CLARK UNIVERSITY

CHALLENGE CONVENTION.
CHANGE OUR WORLD.

School of Professional Studies

Project Charter
General Data Protection Regulation (GDPR) (EU) 2016/679 Project

Client: Clark University ITS Department

Capstone Advisor: Richard Aroian, M.B.A.
(Executive Director of Corporate Outreach and Micro-Credential Strategy)

Client Representative: Alexander Magid, M.A.
(Information & Compliance Analyst)

Presented by

Dannana Harish
Sayan Banerjee

TABLE OF CONTENTS

1.INTRODUCTION

The General Data Protection Regulation (GDPR) is recognized as the world's most comprehensive set of data protection regulations, which enhance people's access to their information and limit what organizations can do with it. 66% percent of the global population has access to the internet. Even though being associated with the world's largest database brings tremendous benefits, it also entails a certain amount of cost. According to subsequent measurements, approximately 63% of online data subjects are now more concerned about their online security. Further statistics included that there's a programmer assault every 39 seconds.

As a result of the increasing cybercrime rate, the European Parliament and the Chamber of the European Union have drafted a Common Information Security Directive GDPR that guarantees information security and social media security to all citizens of the European Financial Region (EEA) and the European Union (EU) as well as the European Union (EU).

Compared to EU directives, GDPR gives individuals complete control over their personal information and centralizes the administrative environment. This information is essential for organizations that handle the data of European Union citizens and residents. Any company forming and storing data about EU citizens in EU states must comply with the GDPR even if they do not have a trade presence within the region. To demonstrate to regulators that organizations are taking their GDPR obligations seriously, they should clearly understand all their systems, how information is processed, and what steps they have taken to reduce errors.

Furthermore, organizations should also have a legal beginning for preparing individual customer data with the GDPR and social media arrangements in place. It is crucial for businesses to comply with data subject’s requests to delete their information and ensure unambiguous and open consent with the option to withdraw. This commitment to transparency and trust-building is a key aspect of GDPR.GDPR makes it more difficult for trade websites to rely heavily on social media to screen client data and behavior for computerized profiling. Most social

media platforms now use these forms (privacy policies or data collection forms), but GDPR requires more detailed information on collected and shared data types.[1]

1.1 .OVERVIEW

This project focuses on ensuring Clark University websites and data processing practices are compliant with the General Data Protection Regulation (GDPR). This Project involves auditing and identifying areas of non-compliance by reviewing each of the Information Technology policies to see that they are aligning practices with GDPR requirements.

This Capstone project also examines other data protection laws, such as China's PIPL (Personal Information Protection Law) and India's (Digital Personal Data Protection) DPDP Bill, to ensure alignment with multiple regulatory requirements. The ultimate goal is to defend people's privacy rights by improving data protection procedures and upholding compliance with applicable GDPR data privacy regulations in Institutions of Higher Education.

1.2 .OBJECTIVE

The project's primary objective is to identify areas of non-compliance with GDPR regarding privacy policies, data collection notices, and GDPR requirements applicable to Clark University's website. Additionally, the project aims to examine other data protection laws, such as China's (Personal Information Protection Law) PIPL and India's (Digital Personal Data Protection) DPDP Bill, to determine if compliance with one aspect of General Data Protection Regulation (GDPR) ensures compliance with these laws.

This Capstone project will serve as a tool for identification of current data protection procedures and recommendations to make those non-compliant, more compliant with various regulations. The ultimate objective of this Capstone Project is to improve Data protection procedures and uphold compliance with applicable data privacy legislation.

[1] Wolford, B. (2023, September 14). What is GDPR, the EU's new data protection law? GDPR.eu. https://gdpr.eu/what-is-gdpr/

2.BACKGROUND

The General Data Protection Regulation (GDPR) law came into action on May 25, 2018, in the European Union (EU), and the European Economic Area (EEA) passed by the European Parliament, the Council of the European Union, and the European Commission. It addresses the export of personal data outside these territories and attempts to improve privacy and data protection for individuals within the EU and EEA.[2]

2.1.Relevance to Institutions of Higher Education:

It is important to note that complying with GDPR is a legal requirement and a crucial aspect of protecting individuals' privacy rights for universities to ensure the privacy and data protection of EU/EEA residents, including students, faculty, and staff. It emphasizes the significant role universities play in safeguarding personal data.

2.2.Impact of GDPR on Institutions of Higher Education:

GDPR significantly impacts Institutions of Higher Education, requiring them to implement robust data protection measures and practices. Some critical aspects of GDPR compliance for universities include:

- **Data Protection Principles:** Institutions of Higher Education must comply with GDPR's data protection principles, including lawful, fair, and transparent processing of personal data and ensuring data integrity and confidentiality.
- **Data Breach Notification:** Institutions of Higher Education must notify the supervisory authority and the affected individuals regarding any data breach that threatens individuals' rights and freedoms.
- **International Data Transfers:** GDPR restricts the transfer of personal data outside the EU/EEA to countries that do not provide adequate data protection unless certain safeguards are in place.
- **Data Protection Impact Assessments (DPIAs):** Institutions of Higher Education are required to perform DPIAs for high-risk data processing operations to evaluate and reduce privacy concerns.

[2] Wolford, B. (2023, September 14). What is GDPR, the EU's new data protection law? GDPR.eu. https://gdpr.eu/what-is-gdpr/

- **Data Protection Officer (DPO):** Institutions of Higher Education may be required to appoint a DPO to oversee GDPR compliance and act as a point of contact for data protection authorities and data subjects. [3]

2.3.Other Data Protection Laws

China's Personal Information Protection Law (PIPL) and India's Digital Personal Data Protection (DPDP) Bill aim to regulate the processing of personal data within their respective jurisdictions. These laws share similarities with GDPR regarding enhancing individuals' rights and imposing obligations on organizations handling personal data.

2.3.1.China's Personal Information Protection Law (PIPL):

PIPL went into effect on November 1, 2021, and applies to the processing of personal information of individuals within China. Organizations must obtain consent for data processing, adhere to data minimization, and purpose limitation principles, and implement data security measures. PIPL also imposes restrictions on cross-border data transfers, requiring organizations to conduct security assessments or obtain approval. [4]

2.3.2.India's Digital Personal Data Protection (DPDP) Bill:

The DPDP Bill aims to regulate individuals' personal data processing in India. It introduces data principals as individuals whose data has been processed and establishes a Data Protection Authority of India to oversee compliance with the law. [5]

Both PIPL and the DPDP Bill reflect a global trend towards stricter data protection regulations, similar to GDPR, to safeguard individuals' privacy rights and ensure responsible handling of personal data.[6]

[3] (How Universities Have to Adapt Under the New EU General Data Protection Regulation (GDPR) | Full Fabric, n.d.)
[4] (Personal Information Protection Law of the People's Republic of China - PIPL, 2022)
[5] (What Is India's Digital Personal Data Protection (DPDP) Act? Rights, Responsibilities & Everything You Need to Know, n.d.)
[6] Briefing, C. (2022, July 21). PIPL vs GDPR - Key Differences and Implications for Compliance in China

2.3.3.Family Educational Rights and Privacy Act (FERPA) :

The Family Educational Rights and Privacy Act (FERPA) is a federal law that safeguards students' privacy in education records. It also grants students the right to access and review their records and sets up procedures for correcting faulty or misleading data through informal and formal hearings. Introduced in 1974 by Senator James Buckley of New York, FERPA was initially part of the General Education Provisions Act. It was called the Protections of the Rights and Privacy of Students and Parents. It is also commonly known as the Buckley Amendment. [7]

3.METHODOLOGY

3.1.Analyzing Clark University Policies

The methodology for this project involved a comprehensive analysis of Clark University's existing policies and procedures related to data privacy and security. This analysis stems from a detailed examination of the Clark University's current practices regarding data collection, storage, processing, and sharing, and focuses on aligning these practices with the requirements of the General Data Protection Regulation (GDPR).

