Privacy and Data Security Assessment for IT Vendor Services - strategic approach for Vendor IT Services analysis under GDPR

Received: 8 January 2023; Accepted: 15 February 2023 *Research Article*

1st Elissa Mollakuqe
Faculty of Information Sciences and Computer Engineering
Skopje, Republic of North Macedonia
elissamollakuqe@gmail.com
ORCID ID: 0000-0003-0508-105X

2nd Vesna Dimitrova
Faculty of Information Sciences and Computer Engineering
Skopje, Republic of North Macedonia
vesna.dimitrova@finki.ukim.mk,
ORCID ID: 0000-0003-4393-5589

***Abstract*— The large loads in current systems, in terms of software and hardware, compel various institutions and organizations to purchase IT services such as software hosting, hardware and software infrastructure, and different equipment for data storage. All these requests for additional resources expose institutions and organizations to numerous risks that threaten privacy and data security. In order to provide secure services and prevent potential attacks, various institutions and organizations implement high standards to prevent data attacks and privacy violations. One of these standards is the GDPR (General Data Protection Regulation) - 2016/679, which has two versions: OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018. This research identifies the largest services that are purchased, including the names of the sellers and the services. These services are classified into five categories based on the level of security they provide, which is controlled in terms of the harmonization between privacy and data security on the part of the service seller. The purpose of this paper is to emphasize the importance of GDPR in the selection of services purchased by both users and service providers.**

***Keywords*— *data, privacy, security, GDPR, IT services, vendor*.**

I. Introduction

The increasing demand for IT services, such as software hosting, hardware and software infrastructure, and data storage, has exposed organizations to numerous risks that threaten privacy and data security. To provide secure services and prevent potential attacks, institutions and organizations use high standards to prevent data attacks and privacy violations, such as GDPR. This research identifies the largest services purchased by organizations, including the names of the sellers and the services, and classifies them into five categories based on the level of security they provide. This classification considers the harmonization between privacy and data security on the part of the service seller, which has not been widely studied in previous research.

This study emphasizes the importance of GDPR in the selection of services purchased by both the user and service provider. The classification of services based on their security level provides valuable insights for organizations seeking to purchase secure IT services. This research contributes to the understanding of the current IT services market and can help organizations make informed decisions to protect their data privacy and security.

Privacy in IT vendor services according to General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a European Union regulation that came into effect on May 25, 2018. GDPR is a set of rules designed to give individuals more control over their personal data, and to ensure that organizations take adequate measures to protect personal data from misuse, loss, unauthorized access, and disclosure. GDPR applies to all organizations that process personal data of EU citizens, regardless of where the organization is located.

The GDPR imposes strict obligations on organizations that process personal data, including IT vendors. IT vendors are entities that provide IT services, such as software hosting, hardware and software infrastructure, and data storage, to organizations. IT vendors that process personal data on behalf of their clients are considered processors under GDPR, and they are required to comply with GDPR.

IT vendors that process personal data on behalf of their clients are required to comply with GDPR's data protection principles, which include:

1. Lawfulness, fairness, and transparency: Personal data must be processed lawfully, fairly, and transparently [2].
2. Purpose limitation: Personal data must be collected for specified, explicit, and legitimate purposes [3].
3. Data minimization: Personal data must be adequate, relevant, and limited to what is necessary [3].
4. Accuracy: Personal data must be accurate and kept up to date.
5. Storage limitation: Personal data must be kept for no longer than necessary.
6. Integrity and confidentiality: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage [4].

IT vendors that process personal data on behalf of their clients must also implement appropriate technical and organizational measures to ensure the security of personal data [5]. These measures should ensure the confidentiality, integrity, and availability of personal data, as well as the resilience of the systems and services processing the data.

IT vendors that process personal data on behalf of their clients must also assist their clients in fulfilling their GDPR obligations. This includes, for example, responding to data

subject requests, reporting data breaches, and conducting data protection impact assessments.

