jaeger et al. [19]. It has, thus, become crucial for organizations to examine employees' behaviors when new technological solutions are implemented [21].

However, our findings also confirm existing knowledge by de Carvalho et al. [7] that users sometimes understand the risk due to increased awareness from the market. Our findings address how banks in Sweden have done this to minimize fraud related to the use of BankID. Crepax et al. [5] pointed out that if private information is accessible to untrusted parties, it can cause financial fraud or identity theft. Informing users about the risks can allow them to make better decisions regarding using personal information [5]. This indicates that depending on the technological solutions that are being implemented or the situation, employees' behaviors might vary as addressed by Li et al. [21].

Non-repudiation

Non-repudiation indicates that an attacker knows that a user has said or done something [34]. Failure to ensure non-repudiation can increase the risk of unauthorized

access [5]. Our findings confirm the already existing knowledge by Domingo-Ferrer et al. [10] that to store and process information in the cloud, one must guarantee that no one else has access to it. This has been deemed tricky when the CSPs and the ones using the cloud are under different jurisdictions [10]. Our findings show that public organizations, especially, are concerned about the US and their surveillance laws. Consequently, failure to comply with the principles of integrity and confidentiality can increase the risk of unauthorized access [5, 11].

Our findings also confirm the already existing knowledge by Moerel and Timmers [23] that the US government can order their companies to foreclose from one day to another. The authors pointed out that the Netherlands and the EU are limited when third countries like the US or China take measures. Solutions need to be developed to ensure less dependence on foreign suppliers [23]. This has been confirmed by our findings but from a Swedish perspective.

Detectability

Detectability indicates the ability to determine that information exists within a system without having access to the system [8]. Based on our empirical findings and evidence from the literature, detectability has an interrelationship with the disclosure of information. This was confirmed by Reisinger et al. [26] and Wuyts et al. [33]. The findings in this study not only address the impact of the GDPR and the use of public cloud services but also show the importance of not performing processes that could increase the risk of detectability. Our findings confirm the existing knowledge by Domingo-Ferrer et al. [10] that public CSPs have been analyzing personal information without users' knowledge and have shared information with a partner who can then offer a service.

Disclosure of information

Disclosure of information indicates the ability to expose personal information to someone who is not supposed to have access to it [8, 34]. To maintain security when outsourcing data, attention should be given to Recital 83 of the GDPR [11]. The findings of this study give significant attention to the need to safeguard information among public organizations. Concerning a European perspective and digital sovereignty, many are concerned that US intelligence agencies can collect information from US companies [23]. Against this background, our findings confirm the preexisting findings by Försäkringskassan [13] that many public cloud services are both inappropriate and illegal to use. To maintain digital sovereignty in Sweden, our findings address the importance of developing solutions in Sweden.

This study discovers that a government initiative in Sweden aims to develop a solution for a secure infrastructure, but it has been deemed to be complicated. This was also confirmed by Moerel and Timmers [23], since larger CSPs have unlimited access to resources and can offer new competitive solutions. However, without government initiatives, there is a risk of increasing vendors' lock-in. Suppliers make it hard to switch from one solution to another, or it could be costlier for an organization to change from one supplier to another [23], which is in line with our findings. In the same context, It-driftsutredningen [17] reports that lock-in effects are one of the greatest obstacles for Swedish public organizations to achieve cost-effective IT operations. One could also argue that without developing solutions in Sweden or in the EU, there is also a risk that technological development will slow down and negatively impact digital sovereignty, as confirmed by Moerel and Timmers [23].

Content unawareness

Content unawareness indicates that users are unaware of sharing information [8]. The study by Islam and Karlsson [16] also confirmed our findings, that the lack of awareness and knowledge of information security is one of the most challenging issues managers face. In the same context, our findings address the importance of establishing routines within public organizations but also the need to have good competence. This is consistent with the government's sub-goal to achieve digital competence [24]. Our findings show that the public organizations interviewed for this study have good IT competence. However, when It-driftsutredningen [17] presented its report, several authorities in Sweden had difficulties in establishing their own IT competence. Therefore, access to relevant competence in Sweden needs to be strengthened. This was also confirmed by Näringsdepartementet [24], who emphasized that digital competence is required to create trust in the services that public organizations in Sweden provide. Additionally, high competence among employees can also provide several benefits such as increased productivity [21].