The analysis will be conducted through a combination of manual review and comparison with GDPR requirements. This will involve reviewing relevant documentation, such as privacy policies, data protection agreements, and internal guidelines, to assess their compliance with GDPR principles.

3.2.Approach

Literature Review: To better understand the current status of GDPR compliance at Clark University and identify common issues and best practices, we have conducted extensive literature research.

Policy Analysis: Evaluate Clark University's current information security and data privacy policies, with a focus on data collection, processing, and dissemination.

[7] (FERPA, n.d.)

Recommendations: Developing recommendations for improving Clark University's data security and privacy practices. Based on the comparison and analysis of Clark University's data security and privacy practices with India's Digital Personal Data Protection Bill(DPDP), China's Personal Information Protection Law (PIPL) and The Family Educational Rights and Privacy Act (FERPA), recommendations include enhancing data collection transparency, implementing strict data transfer agreements, establishing clear procedures for data access requests, improving consent management practices, enhancing incident response procedures, and conducting regular reviews of privacy notices to ensure compliance with relevant regulations.

3.3.Expected Outcomes

- Identify and review any areas of non-compliance on the policies with the General Data Protection Regulation (GDPR) and other applicable data protection laws.
- Provide recommendations for improving Clark University's data privacy and security practices.
- Provide insights into industry best practices for GDPR compliance in institutions of higher education and guidance on implementing GDPR compliance.

3.4.GDPR Articles That Are Relevant To Higher Education Privacy Practices And Alignment With Strict Compliance.

3.4.1 **Article 5 - Principles relating to the processing of personal data**: This article summarizes the principles for processing personal data, including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality. [8]

3.4.2 **Article 6 - Lawfulness of processing**: This article specifies the conditions under which processing of personal data is lawful, including consent, contract performance, legal obligations, vital interests, public interest, and legitimate interests.

3.4.3 **Article 9 - Processing of special categories of personal data**: According to Article 9 - the processing of special categories of personal data, such as data revealing racial or ethnic origin, political opinions,

[8] (Chapter 2 – Principles - General Data Protection Regulation (GDPR), 2018)

religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3.4.4 **Article 12 - Transparent information, communication, and modalities for the exercise of the rights of the data subject**: This article specifies the information that should be provided to data subjects regarding the processing of their personal data and their rights under the GDPR.

3.4.5 **Article 15 - Right of access by the data subject**: This article grants data subjects the right to obtain confirmation from the data controller as to whether or not personal data concerning them is being processed, and, where that is the case, access to that personal data.

3.4.6 **Article 17 - Right to erasure ("right to be forgotten")**: This article grants data subjects the right to have their personal data erased by the data controller under certain conditions.

3.4.7 **Article 25 - Data protection by design and by default**: This article requires data controllers to implement appropriate technical and organizational measures to ensure that, by default, only personal data necessary for each specific purpose of the processing are processed.

3.4.8 **Article 30 - Records of processing activities**: This article requires data controllers and processors to maintain records of processing activities under their responsibility.

3.4.9 **Article 32 - Security of processing**: This article requires data controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

3.4.10 **Article 37** – Article 37 of the General Data Protection Regulation(GDPR) requires organizations to appoint a Data Protection Officer (DPO) in certain circumstances, such as when processing personal data on a large scale or when processing sensitive categories of data.

3.4.11 **Article 39 - Tasks of the data protection officer**: This article outlines the tasks of the data protection officer (DPO), including informing and advising the organization and its employees about their obligations under the GDPR, monitoring compliance with the GDPR, and cooperating with the supervisory authority.

4.DATA COLLECTION

4.1.List of Clark University Policies

4.1.1 Clark's Information Technology System Policy

Clark's Information Technology System Policy establishes guidelines or rules that define what is considered responsible and acceptable use of Clark University's Information Technology Systems (ITS) resources. These resources include computer systems, computer labs, applications, networks, software, electronic communications and information sources, web pages, and related services. This Policy complies with GDPR's data minimization and integrity principles by outlining acceptable use practices that help prevent unauthorized access or data breaches and Clark's Information Technology System Policy aligns with Articles 5 and 32, emphasizing data minimization and security measures**.** [9]

4.1.2 Change Management Policy

Change Management aims to ensure that consistent methods and procedures are followed in the production environment for any changes. This helps reduce any negative effects on services and customers and also ensures that these changes comply with audit requirements. This Policy adheres to GDPR's requirement for ensuring data security and integrity during changes. Articles 5 and 32 highlight the importance of ensuring data security and integrity throughout the processing of personal data.

4.1.3 Clark Account Policy

Clark Account Policy states that an individual with a Clark Account can be able to access computing resources across the University. It is used to access campus computers, the wireless network, your email, file shares, CUWeb, and many other services. Data Subjects Clark Account credentials secure their online identity, and the data subject is solemnly responsible for securing these credentials and the actions taken using their credentials. By securing online identities, the policy complies with GDPR's principles of data security and integrity. Therefore, Articles 5 and 32 emphasize that data security measures are met.

[9] (Policies and Standards | Information Technology Services | Clark University, 2023)

4.1.4 Data Classification Policy

The Clark data classification policy provides a framework for securing data from risks including, but not limited to, unauthorized destruction, modification, disclosure, access, use, and removal. This policy outlines the measures and responsibilities required for securing data resources. It establishes a framework for securing data from risks and classifying data accordingly. This policy complies with GDPR's requirements for data minimization and security measures. Therefore, it aligns with Articles 5 and 32, implementing data minimization and security measures.

4.1.5 Data Security Policy for All Faculty, Staff, and Student Employees

The Data Security Policy for All Faculty, Staff, and Student Employees outlines that no member of the Clark community is allowed to electronically store or maintain credit card or debit card numbers, expiration dates, and/or security codes in any way relating to Clark or Clark-sponsored activities. Information Technology Services (ITS) must approve the use of any system or application that electronically processes, stores, or transmits credit card data. Because of the string language surrounding prohibition of electronic storage or maintenance of certain sensitive information and by restricting the storage of sensitive data, the policy aligns with GDPR's principles of data minimization and security; Articles 5 and 32, emphasizing data minimization and security measures. Therefore this policy complies with GDPR requirements

4.1.6 Data Security Policy for Supervisors, Data Managers, and Data Custodians

The Employees at Clark University are given administrative responsibilities and roles that include handling confidential or restricted data and are responsible for ensuring compliance with Clark's data security policies as well as taking corrective measures when necessary. The Policy supports Articles 5 and 32, emphasizing data security measures and therefore the Policy complies with GDPR's data security and integrity requirements by enforcing data security policies.