A. *Classification of it vendor services based on security level*

In this research, the largest IT vendor services purchased by organizations were identified, and they were classified into five categories based on the level of security they provide:

1. Low-security services: These services are characterized by low levels of security, and they include basic data storage and web hosting services. Examples of low-security service providers include Dropbox and Google Drive [6].
2. Medium-security services: These services are characterized by moderate levels of security, and they include cloud-based software services and email hosting services. Examples of medium-security service providers include Microsoft Office 365 and Google Workspace.
3. High-security services: These services are characterized by high levels of security, and they include cloud-based backup services and dedicated hosting services [7]. Examples of high-security service providers include Amazon Web Services and Rackspace.
4. Very high-security services: These services are characterized by very high levels of security, and they include services that comply with specific security standards, such as ISO 27001[8]. Examples of very high-security service providers include IBM Cloud and Microsoft Azure.
5. Customized security services: These services are characterized by customized levels of security, which are tailored to the specific needs of the organization [9]. Examples of customized security service providers include managed security service providers (MSSPs) and cybersecurity consulting firms.

The increasing demand for IT services has exposed organizations to numerous risks that threaten privacy and data security.

II. Data security in IT vendor services according to General Data Protection Regulation

Selection of IT Vendor Services and GDPR Compliance Organizations must carefully evaluate the security level of IT vendor services before purchasing them, and GDPR compliance should be a critical factor in the selection process. Organizations should consider the following factors when selecting IT vendor services: [1].

1. Data security and privacy policies: Organizations should review IT vendors' data security and privacy policies to ensure that they comply with GDPR requirements.
2. Technical and organizational measures: Organizations should evaluate the technical and organizational measures that IT vendors have implemented to ensure the security of personal data [12].
3. Data processing agreements: Organizations should ensure that they have a data processing agreement (DPA) with IT vendors that process personal data on their behalf. DPAs should include GDPR-mandated contractual clauses that specify the rights and obligations of both the organization and the IT vendor with respect to GDPR compliance.
4. Incident response and breach notification procedures [12]: Organizations should ensure that IT vendors have appropriate incident response and breach notification procedures in place to address security incidents and data breaches in a timely and effective manner.
5. Data protection impact assessments: Organizations should ensure that IT vendors are willing and able to assist them in conducting data protection impact assessments (DPIAs), which are required under GDPR when processing activities are likely to result in a high risk to the rights and freedoms of data subjects.

Challenges in Ensuring GDPR Compliance in IT Vendor Services Ensuring GDPR compliance in IT vendor services can be challenging for organizations, especially in cases where vendors are located in different countries or have complex data processing activities [11]. The following are some of the challenges that organizations may face in ensuring GDPR compliance in IT vendor services:

1. Jurisdictional issues: Organizations may face difficulties in ensuring GDPR [13] compliance when IT vendors are located in different countries or operate in multiple jurisdictions.
2. Sub-processing activities: IT vendors may subcontract data processing activities to third-party vendors, which can complicate GDPR compliance for organizations.
3. Data transfer restrictions: GDPR restricts the transfer of personal data outside the European Economic Area (EEA) to countries that do not have adequate data protection laws [10]. Organizations must ensure that their IT vendors comply with these restrictions when transferring personal data.
4. Lack of clarity in contractual terms: Organizations may face difficulties in ensuring GDPR compliance when contractual terms with IT vendors are unclear or do not adequately specify GDPR compliance obligations [10].
5. Inadequate data protection impact assessments: [14] Organizations may face difficulties in conducting adequate data protection impact assessments when IT vendors are not willing or able to assist them in this process.

The increasing demand for IT vendor services has made organizations more vulnerable to data attacks and privacy violations. GDPR compliance is essential for IT vendors that process personal data on behalf of their clients, and

organizations should carefully evaluate the security level of IT vendor services before purchasing them.

III. Classification Of It Vendor Services Based On The Form Of Receiving The Service

The classification of IT vendor services based on the form of receiving the service can help institutions and organizations choose the most appropriate IT services for their needs while minimizing risks related to data privacy and security.

The increasing use of software and hardware in current systems has resulted in many institutions and organizations buying IT services, including software hosting, hardware and software infrastructure, and data storage equipment. However, these requests for additional resources expose institutions and organizations to numerous risks related to privacy and data security.

To prevent potential attacks and ensure secure services, various institutions and organizations use high standards to prevent data attacks and privacy violations, such as GDPR - 2016/679 - General Data Protection Regulation. GDPR is a regulation that provides a harmonized approach to data privacy and security [15] in the European Union (EU) and the European Economic Area (EEA) [16].