Policy and non-compliance

Policy and Non-compliance indicate that applicable legislation has not been complied with Crepax et al. [5] and Wuyts and Joosen [34]. Recital 6 of the GDPR [11] informs that digitalization enables a free flow of personal information both within the EU and outside. The GDPR is intended to establish a framework that guides the use of personal information and simultaneously strengthens data protection rights [7]. Our findings confirm the preexisting knowledge of de Carvalho et al. [7] that to

ensure GDPR compliance, all organizations must register and keep evidence of data processing activities. Based on this, we can see that there is an interrelationship between Policy and Non-compliance and Content Unawareness, as confirmed by Wuyts et al. [34] and Reisinger et al. [26]. To meet the requirements of the GDPR, Li et al. [20] emphasized that many resources are needed to adjust the processes. Our findings confirm this and address that adjusting the process was also done after the Schrems II judgment.

Conclusion

This study aims to uncover privacy issues and solutions related to the GDPR from Swedish public organizations' perspectives. We investigated the following two research questions: (1) What are the privacy issues related to the GDPR that the public organizations of Sweden face when using public cloud services?, and (2) How do public organizations address those issues? A summary of the findings of these two questions is presented in Table 2.

With the establishment of the GDPR, privacy protection has become crucial for all organizations. This applies especially when considering public organizations in Sweden. Sweden strives to be one of the leading countries in the world in using digital technologies [24]. This study has reported that there is a great interest in the public sector in using public cloud services provided by international companies. However, at the same time, many public cloud services that are available on the market are not suitable or legal to use.

This study presents several privacy issues that have occurred since implementing the GDPR; however, it has been unclear whether some are related to the use of public cloud services. For instance, one issue concerns the amount of information shared among users. This is in line with the preexisting findings by de Carvalho et al. [7] and Crepax et al. [5]. In summary, public cloud services can cause many privacy issues if public organizations are unaware of how they have been employed (see Table 2, column 1). Regardless, this study demonstrated the importance of digital solutions for public organizations in Sweden. Therefore, to ensure compliance with the GDPR, public organizations in Sweden must carefully use public cloud services. Considering the privacy issues and solutions associated with the public cloud will eventually contribute to the government's vision for Sweden. At the same time, Näringsdepartementet [24] emphasized that it will eventually increase the confidence of the digital society in Sweden.

Policy recommendation

We have previously mentioned in this paper that the use of public cloud services enables public organizations to transfer their data across the border. It has made information more easily and practically accessible [1]. With the establishment of the GDPR and the need to protect digital sovereignty, this paper has also emphasized the restriction on transferring data outside the EU. However, at the same time, different agreements between the EU and the US have been established to provide legal obligations to transfer data across the Atlantic. Nevertheless, due to varying views regarding protecting human rights and freedom, everyone has failed [29]. As a result, most of the findings in this study correspond to issues regarding transferring personal information due to the Schrems II judgment. In the study by Abraha [1], the author emphasized the consequences, such as the security and privacy of individuals when a legal agreement has failed. One can conclude that the current system has become problematic for several parties both in the EU and the US, as confirmed by our findings, Tracol [32], and Abraha [1]. It is only fair that some legal clarity is provided, and at the same time, there is also a need for the US to amend its domestic law on surveillance [32] or establish a comprehensive privacy framework [29]. Otherwise, there is a risk that future agreements between the EU and the US could fail again.

Contributions and future research

Ever since the GDPR became directly applicable in all EU Member States [11], several concerns have arisen about how to efficiently process and store personal data in the cloud [14]. This study aims to uncover issues and solutions that public organizations in Sweden experience with the use of public cloud services following the GDPR. Our analyses in this study have added to existing research by studying public organizations in Sweden. By analyzing our findings, we were able to determine the most significant privacy issues that public organizations experience with the use of public cloud services, such as unauthorized access, misuse of information, lack of awareness, legal uncertainties, and lack of trust. We contribute to the theory by studying public cloud services among public organizations from a Swedish perspective, in contrast to the previous literature that tends to focus more on the EU-US relationships rather than a specific nation [29].