4.1.7 Document Retention and Destruction Policy

The Document and Retention Policy adds to and supports Clark University’s Data Security Policies by outlining how the university handles the retention and removal of documents containing Confidential and

restricted data as discussed earlier in Data Classification Policies. Therefore, this policy complies with GDPR's Principle of keeping data to a minimum and ensuring security by specifying this procedure for keeping and destroying documents aligning with Articles 5 and 32, which highlights the importance of minimizing data and maintaining security.

4.1.8 Email Policy

The Email Policy includes a working spreadsheet that lists specific documents containing protected data and specifies the schedule for retaining and destroying each document type. This spreadsheet can be used as a resource for future Discovery/eDiscovery proceedings. This Policy ensures the proper Use of Clark University's email system by regulating email use. Therefore, this policy complies with GDPR's principles of data minimization and security and aligns with Articles 5 and 32, emphasizing data minimization and security measures.

4.1.9 File Sharing and Copyright Policy

The File Sharing and Copyright Policy described ensures that Clark University provides electronic resources to its faculty, staff, and students to support its educational, research, and service missions. This means that the policy includes guidelines on how to use electronic resources in a way such as not downloading or sharing copyrighted materials without permission. Therefore, by promoting responsible internet use, the policy helps to minimize the risk of data breaches and supports GDPR's principles of data minimization and security, aligning with Articles 5 and 32 of GDPR.

4.1.10 File Sharing and the Higher Education Opportunity Act

This File Sharing and the Higher Education Opportunity Act is responsible in decreasing the illegal sharing of copyrighted work such as copyrighted materials through peer-to-peer (P2P) networks which is often done by students. Institutions of Higher Education are responsible for taking steps to prevent illegal file sharing on their networks. Therefore, by reducing this illegal sharing, the policy aligns with GDPR's regulations on keeping data secure and intact, as well as supporting Articles 5 and 32, which emphasize security measures for data.

4.1.11 Maintaining Clark Web Sites Policy

Clark University Web Sites Policy refers to the guidelines and procedures established by Clark University for managing and updating the content on its official websites. This policy explains the roles and responsibilities of individuals in each academic department and administrative office who are assigned to maintaining the content on their respective websites. It aims to ensure that the content on Clark University's websites is accurate, up-to-date, and compliant with relevant laws and regulations, including data protection laws like GDPR. This policy requires every academic department and administrative office at Clark University to appoint someone to manage the content on their official website. This person is typically called the Web Content Manager (Web CM) and should be a staff member from within the department. By assigning this responsibility, the policy ensures that there is accountability for the content on the website. This aligns with GDPR's principles of accountability and data protection, as well as with Articles 5 and 32 making this compliant.

4.1.12 Password Policy

The Password Policy at Clark University explains the importance of strong passwords for computer and data security. Passwords are an important aspect of computer security. This policy highlights that weak passwords can lead to unauthorized access to university resources. The policy applies to all users, including employees, students, contractors, and vendors, who are responsible for choosing and protecting their passwords. By enforcing secure password practices in accordance with GDPR's principles of data security and integrity, as well as Articles 5 and 32, which highlights the importance of data security measures this policy is compliant with General Data Protection Regulation (GDPR) regulations.

4.1.13 Physical Access to Restricted IT Areas Policy

The Physical Access to Restricted IT Areas Policy states the rules for who can enter and how access is managed in Clark University's IT facilities. It says that everyone with access needs to keep these areas secure. The policy's goal is to create guidelines for allowing, controlling, monitoring, and removing access to IT facilities managed by Clark University. It applies to everyone using the university's information resources.

By following these rules, the policy helps make sure the university meets GDPR's rules for keeping data secure and intact, and supports Articles 5 and 32, which focus on data security making this complaint.

4.1.14 Privacy Policy

Clark University's privacy policy aims to provide an informative, useful, and engaging website for its visitors. It outlines how Clark uses and protects any information that visitors provide when using Clark-controlled and operated websites, as well as other information provided to Clark from time to time. The policy informs visitors about Clark's data protection practices and complies with GDPR's transparency and data protection principles, supporting Articles 5 and 12, which emphasize transparency and communication regarding data protection practices

4.1.15 Remote Access Policy

The Remote Access Policy at Clark University creates guidelines for accessing the university's computing resources remotely using Virtual Private Network (VPN) technology. VPNs are used to securely connect to the university's network over the internet, ensuring that data transmitted between the user and the university's network is encrypted and protected.

By requiring remote access to be done using VPN technology, the policy helps ensure the security and integrity of data. This is important for compliance with GDPR, which requires organizations to implement measures to protect the security and privacy of personal data. The policy aligns with GDPR's principles by emphasizing the importance of data security measures Articles 5 and 32 in remote access to computing resources.

4.1.16 Security Awareness Training and Testing Policy

The purpose of this policy is to specify the Clark University internal information security awareness and training program to inform and assess all faculty and staff regarding their information security obligations. This policy applies regardless of whether staff use computer systems and networks, since all staff are expected to protect all forms of information assets including computer data, written materials/paperwork, and intangible forms of information. This Policy informs and assesses faculty and staff regarding information

security obligations, complies with GDPR's accountability and data protection principles, and supports Articles 5 and 39, emphasizing accountability and information provision.

4.1.17 Security Extension to Appropriate Use Policy

The Security Extension to Appropriate Use Policy at Clark University makes sure that the University's network is safe and secure for research, instructional, and administrative purposes. This policy is applicable to all the members of the university whose device is connected to the network including devices such as desktop and laptop computers, servers, wireless devices, specialized equipment, cameras, and building and environmental controls.

This policy aims to provide a secure network environment by outlining guidelines for using connected devices. It complies with GDPR's principles of data security and integrity, as well as supporting Articles 5 and 32, which emphasize data security measures. This means that the policy is designed to protect the security and integrity of data transmitted and stored on the university's network.

4.1.18 Website Policy

The Website Policy at Clark University highlights the significance of the university's website as a primary communication and information tool. This digital platform serves as the university's public image, attracting prospective students and keeping alumni, friends, current students, faculty, staff, and the press informed about campus news and events.

The policy provides guidelines for creating and maintaining departmental web pages to ensure they reflect the values and mission, and providing accurate and engaging information about its programs, events, and activities. It adheres to GDPR's transparency and data protection principles, supporting Articles 5 and 12 and making it compliant.

4 ANALYSIS

Project Outcomes	Measure of Success
• Evaluations should be made to assess the level of compliance or potential data privacy risks as well as identify any potential gaps in compliance.	• Identify and document compliance gaps in the University's current level of compliance with GDPR regulations.
• Determine if the processes and privacy protocols currently in place, satisfy those needed to improve data protection.	• Confirm that the existing processes and privacy protocols in place meet the requirements needed for enhancing data protection.
• Identify compliance of data handling within the university network and with third parties.	• Identification and remediation of compliance gaps in data handling within the university network and with third parties.
• Explore other laws, such as PIPL, DPDP, and FERPA, and determine if there is any overlap with GDPR.	• Identification of overlaps of non- compliance between GDPR and other relevant data privacy laws, along with recommendations to address them.
• Review and assess Clark University policies for data collection, transfer, right to access, consent management, data breach notification, privacy notices, and data minimization to ensure compliance with GDPR requirements.	• Ensuring that all policies related to data collection, transfer, right to access, consent management, data breach notification, privacy notices, and data minimization align with GDPR standards and are fully compliant with regulatory requirements.
• Check how the data subject access requests (DSAR) are handled and determine what level of compliance is met with GDPR.	• Identification of the flexibility and procedures of data subject access requests (DSAR).
• Provide technical recommendation, such as software or workflow, to support continuous monitoring and auditing processes to ensure ongoing GDPR privacy compliance.	• Implementation of technical recommendations, such as software or workflows, supporting continuous monitoring and auditing processes to ensure ongoing GDPR privacy compliance.