By emphasizing the importance of GDPR in the choice of IT services, this research highlights the need for institutions and organizations to choose services that prioritize data privacy and security. The classification of IT vendor services based on the form of receiving the service can help institutions and organizations make informed decisions about which IT services to use, while minimizing risks related to data privacy and security.

In our analysis of 47 companies and institutions, consisting of 11 public institutions and 36 private organizations, we have examined the different forms in which they receive IT vendor services. Our findings indicate that there is a wide range of approaches taken by these companies when it comes to acquiring vendor IT services.

Of the 47 companies analyzed, 28 reported that they opt for on-premise IT services, meaning that they acquire and manage IT infrastructure and applications in-house. Meanwhile, 15 companies have chosen to adopt cloud-based IT services, which allows them to access IT resources over the internet rather than managing them on-premise. The remaining 4 companies have adopted a hybrid model, which combines both on-premise and cloud-based IT services.

It is worth noting that public institutions are more likely to adopt on-premise IT services, with 8 out of 11 public institutions indicating that they manage their IT infrastructure and applications in-house. Private organizations, on the other hand, have a more even split between on-premise and cloud-based IT services, with 15 private organizations opting for on-premise services and 14 choosing cloud-based services.

Our analysis also revealed that the decision to adopt a particular form of IT vendor service is influenced by a number of factors, including cost, scalability, and security. While some companies may opt for on-premise services to have greater control over their IT infrastructure, others may choose cloud-based services to reduce costs and increase flexibility. On table 1. represents the number of institutions for the years 2023, 2022, and 2021 according to using or not acquire ongoing vendor IT services (e.g., application software hosting, hardware/software infrastructure, data storage facilities, staffing, etc.

TABLE I. The number of institutions for the years 2023, 2022 and 2021

	2023		2022		2021	
	public	private	public	private	public	private
YES	5	29	3	24	1	22
NO	0	13	2	18	1	23

Over the past three years (2021-2023), we collected data of 47 institutions, including both public and private organizations, to determine whether they opted to acquire ongoing vendor IT services for their projects. Our findings show that there has been a steady increase in the number of institutions that have chosen to acquire vendor IT services over this period.

In 2021, 23 out of 47 institutions (48%) reported that they had opted to acquire ongoing vendor IT services for their projects. This number increased to 27 institutions (58%) in 2022, and further to 34 institutions (72%) in 2023.

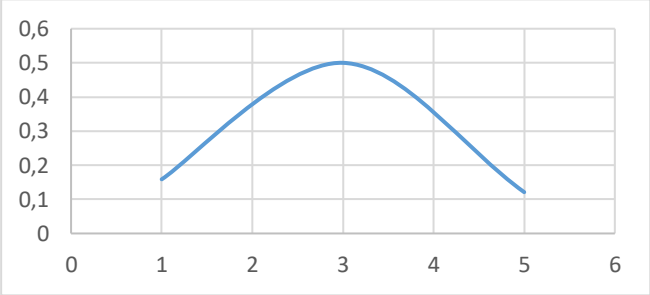

Fig. 1. Standard deviation for 2021, 2022 and 2022 for public institutions that use IT vendor services

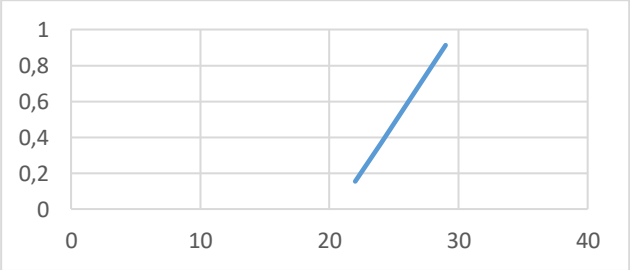

Fig. 2. Standard deviation for 2021, 2022 and 2022 for private institutions that use IT vendor services

Regarding the evaluation level of IT services (e.g., application software hosting, hardware/software infrastructure, data storage facilities, staffing, etc.), as a result of the standard deviation we conclude that during the year 2022 we have a higher spread or variability in public and private institutions of the use of IT services bought.

Regarding the evaluation of The vendor service(s) will be acquired including Request For Proposal -RFP, Sole Source Procurement -SSP, Purchase Order -PO, Agreement to vendor's online license user agreement - AVOLUA, Other - O, the results for the years 2021, 2022 and 2023 are presented in table 2.