Limitations

The major limitation of this study is the low number of respondents. Even though we attended data saturation to confirm our result even further, more interviews would have been performed. One critical view of our study is that other studies have got a similar result. But at the same time, the main focus has been on the EU, and there is a lack of studies according to Swedish perspectives. Therefore, we had some difficulties confirming our

Table 2 Summary of the findings

LINDDUN	Privacy issues	Solutions
Linkability	The risk of cloud service providers misusing and sharing information is concerning. There is a trust issue with cloud service providers. Privacy issues related to Linkability can violate all of the principles of the GDPR	The need to establish contractual agreements with cloud service providers and to use EU cloud service providers is crucial to ensure GDPR compliance
Identifiability	Information can become sensitive over time, especially when storing a large volume of data with a third party, as it can be identified. One of the contributing factors to this is the lack of awareness among employees. Privacy issues related to Identifiability can potentially violate all of the principles of the GDPR	To ensure that personal information remains unidentified, GDPR measures such as anonymization or pseudonymization need to be implemented. Simultaneously, it has become crucial to exercise control over the cloud service provider and enhance employee awareness
Non-repudiation	The surveillance laws in the US raise concerns about the risk of unauthorized access and the potential loss of digital sovereignty. Privacy issues related to Non-Repudiation have the potential to violate several GDPR principles, including Integrity and Confidentiality, Accountability, and Accuracy	To avoid surveillance, strong encryption is necessary if data are to be stored within the US. It is essential to uphold digital sovereignty within Sweden. Collaborations and the development of secure cloud solutions in Sweden are of great importance to ensure GDPR compliance
Detectability	Public cloud service providers have been analyzing and exploiting personal data without users' knowledge. Privacy issues related to Detectability can potentially violate all of the principles presented in the GDPR	To mitigate the risk of detecting sensitive information, certain measures need to be implemented, such as conducting due diligence and closely monitoring the activities of cloud service providers to ensure GDPR compliance
Disclosure of information	The exposure of personal information to unauthorized individuals, the presence of surveillance laws in the US, and the lack of resources among public organizations are all concerning factors. Privacy issues related to Disclosure of Information can indeed impact all of the principles presented in the GDPR	Safeguarding information has become crucial to ensure confidentiality. It is necessary to develop secure infrastructure in Sweden or Europe to strengthen data protection measures. Contractual agreements can also be utilized to limit access from suppliers and further enhance security. Additionally, conducting an information classification process can help categorize data appropriately, thereby aiding in its protection
Content unawareness	The lack of awareness among users and organizations on how to handle information is a significant concern. Additionally, the vast amounts of information provided by users add to the complexity of data management. Misunderstandings regarding the distinction between IS and IT further compound the challenges. Privacy issues related to Content Unawareness can indeed lead to violations of GDPR principles, as it may result in mishandling and unauthorized access to sensitive data	Absolutely, to ensure GDPR compliance, it is essential to establish routines and policies for information security awareness within an organization. Moreover, educating users about their behaviors when sharing or managing personal information is crucial. By promoting a culture of data protection and privacy consciousness, organizations can strengthen their overall security posture and effectively meet the requirements set forth by the GDPR
Policy and non-compliance	The legal uncertainty surrounding transferring data outside the EU and the risk of misinterpreting Schrems II ruling are major concerns for organizations. Privacy issues related to Policy and Non-compliance can significantly impact the GDPR principles of Lawfulness, Transparency, and Accountability	Provide recommendations and guidelines to avoid legal uncertainties. The need to establish a new privacy agreement between the EU and US in order to ensure GDPR compliances

findings from a Swedish perspective. However, still, this limitation demonstrates the importance of continuing to study cloud services in Sweden.

Abbreviations

CSP	Cloud Service Provider
EEA	European Economic Area
ENISA	The European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation
HR	Human resources
IS	Information security
ISP	Information security policy
IT	Information Technology
LINDDUN	Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Content Unawareness, Policy and Non-compliance
MSB	Swedish Civil Contingencies Agency
NIST	National Institute of Standards and Technology
NSA	National Security Agency
US	United States
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of privilege

Acknowledgements
The authors would like to thank Professor Åke Grönlund for his remarks during the study.