Project Outcomes	Measure of Success
• Evaluations should be made to assess the level of compliance or potential data privacy risks as well as identify any potential gaps in compliance.	• Identify and document compliance gaps in the University's current level of compliance with GDPR regulations

1. Evaluations conducted to assess the compliance of any potential data privacy risks or identify any potential gap.

1. Problem:

The issue arises from the installation of cookies during the loading of web pages without obtaining prior consent from users, particularly concerning the processing of personal data. Although a cookie consent banner is displayed, it just has the “Accept and Continue” option. The user should have full access to the Accept, Reject, or Customize cookie collection mechanisms. Additionally, users should have the option to change their consent at any point in time. These cookies are typically utilized for tracking site visitors' behavior, gathering data for marketing purposes, and displaying targeted advertisements. According to Articles 30 and 32 of the General Data Protection Regulation (EU) 2016/679, it is mandatory to obtain explicit consent from users before installing cookies that process personal data, such as those used for tracking and targeted advertising. Failure to obtain consent can result in a breach of privacy rights and may lead to regulatory penalties- which can be up to 20 million euros or 4% of the total global turnover in a fiscal year Art. 83(5).

Solution: To address this issue, the website must **implement a robust cookie consent mechanism** that complies with GDPR requirements. This entails integrating **a cookie consent form** into the website's design, which should prominently **display all the options (accept, reject, and customize) to users upon their initial visit**. The consent form should clearly explain the purpose of the cookies, the types of data collected, and how it will be used. Users must be given the option **to either accept or reject** the use of cookies before any data processing occurs. If a user chooses not to provide consent, the website should refrain from installing cookies that process personal data, effectively blocking their deployment. By ensuring that user consent is obtained prior to the installation of cookies, the website can uphold GDPR principles of transparency, accountability, and user control over their personal data. There are no changes in the cookie collection mechanism if any Clark community member uses a VPN.

Examples of how a proper cookie consent mechanism can be implemented

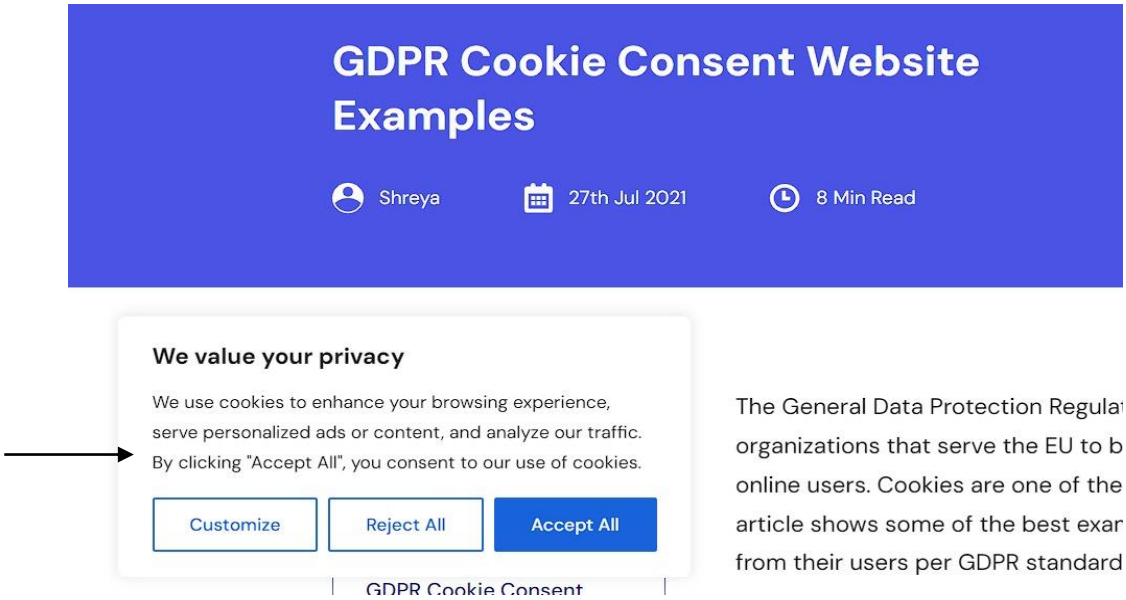

Fig 1

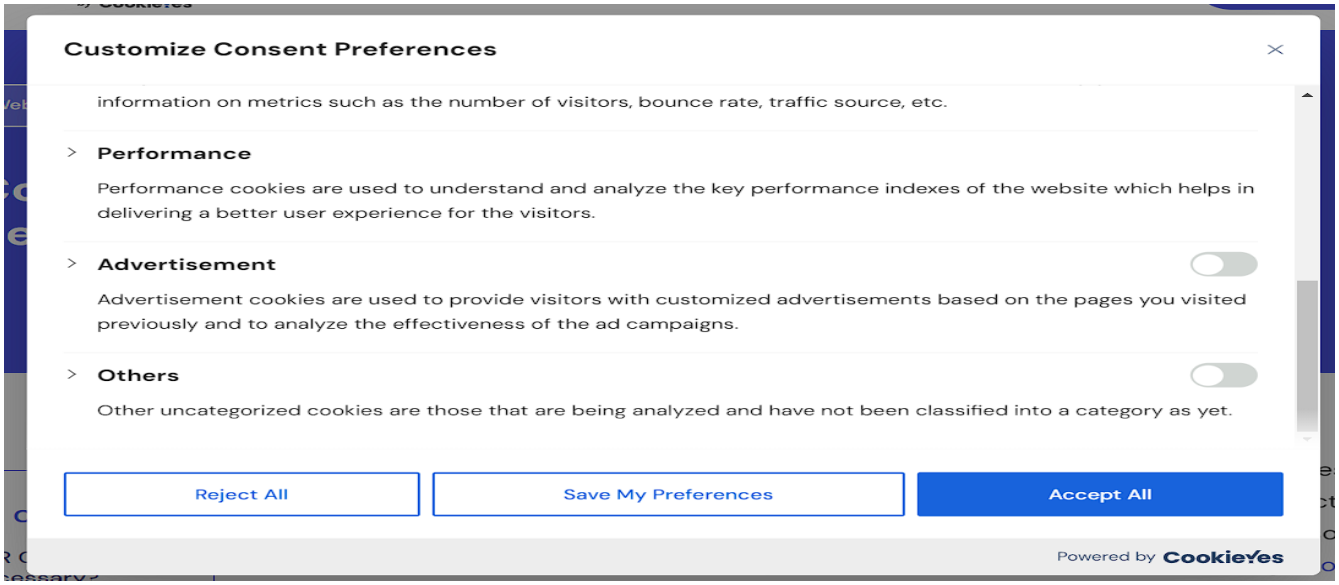

Fig 2

Fig 3

1. **Problem**:

Cookies installed during the loading of pages are **not strictly necessary**, meaning they do not fall under the **category of essential cookies** required for the basic **functioning of the website.** This non-compliance poses a risk of violating regulations such as the ePrivacy Directive, particularly for users within the European Union (EU). According to Articles 30 and 32 of the General Data Protection Regulation (EU) 2016/679, explicit consent from users is required before installing non-essential cookies, including those used for tracking, analytics, or advertising purposes. (Student Resources | Clark University, 2023)[10]

Example:

Cookies collected:

Cookie (Facebook): _fbp;

Cookie (Google AdSense): _gcl_au;

Cookie (Google Analytics): _ga;

Solution: To address this issue, it is essential to implement a **cookie consent mechanism on the website.** This consent form should be prominently displayed and require users to actively consent to the use of cookies before any non-essential cookies are installed. If a user does not provide consent, the website should refrain from loading non-essential cookies, effectively blocking their installation. By obtaining prior consent in compliance with

[10] Student Resources | Clark University. (2023, December 1). Clark University. https://www.clarku.edu/student-resources/

relevant regulations, such as the ePrivacy Directive and GDPR, the website can ensure transparency and respect users' privacy rights regarding their online data.

Examples of what kinds of cookies are being collected:

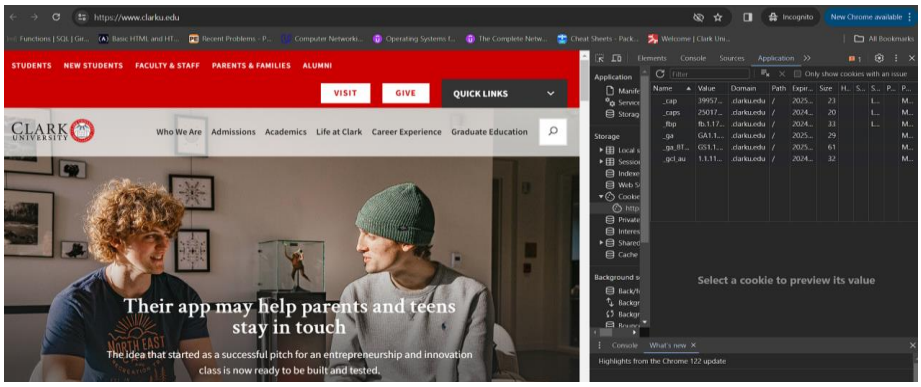

Fig 4

Project Outcomes	Measure of Success
• Determine if the processes and privacy protocols currently in place, satisfy those needed to improve data protection.	• Confirm that the existing processes and privacy protocols in place meet the requirements needed for enhancing data protection.

2.Determine if the processes and privacy protocols currently in place satisfy those needed to improve data protection.

A. **Problem statement:** "ENTITIES AFFECTED BY THIS POLICY" section in the “Change Management Policy” outlines who is affected by the policy, it does not explicitly mention **how personal data and privacy will be protected** for these individuals. The policy states that individuals involved in the management, operation, and maintenance of systems are subject to the policy, but it does not provide details on how their personal information will be handled in the context of change management. This lack of clarity could potentially lead to privacy breaches, especially if personal data is mishandled during the change management process. Therefore, it could be seen as a potential violation of (EU) 2016/679, which require clear and transparent handling of personal data. **Solution**: A comprehensive **Privacy Impact Assessment (PIA)** must be carried out as the first stage in order to address any potential privacy concerns and guarantee compliance with (EU) 2016/679 regulations. The goal of this

assessment is to find and analyze any privacy issues related to the change management procedure, with an emphasis on the management, storage, and protection of personal data at every stage of its lifespan. To guarantee that privacy issues are incorporated into system design and operation, privacy by design and default principles must be implemented into the change management process. Data reduction techniques will also restrict the amount of personal data that is gathered and processed to what is absolutely required. Encryption and strong access restrictions are necessary to protect personal information from disclosure or unwanted access. Organizations can reduce risks and protect individuals' rights under (EU) 2016/679 legislation by putting privacy first and implementing these actions. (Change Management Policy| Clark University, 2023)[11]

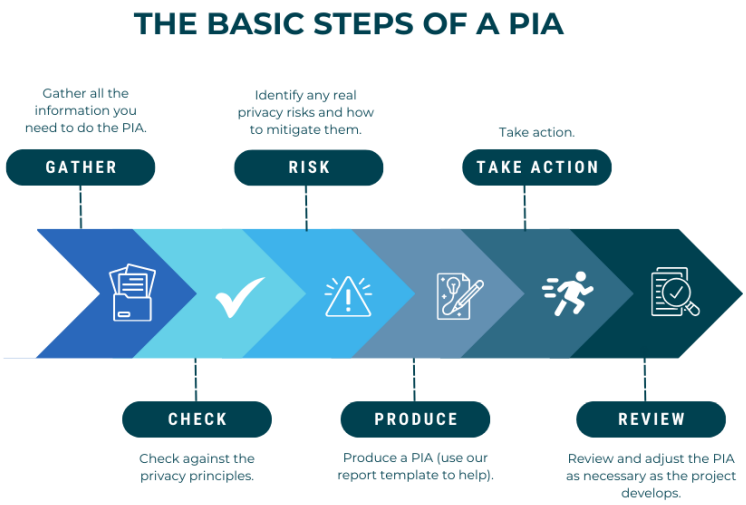

Fig 5

2.

A. **Problem statement:** Currently, Clark University does not have a designated Data Protection Officer (DPO). While (EU) 2016/679 mandates publicly traded companies to appoint a DPO, as a private non-profit organization, Clark University is not obligated to do so. However, the university has a position for an Information Privacy and Compliance Analyst who assumes responsibilities akin to those of a DPO, overseeing all relevant activities.

[11] https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/09/Change-Management-Policy-v.2.pdf

B. **Suggestion**: Clark University, while not legally obligated to appoint a Data Protection Officer (DPO) like publicly traded companies under GDPR, can enhance its data privacy and compliance efforts by designating clear responsibilities to its Information Privacy and Compliance Analyst. This individual would oversee all activities akin to those of a DPO, including staying updated on regulations, managing policies and procedures, and serving as a point of contact for privacy inquiries. Providing comprehensive training and resources, establishing an oversight committee, and conducting regular compliance audits will further strengthen the university's data protection measures and ensure alignment with strategic objectives.

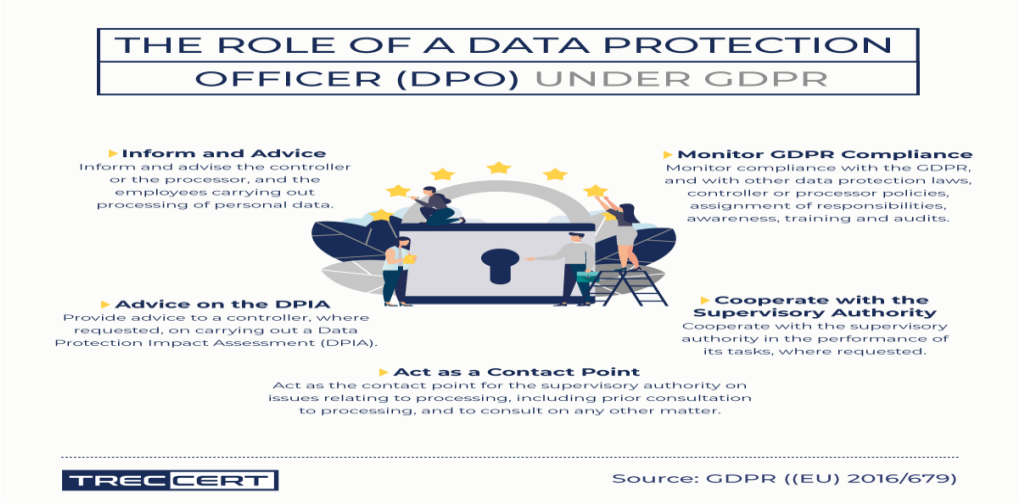

Fig 6

Project Outcomes	Measure of Success
• Identify compliance of data handling within the university network and with third parties.	• Identification and remediation of compliance gaps in data handling within the university network and with third parties.