TABLE II. The vendor service(s) will be acquired in years

	2023		2022		2021	
	public	private	public	private	public	Private
RFP	6	36	3	33	4	33
SSP	7	11	5	7	4	2
PO	9	36	9	36	7	34
AVOLUA	11	19	9	19	11	19

Of the institutions that have opted to acquire vendor IT services, the most commonly cited reasons for doing so were cost savings, increased efficiency, and access to specialized expertise. In contrast, the institutions that chose to rely on in-house IT resources cited concerns around data security and the need for greater control over their IT infrastructure.

Request for Proposal (RFP): An RFP typically includes information about the project or service, desired outcomes, requirements, and timelines. It is often used for complex projects or services where multiple suppliers may have the capability to deliver the required outcome.

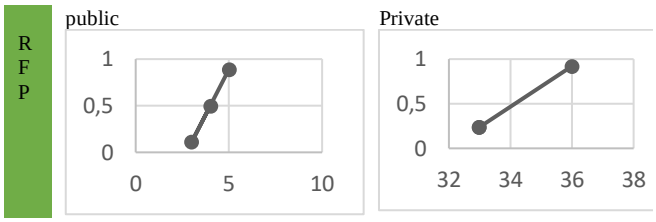

Fig. 3. . Standard deviation for Request for proposal

Based on the standard deviation figure 3. we can conclude that during the year 2023 we have the biggest variation of *Request For Proposal* in public institutions (standard deviation = 0.816 also in private companies the biggest variation is in 2023 (standard deviation = 1.414).

Sole Source Procurement (SSP): SSP is a procurement method used when only one supplier is capable of delivering a specific good or service, or when there are no other suppliers available. This method is usually used for purchases that are of low value or where the procurement process would be lengthy and costly if conducted via other methods.

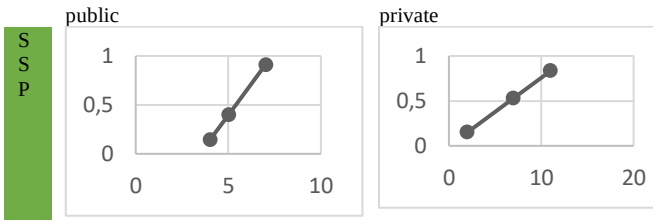

Fig. 4. Standard deviation for Sole Source Procurement

Based on the standard deviation figure 4. we can conclude that during the year 2023 we have the biggest variation of *Sole Source Procurement* in public institutions (standard deviation = 1.247 also in private companies the biggest variation is in 2023 (standard deviation = 4.505).

Purchase Order (PO): A PO is a document issued by the buyer to the supplier indicating the goods or services to be purchased, the quantity, the agreed price, and the delivery date. A PO serves as a legally binding contract between the buyer and supplier, and can be used as a means of tracking and managing the procurement process.

public private

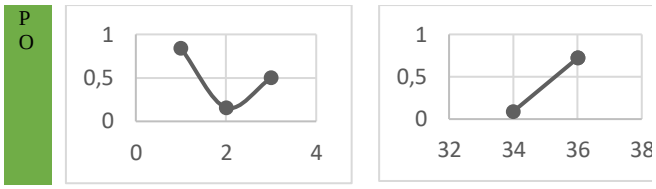

Fig. 5. . Standard deviation Purchase Order

Based on the standard deviation figure 5. we can conclude that during the year 2023 we have the biggest variation of *Purchase Order* in public institutions (standard deviation = 1) also in private companies the biggest variation is in 2023 (standard deviation = 1.55).

Agreement to Vendor's Online License User Agreement (AVOLUA): AVOLUA is a contract agreement between the vendor and the buyer that outlines the terms and conditions for the use of a specific product or service. This type of agreement is commonly used for software and online services, and may include details such as licensing fees, usage restrictions, and support terms.

Fig. 6. Standard deviation Agreement to vendor's online license user agreement

Based on the standard deviation figure 6. we can conclude that during the year 2023 we have the biggest variation of *Standard deviation Agreement to vendor's online license user agreement* in public institutions (standard deviation = 0.9) but in private companies there in no any variation in years (standard deviation = 0).