Author contributions
While the first two authors were actively involved in data collections, analysis, and writing; corresponding author mostly involved guiding in methods, structuring, and finalizing. All authors read and approved the final manuscript.

Funding
Not applicable.

Availability of data and materials
Will be made available as and when needed.

Declarations

Ethics approval and consent to participate
No ethical issues involved. Interviews were anonymous.

Consent for publication
Authors hereby give consent for publication after passing the review processes.

Competing interests
The authors have no competing interests, including financial and non-financial, to declare that are relevant to the content of this article.

Received: 18 May 2023 Accepted: 30 November 2023
Published online: 15 December 2023

References

1. Abraha HH (2021) Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives. Int J Law Inf Technol 29(2):118–153. https://doi.org/10.1093/ijlit/eaab001
2. Aslak Juliussen B, Kozyri E, Johansson D, Rui JP (2023) The third country problem under the GDPR: enhancing protection of data transfers with technology. Int Data Priacy Law 6:66
3. Azeemi IK, Lewis M, Tryfonas T (2013) Migrating to the cloud: lessons and limitations of "Traditional" IS success models. Procedia Comput Sci 16:737–746. https://doi.org/10.1016/j.procs.2013.01.077
4. Bogdan RC, Bilden SK (1998). Qualitative research for education: an introduction to theories and methods, 3 edn. Allyn & Bacon. http://math.buffalostate.edu/dwilson/MED595/Qualitative_intro.pdf. Accessed 15 June 2022
5. Crepax T, Diaz N, Muntés V, González E, Dominiak J, Sánchez D, Rios E, Iturbe E, Ruiz A, Miadzvetskaya Y (2020) Risk management method for data protection and privacy V2, Version V1. Project PDP4E
6. Crowe S, Cresswell K, Robertson A, Huby G, Avery A, Sheikh A (2011) The case study approach. BMC Med Res Methodol 11:article 100. https://doi.org/10.1186/1471-2288-11-100
7. de Carvalho M, Prete C, Martin Y, Rivero R, Önen M, Schiavo F, Rumín F, Mouratidis H, Yelmo J, Koukovini M (2020) Protecting citizens' personal data and privacy: joint effort from GDPR EU cluster research projects. SN Comput Sci 1:Article 217. https://doi.org/10.1007/s42979-020-00218-8
8. Deng M, Wuyts K, Scandariato R, Preneel B, Joosen W (2011) A privacy threat analysis framework: supporting the elicitation and fulfilment of privacy requirements. Requir Eng 16(1):3–32. https://doi.org/10.1007/s00766010-0115-7
9. Diker Vanberg A (2020) Informational privacy post GDPR—end of the road or the start of a long journey? Int J Hum Rights 25(1):52–78. https://doi.org/10.1080/13642987.2020.1789109
10. Domingo-Ferrer J, Farrás J, Ribes-González J, Sánche D (2019) Privacy-preserving cloud computing on sensitive data: a survey of methods, products and challenges. Comput Commun 140–141:38–60. https://doi.org/10.1016/j.comcom.2019.04.011
11. EU (2016) Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016. Official Journal of the European Union. L127 https://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
12. Fernandes DAB, Soares LFB, Gomes JV, Freire MM, Inácio PRM (2014) Security issues in cloud environments: a survey. Int J Inf Secur 13:113–170. https://doi.org/10.1007/s10207-013-0208-7
13. Försäkringskassan (2019) Vitbok - Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt (dnr 013428–2019)
14. Georgiou D, Lambrinoudakis C (2020) Compatibility of a security policy for a cloud-based healthcare system with the EU General Data Protection Regulation (GDPR). Information 11:Article 586. https://doi.org/10.3390/info11120586
15. Gleeson N, Walden I (2016) Placing the state in the cloud: issues of data governance and public procurement. Comput Law Secur Rev 32(5):683–695. https://doi.org/10.1016/j.clsr.2016.07.004
16. Islam MS, Karlsson F (2022) The public sector cloud service. Procurement in Sweden: an exploratory study of use and information security challenges. Int J Public Adm Digit Age 8(1):66. https://doi.org/10.4018/IJPADA.302906
17. It-driftsutredningen (2021) Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering. Delbetänkande (SOU 2021:1). Stockholm: Regeringen https://www.riksdagen.se/sv/dokument-lagar/dokument/statens-offentligautredningar/saker-och-kostnadseffektiv-it-drift_ZZB31
18. Jaatun M, Pearson S, Gittler F, Leenes R, Niezen M (2020) Enhancing accountability in the cloud. Int J Inf Manag 53:Article 101498. https://doi.org/10.1016/j.ijinfomgt.2016.03.004
19. Jaeger L, Eckhard A, Kroenung J (2021) The role of deterrability for the effect of multi-level sanctions on information security policy compliance: results of a multigroup analysis. Inf Manag 58(3):Article 103318. https://doi.org/10.1016/j.im.2020.103318
20. Li H, Yu L, He W (2019) The impact of GDPR on global technology development. J Glob Inf Technol Manag 22(1):1–6. https://doi.org/10.1080/1097198X.2019.1569186
21. Li Y, Al-Sulaiti K, Dongling W, Al-Sulaiti I (2022) Tax avoidance culture and employees' behavior affect sustainable business performance: the moderating role of corporate social responsibility. Front Environ Sci. https://doi.org/10.3389/fenvs.2022.964410
22. Mell P, Grance T (2011) The NIST definition of cloud computing. NIST National Institute of Standards and Technology. U.S Department of Commerce. Special Publication 800-145. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
23. Moerel EML, Timmers P (2021) Reflections on digital sovereignty. EU Cyber Direct, Research in Focus series 2021, Available at SSRN: https://ssrn.com/abstract=3772777