2. Identify compliance with data handling within the university intranet and with third parties.

Current data sharing infrastructure with third party seems adequate and follows all the required (EU) 2016/679 rules. However, there are some recommendations and changes to the rules that we would like to give to enhance data sharing with vendors.

3. Data Minimization and Lawful use: Organizations should avoid disclosing any information that is unnecessary or irrelevant to third parties and should only release as much personal data as is required for the intended use. Data sharing needs to be legal; this means it needs to be justified by legitimate interests, explicit consent, or special data protection clauses in contracts.

In general, GDPR places stringent requirements on enterprises regarding the sharing of personal data with third parties, with a focus on accountability, openness, and safeguarding individuals' privacy rights at every stage of the data processing lifecycle. To improve security, this clause can be added to the current policy. (File Sharing and Copy Right Policy |File Sharing and Higher Education Opportunity Act| Clark University, 2023)[12][13]

Project Outcomes	Measure of Success
• Explore other laws, such as PIPL, DPDP, and FERPA, and determine if there is any overlap with GDPR.	• Identification of overlaps of non-compliance between GDPR and other relevant data privacy laws, along with recommendations to address them

A. Data Protection Principles: The Digital Personal Data Protection (DPDP) Act, PIPL, FERPA, and GDPR all place a strong emphasis on data protection principles such accuracy, security, purpose limitation, and data minimization. Article 5 of the GDPR, Article 6 of the PIPL, FERPA regulations, and particular sections of the DPDP Act all set forth these concepts in clearly stated terms. Although GDPR emphasizes the principles of lawfulness, fairness, and transparency, FERPA emphasizes the need for education records to remain confidential and of high quality, the DPDP Act complies with international standards for data protection and emphasizes consent and data security, and PIPL emphasizes the significance of data processing for lawful purposes.

B. **Consent:** Organizations are typically required by GDPR, PIPL, FERPA, and the DPDP Act to seek individuals' consent before collecting, processing, or disclosing their personal data. While the DPDP Act requires obtaining consent as a fundamental principle of data processing, FERPA requires consent under certain circumstances for the

[12] https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/08/File-Sharing-and-the-Higher-Education-Opportunity-Act-Policy.pdf
[13] https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/08/File-Sharing-and-Copyright-Policy.pdf

disclosure of education records, PIPL's consent provisions are outlined in Article 12, and the GDPR is explicit about consent requirements in Articles 6 and 7. Nonetheless, given the distinct aims and circumstances of the areas they oversee, each statute may have different consent procedures and standards.

C. Individual Rights: Individuals have various rights to their personal data, including the ability to access, correct, and delete it, thanks to laws like the DPDP Act, FERPA, GDPR, and PIPL. Articles 15–22 of the GDPR explain individual rights; Articles 43–52 cover PIPLs; particular sections of FERPA outline rights of access and amendment; and the DPDP Act, which complies with international standards, gives people the ability to view and update their personal data. The legal frameworks and societal norms of the various countries may influence the differences in the laws' scope of application and precise processes for exercising the rights, despite potential parallels in the rights conferred.

D. Data Security: Organizations are required by the DPDP Act, FERPA, GDPR, and PIPL to put in place the necessary organizational and technical safeguards to protect personal data. The DPDP Act requires data security as a critical component of compliance, the GDPR lays out security standards in Article 32, the PIPLs in Article 41, and FERPA offers guidance for securing school information in various portions of the legislation. The general objective of guaranteeing data security is the same for all of these regulations, but the particular standards and methods that are required may differ due to the dynamic nature of technology and the distinct risk environments that exist for businesses operating in various industries and regions.

Project Outcomes	Measure of Success
• Review and assess Clark University policies for data collection, transfer, right to access, consent management, data breach notification, privacy notices, and data minimization to ensure compliance with GDPR requirements.	• Ensuring that all policies related to data collection, transfer, right to access, consent management, data breach notification, privacy notices, and data minimization align with GDPR standards and are fully compliant with regulatory requirements.

Review and Assessment of Policies for GDPR Compliance: The following is an outline of the review and assessment of Clark University's policies concerning data collection, transfer, right to access, consent management, data breach notification, privacy notices, and data minimization to ensure compliance with GDPR requirements. It includes reasons, recommendations, and examples to see that it complies with GDPR Regulations. (Policies and Standards | Information Technology Services | Clark University, 2023)[14]

A. **DATA COLLECTION: (Baig, 2022)**

Example: Data Collection within Appropriate Use of Clark's Information Technology System Policy.

- **Appropriate Use of Clark's Information Technology System Policy :** The Appropriate Use of Clark's Information Technology System Policy has to make sure that it is responsible and acceptable use of computer systems, applications, and electronic communications, highlighting lawful and transparent data processing procedures.
- **Non- Compliant:** After reviewing the policy, we can see that there is a need for periodic audits, but the policy does not clearly identify or assign the specific individuals or roles within the organization who are responsible for carrying out these periodic audits as required by GDPR Article 32. This article requires organizations to implement measures, including audits, to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services. This policy's lack of clear assignment for audit responsibility does not meet GDPR's accountability and oversight requirements (GDPR, Article 32).[15]

Fig 7

[14] Policies and Standards | Information Technology Services | Clark University, 2023
[15] (Art. 32 GDPR – Security of Processing - General Data Protection Regulation (GDPR), 2016)

Recommendation:

Our recommendations are as follows

- Our Recommendation is to conduct regular audits annually or biannually to make sure that there is ongoing compliance and clarity in data collection[16] practices.
- Our Recommendation is to implement a regular review process for data collection forms to make sure they collect only information that is required.
- Our Recommendation is to define a clear schedule for audits, such as conducting them once or twice a year, and assigning responsibility to a specific individual or team.

Analysis of Clark University Policies and identification of GDPR, PIPL and DPDP Compliance and Non-Compliance:

- **GDPR:** The General Data Protection Regulation requires organizations to provide clear information on data processing purposes and easy mechanisms for consent withdrawal.
- **PIPL:** The China's Personal Information Protection Law mandates organizations to inform individuals about data processing purposes and obtaining explicit consent.
- **DPDP:** The India's Digital Personal Data Protection Bill requires providing notice about data collection and obtaining consent for processing.

B. DATA TRANSFER:

Example: Data Transfer within Policy on Data Security for All Faculty, Staff, and Student Employees.