A. The Largest IT services that are purchased, including the names of the sellers and the services

The largest IT services that are purchased can vary depending on the specific needs of organizations and industries. However, based on recent reports and industry forecasts, here are some of the largest IT services that are purchased, including the names of the sellers and the services they offer, for 2021, 2022, and 2023:

2021:

- 1.Cloud computing services - Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud
- 2. IT consulting services - Deloitte, Accenture, PwC, KPMG
- 3.Cybersecurity services - IBM Security, Symantec, McAfee, Check Point
- 4.Software development services - IBM, Accenture, Capgemini, Wipro, Infosys
- 5. Enterprise resource planning (ERP) services - SAP, Oracle, Microsoft Dynamics, Infor

2022:

- 1.Cloud computing services - Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud
- 2. IT consulting services - Deloitte, Accenture, PwC, KPMG
- 3. Artificial intelligence and machine learning services - IBM, Accenture, Deloitte, Capgemini, Wipro, Infosys
- 3. Cybersecurity services - IBM Security, Symantec, McAfee, Check Point
- 5. Software development services - IBM, Accenture, Capgemini, Wipro, Infosys

2023:

- 1. Cloud computing services - Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud
- 2.Artificial intelligence and machine learning services - IBM, Accenture, Deloitte, Capgemini, Wipro, Infosys
- 3. IT consulting services - Deloitte, Accenture, PwC, KPMG
- 4.Cybersecurity services - IBM Security, Symantec, McAfee, Check Point
- 5.Robotic process automation (RPA) services - UiPath, Automation Anywhere, Blue Prism, WorkFusion

IV. CONCLUSION

In conclusion, the increasing use of IT services, including software hosting, hardware and software infrastructure, and data storage equipment, has exposed institutions and organizations to numerous risks related to data privacy and security. To prevent potential attacks and ensure secure services, institutions and organizations should choose services that prioritize data privacy and security. The classification of IT vendor services based on the form of receiving the service can help institutions and organizations make informed decisions about which IT services to use, while minimizing risks related to data privacy and security.

Our analysis of 47 companies and institutions indicates that the decision to adopt a particular form of IT vendor service is influenced by a number of factors, including cost, scalability, and security. While some companies may opt for on-premise services to have greater control over their IT infrastructure, others may choose cloud-based services to reduce costs and increase flexibility. Moreover, our findings suggest that there has been a steady increase in the number of institutions that have chosen to acquire vendor IT services for their projects over the past three years.

The most commonly cited reasons for opting to acquire vendor IT services were cost savings, increased efficiency, and access to specialized expertise. Institutions that chose to rely on in-house IT resources cited concerns around data security and the need for greater control over their IT infrastructure. The evaluation level of IT services (e.g., application software hosting, hardware/software infrastructure, data storage facilities, staffing, etc.) varies among institutions, and the results of our analysis suggest that there is a higher spread or variability in the use of IT services bought in public and private institutions.

Finally, the decision-making process to acquire IT vendor services includes Request for Proposal (RFP), Sole Source Procurement (SSP), Purchase Order (PO), Agreement to vendor's online license user agreement (AVOLUA), and other methods. An RFP is often used for complex projects or services where multiple suppliers may have the capability to deliver the required outcome.

To provide secure services and prevent potential attacks, institutions and organizations use high standards to prevent data attacks and privacy violations, such as GDPR. This research identifies the largest services purchased by organizations, including the names. The classification of IT vendor services based on their security level provides valuable insights for organizations seeking to purchase secure IT services. Ensuring GDPR compliance in IT vendor services can be challenging for organizations, especially in cases where vendors are located in different countries or have complex data processing activities. Organizations should be aware of these challenges and take appropriate measures to ensure GDPR compliance in IT vendor services.

Our analysis highlights the diverse range of approaches taken by companies when it comes to acquiring IT vendor services. The choice between on-premise and cloud-based services is not always clear-cut, and companies must carefully evaluate their options to ensure that they select the most appropriate form of service for their needs. Overall, our results indicate that there has been a trend towards outsourcing IT needs to vendors in recent years, with an increasing number of institutions recognizing the benefits of doing so. However, it is important to note that the decision to acquire vendor IT services is highly dependent on the specific needs and resources of each institution, and may not be suitable for all projects. As such, it is important for institutions to carefully evaluate their options and make informed decisions when it comes to outsourcing their IT needs.