24. Näringsdepartementet (2017) För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi. Regeringskansliet (Dnr N2017/03643/D). https://www.regeringen.se/49adea/contentassets/5429e024be6847fc907b786ab954228f/digitaliseringsstrategin_slutlig_170518-2.pdf
25. Oates BJ (2006) Researching information systems and computing. Sage, London
26. Reisinger T, Wagner I, Boiten EA (2022) Security and privacy in unified communication. ACM Comput Surv 55(3):1–35. https://doi.org/10.1145/3498335
27. Robles-Gonzales A, Parra-Arnau J, Forné J (2020) A LINDDUN-based framework for privacy threat analysis on identification and authentication processes. Comput Secur 94:Article 101755. https://doi.org/10.1016/j.cose.2020.101755
28. Rodriguez-Doncel V, Santos C, Casanovas P, Gómez-Pérez A (2016) Legal aspects of linked data—the European framework. Comput Law Secur Rev 32(6):799–813. https://doi.org/10.1016/j.clsr.2016.07.005
29. Rotenberg M (2020) Schrems II, from Snowden to China: toward a new alignment on transatlantic data protection. Eur Law J 26:141–152. https://doi.org/10.1111/eulj.12370
30. Shastri S, Wassernan M, Chidambaram V (2021) How design and operation of modern cloud-scale systems conflict with GDPR. Commun ACM 64(2):66. https://doi.org/10.1145/3378061
31. Soria-Comas J, Domingo-Ferrer J (2016) Big data privacy: challenges to privacy principles and models. Data Sci Eng 1:21–28. https://doi.org/10.1007/s41019-015-0001-x
32. Tracol X (2020) "Schrems II": the return of the privacy shield. Comput Law Secur Review 39:Article 105484. https://doi.org/10.1016/j.clsr.2020.105484
33. Wuyts K, Scandariato R, Joosen W (2014) LIND(D)UN privacy threat tree catalog. Version 2.0—September 2014. Department of computer science, KU Leuven, Belgium. https://www.linddun.org/_files/ugd/cc602e_d7cf949767b7486d8bff0ecc05b91db6.pdf
34. Wuyts K, Joosen W (2015) LINDDUN privacy threat modelling: a tutorial. (Technical Report (CW Reports), V. CW685), Department of Computer Science, KU Leuven. https://www.linddun.org/_files/ugd/cc602e_f98d9a92e4804e6a9631104c02261e1f.pdf

Publisher's Note