Policy on Data Security for All Faculty, Staff, and Student Employees: The Policy on Data Security for All Faculty, Staff, and Student Employees at Clark University is designed to ensure the secure transfer of data, especially when transferring data outside the European Economic Area (EEA). This policy outlines specific measures and provisions that must be followed to maintain data security standards.

- **Compliant:** Clark University has implemented a strict process to safeguard the confidentiality and privacy of data shared with external vendors. This process involves requiring all vendors to sign and

[16] Baig, A. (2022, September 2). *GDPR Data Collection Requirements*. Security. https://securiti.ai/blog/gdpr-data-collection/

adhere to the Vendor Data Privacy and Confidentiality Agreement (VDPCA), which outlines strict guidelines for the handling and protection of sensitive information.

- Furthermore, the university conducts thorough assessments of third-party data processors to ensure compliance with data protection regulations. These assessments include a review of the sub-processors used by vendors and an examination of their data processing practices. This comprehensive approach ensures that all vendors adhere to the requirements of the General Data Protection Regulation (GDPR) and that data is managed securely and confidentially throughout the vendor relationship.

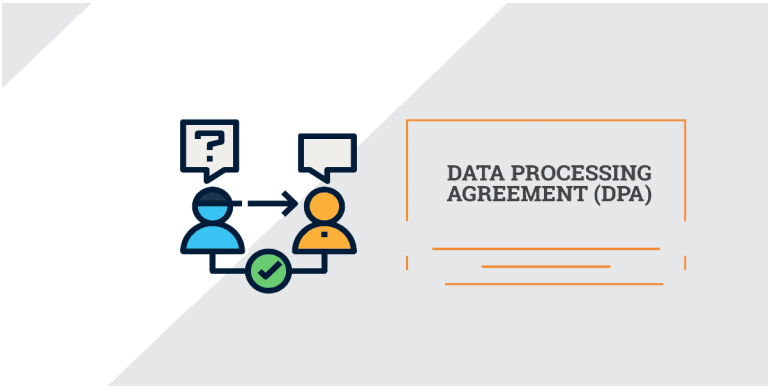

Fig 8

- **PIAs for Individual Software Solutions:** Privacy Impact Assessments (PIAs) are done for each individual software solution to review its effect on privacy and safeguard compliance with GDPR. These assessments are important for identifying and justifying privacy risks associated with the use of software solutions, to make sure that data transfers are conducted securely and in compliance with data protection laws.

Recommendation:

- Our recommendation is to further improve data transfer practices, Clark University could consider regularly reviewing and updating its data transfer agreements and assessment processes to make sure that they align with the latest GDPR standards and practices. This kind of active step can help maintain a high level of data protection and compliance with relevant regulations.
- Our recommendation is to ensure that data transfer agreements have all necessary sections to comply with GDPR requirements, such as those related to data security and third-party data processor agreements.

Analysis of Clark University Policies and identification of GDPR, PIPL and DPDP Compliance and Non-Compliance:

- **GDPR:** Per the General Data Protection Regulation(GDPR) Universities or Organizations requires the vendors to make sure to have data transfer agreements in place and the assessment of third-party data processors for compliance align with GDPR's importance on ensuring secure data transfers and compliance with data protection standards.
- **PIPL:** Per China's Personal Information Protection Law (PIPL) vendors are required to sign data transfer agreements and evaluate third-party data processors for compliance in accordance with PIPL's terms for ensuring secure cross-border data transfers and adherence to data protection regulations. This practice helps to ensure that all data processors involved in handling personal information are compliant with PIPL's regulations and that the data is transferred securely and in accordance with the law.
- **DPDP:** Clark University's approach of being compliant aligns with the requirements of the Digital Personal Data Protection (DPDP) Bill regarding obtaining consent for cross-border data transfers and ensuring compliance with data protection laws. This means that the university follows the DPDP's guidelines for obtaining explicit consent from individuals before transferring their data across borders. Additionally, the University ensures that its data protection practices comply with the regulations outlined in the DPDP Bill, thus prioritizing the security and privacy of personal data in line with the requirements of the law.

C. RIGHT TO ACCESS:

Example: Let’s see an example for Right to Access on Clark Account Policy

Clark Account Policy: The Clark Account Policy sets regular guidelines for accessing university computing resources. It ensures secure access to data subjects personal data stored in Clark's systems by defining specific procedures and protocols for authentication and data retrieval. The policy aims to provide a consistent and secure method for users to manage and access their personal information within the university's computing environment.

• **Non-Compliant:** Here it is non-compliant as policy recognizes the importance of improving how quickly requests for data access are handled, it doesn't explain how to deal with delays in responding to these requests.

This could lead to inconsistent or slow responses, which might break the rules set by data protection laws like GDPR. To be compliant, it's important not only to have efficient procedures for handling these requests but also to address and reduce any delays in responding to them. [17]

Fig 9

Recommendation:

Our recommendation are as follows

- As we can see that there is a need to respond in a timely manner, we can include recommendations such as making the process easy for data access requests and ensuring timely responses.
- Provide an online portal for individuals to submit data access requests, with a clear timeline for responses such as ServiceNow, Zendesk and more. (Product Documentation | ServiceNow, n.d.)[18]
- Establish a clear timeline for responding to data access requests and allocate sufficient resources to ensure timely responses.

Analysis of Clark University Policies and identification of GDPR, PIPL and DPDP Compliance and Non-Compliance:

- **GDPR:** The General Data Protection Regulation (GDPR) gives individuals the right to access their personal data and requires organizations to respond to access requests in a timely manner.

[17] (Art. 15 GDPR – Right of Access by The Data Subject - General Data Protection Regulation (GDPR), 2018)
[17](Product Documentation | ServiceNow, n.d.)

- **PIPL :** China's Personal Information Protection Law(PIPL) grants individuals the right to access and correct their personal information. This supports the suggestion to ease the data access request process, as it allows individuals to easily access and rectify their personal information.
- **DPDP :** India's Digital Personal Data Protection Bill (DPDP) allows individuals the right to access and correct their data and requires organizations to respond to access requests in a timely manner. The recommendation to establish a clear timeline for responding to data access requests is based on DPDP's requirements for timely responses**.**

D. CONSENT MANAGEMENT: (Consent - (GDPR), 2021)

Example within Email Policy:

Email Policy: This Policy regulates the use of Clark University's email communication system, ensuring that email communications comply with GDPR principles for obtaining and documenting consent.

- **Non-Compliant:** While the Policy suggests providing clear information on data processing purposes and offering easy mechanisms for consent withdrawal, it does not specify how this should be implemented. [19]

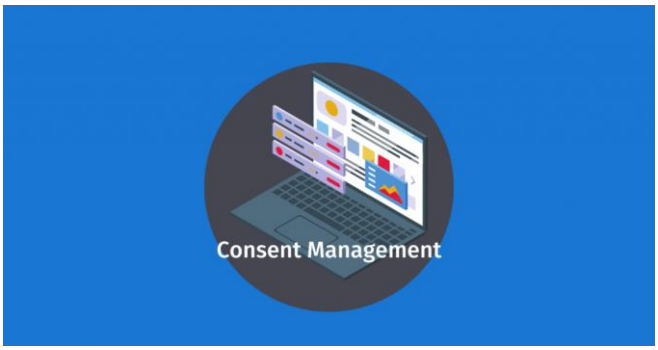

Fig 10

Recommendation:

Recommendations are as follows

- Our Recommendation is to provide clear information on data processing purposes and offer easy mechanisms for consent withdrawal.