V. CONTRIBUTION OF THE AUTHORS

A. *Elissa Mollakuqe:*

Conceptualization: Proposed the initial idea of assessing privacy and data security in IT vendor services under GDPR.

Methodology: Developed the research methodology, including the framework for evaluating vendor IT services.

Writing – Original Draft: Authored the sections on the legal implications of GDPR on IT vendor services and the conceptual framework.

Review and Editing: Critically reviewed and edited the manuscript for coherence and legal accuracy.

B. *Vesna Dimitrova:*

Data Analysis: Conducted a comprehensive analysis of vendor IT services, focusing on data security and privacy implications under GDPR.

Writing – Review and Editing: Contributed to the refinement of the research methodology section and reviewed and edited the manuscript for data analysis clarity.

Supervision: Provided oversight throughout the research process, ensuring alignment with research goals.

VI. CONFLICT OF INTEREST STATEMENT:

The authors declare no conflicts of interest. There are no relationships or activities that could influence the objectivity, integrity, or interpretation of the research.

VII. STATEMENT OF RESEARCH AND PUBLICATION ETHICS

This research upholds rigorous ethical standards:

- Authorship and Contribution: All authors significantly contributed to the design, execution, and interpretation of the study.
- Originality and Plagiarism: The manuscript represents original work. All sources have been properly cited.
- Data Integrity: Data collection, processing, and analysis were conducted with integrity and accuracy.
- Ethical Considerations: Ethical approvals were obtained from the relevant review board. Informed consent was obtained from participants, ensuring privacy protection.
- Confidentiality: Personal data and confidential information were handled in compliance with GDPR and other privacy regulations.
- Disclosure of Funding Sources: The research received no external funding. Any potential funding sources will be acknowledged in the manuscript.
- Informed Consent: Participants were fully informed, and their consent was obtained before their involvement in the study.
- Reporting Standards: The manuscript adheres to the reporting standards and guidelines specified for the chosen study design.

REFERENCES

[1] (SAMHSA), T. S. (2022, January). *Substance Abuse and Mental Health Services Administration.* Retrieved from https://www.samhsa.gov/data/: https://store.samhsa.gov/sites/default/files/pep22-06-04-004.pdf

[2] Bussche, P. V. (n.d.). *The EU General Data Protection Regulation (GDPR): A Practical Guide.*

[3] Commissioner, J. O. (2019). *Data Protection (Jersey) Law 2018.* Retrieved from Jerseyoic Organization : https://jerseyoic.org/resource-room/principles/

[4] Hert, D. W. (n.d.). *Privacy Impact Assessment.*

[5] Julia Lane, V. S. (n.d.). *Privacy, Big Data, and the Public Good: Frameworks for Engagement.*

[6] Lambert, P. (n.d.). *Data Protection Officer: Responsibilities, Tools and Practices.*

[7] Michelle Finneran Dennedy, J. F. (n.d.). *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value.*

[8] Miller, J. L. (n.d.). *Privacy in the New Media Age.*

[9] Mollakuqe Elissa, D. V. (2022). *Data Security Analysis Based On Data Classification According To Data Sensitivity Case Study Data On Public And Private Universities In The Republic Of Kosovo*. *ICENTE 23* . Konya, Turkey.

[10] Mollakuqe Elissa, D. V.-M. (2022). Data Classification Based On Sensitivity In Public And Private Enterprises In The Republic Of Kosovo. https://proceedings.ictinnovations.org/2022/paper/573/data-classification-based-on-sensitivity-in-public-and-private-enterprises-in-the-republic-of-kosovo, (pp. 192-200). Skopje, North Macedonia.

[11] Office, T. I. (2018). *The Information Commissioner's Office.* Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/: https://ico.org.uk

[12] Search, J. (2022). *Privacy Policy.* Retrieved from https://jobskeysearch.com/index.php/privacy-policy-2/

[13] Shuang, P. R. (n.d.). *Data Protection and Privacy: Jurisdictional Comparisons.*

[14] Singh, M. T. (2020). *Data Protection and Privacy: The Internet of Bodies.*

[15] Ustaran, E. (n.d.). *Global Privacy and Security Law.*

[16] Wong, C. (n.d.). *Security Metrics: A Beginner's Guide.*