[19] Consent - General Data Protection Regulation (GDPR). (2021, October 22). General Data Protection Regulation (GDPR). https://gdpr-info.eu/issues/consent/

- Our Recommendation is to include detailed descriptions of data processing activities in consent forms, along with clear instructions for withdrawing consent.
- Our Recommendation is to clearly communicate the process for withdrawing consent, such as providing a dedicated email address or online form for withdrawal requests.

Analysis of Clark University Policies and identification of GDPR, PIPL and DPDP Compliance and Non-Compliance:

- **GDPR:** To comply with General Data Protection Regulation (GDPR), organizations must obtain clear consent from individuals before processing their data and provide mechanisms for individuals to withdraw this consent.
- **PIPL:** Compliance with China's Personal Information Protection Law (PIPL) involves organizations obtaining consent from individuals for data processing and offering them the ability to withdraw this consent.
- **DPDP:** Complying with India's Digital Personal Data Protection Bill (DPDP) similarly entails obtaining consent from individuals for data processing and providing them with means to withdraw this consent.

E. DATA BREACH NOTIFICATION:

Example within Security Extension to Appropriate Use Policy.

Security Extension to Appropriate Use Policy: This policy establishes rules for securing the network to prevent data breaches and outlines procedures for reporting and responding to data breaches.

- **Non- Compliant:** This policy recommends regular testing of incident response procedures but does not specify how often this should occur or what constitutes a sufficient test. [20]

Recommendation:

- Our recommendation is to regularly test incident response procedures and enhance communication protocols.
- Our recommendation is to conduct regular tabletop exercises to simulate data breach scenarios and test the effectiveness of the response plan.

[20] (Art. 33 GDPR – Notification of a Personal Data Breach to The Supervisory Authority - General Data Protection Regulation (GDPR), 2018)

- Conduct regular tabletop exercises to simulate data breach scenarios and evaluate the effectiveness of the response plan, adjusting as needed.

(This is already in practice and Incident Response procedures are tested on a bi-monthly basis.)

Analysis of Clark University Policies and identification of GDPR, PIPL and DPDP Compliance and Non-Compliance:

- **GDPR**: This regulation mandates that organizations notify the relevant supervisory authority of a data breach within 72 hours of becoming aware of it unless the breach is unlikely to result in a risk to individuals' rights and freedoms.
- **PIPL**: China's Personal Information Protection Law(PIPL) requires organizations to report data breaches to both the authorities and affected individuals. As per this it should inform the individual immediately when their data is compromised.
- **DPDP** : Similar to PIPL, the DPDP also requires organizations to report data breaches to the authorities and affected individuals.

F. PRIVACY NOTICES:

Example

Privacy Policy: Defines how Clark University uses and protects personal information, ensuring that privacy notices provided to data subjects meet GDPR requirements for informing them about data processing activities.

- **Non-Compliant:** The Policy recommends regular reviews of privacy notices but does not specify who should conduct these reviews or how often they should occur.

Recommendation:

Our recommendations are as follows

- We recommend conducting regular reviews of privacy notices to ensure accuracy and completeness.
- We recommend scheduling quarterly reviews of privacy notices to align with any changes in data processing activities.

- We recommend assigning responsibility for reviewing privacy notices to a specific individual or team and establishing a schedule for regular reviews, such as quarterly or biannually.

Analysis of Clark University Policies and identification of GDPR, PIPL and DPDP Compliance and Non-Compliance:

- **GDPR:** General Data Protection Regulation requires organizations to provide individuals with clear and concise information about how their personal data is processed. This includes information about the purposes of processing, the legal basis for processing, and the rights of individuals in relation to their data.
- **PIPL:** China's Personal Information Protection Law(PIPL) emphasizes the importance of providing clear and detailed notices to individuals about the collection and use of their personal information. It requires organizations to be transparent about their data processing activities and obtain consent where necessary.
- **DPDP:** Similar to General Data Protection Regulation(GDPR) and China's Personal Information Protection Law (PIPL), India's Digital Personal Data Protection Bill (DPDP) requires organizations to provide clear and transparent information to individuals about the collection and processing of their personal data. It also emphasizes the need for organizations to obtain consent and inform individuals about their rights regarding their data.

Project Outcomes	Measure of Success
• Check how the Data Subject Access Requests (DSAR) are handled and determine what level of compliance is met with GDPR.	• Identification of the flexibility and procedures of Data Subject Access Requests (DSAR).

Fig11

Introduction:

Clark University's approach to Data Subject Access Requests (DSAR) is crucial for ensuring compliance with the General Data Protection Regulation (GDPR). Clark University has a strong framework in place for handling data erasure requests. The policies emphasize the secure transfer of data, restrict the storage of sensitive information like credit card numbers, and define procedures for retaining and destroying documents containing confidential data. Additionally, the Email Policy ensures compliance with GDPR principles for obtaining and documenting consent, while the Password Policy sets minimum standards for selecting and protecting passwords. The Privacy Policy outlines how Clark uses and protects information provided to the university, demonstrating a commitment to data privacy. Clark University's policies show a proactive approach to data protection and suggest a strong foundation for handling data erasure requests in compliance with GDPR, DPDP, and PIPL. **(Art. 17 GDPR)**[21]

Recommendation:

- Our Recommendation is to create a standalone Data Erasure Policy outlining procedures for handling data erasure requests to ensure consistency and clarity.
- Example: Implement a process for individuals to submit data erasure requests through a designated portal or email address.

[21] (Art. 17 GDPR – Right to Erasure ('Right to Be Forgotten') - General Data Protection Regulation (GDPR), 2017)

GDPR Compliance:

- **Non-Compliant**: While the university's policies demonstrate a commitment to GDPR compliance, there may be gaps in ensuring all aspects of data erasure requests that are addressed.
- **Recommendation**: Conduct a review of some existing policies to ensure they fully align with GDPR requirements for data erasure requests as follows

a) Document Retention and Destruction Policy

Fig 12

- **Compliance**: The Document Retention and Destruction Policy is compliant as it defines procedures for retaining and destroying documents containing any Confidential and/or Restricted data types.
- **Recommendation**: Our Recommendation is that the policy should define specific data retention periods for different types of data to ensure compliance with GDPR, DPDP, and PIPL. It should specify the maximum allowable retention period for each type of data and provide guidelines for securely and irreversibly destroying data at the end of its retention period. Additionally, the policy should clarify the responsibilities of third-party data processors in complying with data erasure requests and ensure they adhere to the same standards as the university.

b) Email Policy

- **Compliance**: The Email policy is compliant as it regulates the use of Clark University's email communication system.
- **Recommendation**: The policy should include specific procedures for handling data erasure requests related to email communications. It should outline the process for individuals to request the erasure of their email data, including the required information and the format for submitting requests. Additionally, the policy

should specify the steps for verifying the identity of the requester and the process for securely erasing the email data from all relevant systems.

c) File Sharing and Copyright Policy

- **Compliance:** The File Sharing and Copyright policy is compliant as it encourages appropriate use of the Internet with respect to copyright law.
- **Recommendation:** Our Recommendation is that the policy should include specific procedures for handling data erasure requests related to file sharing activities. It should outline the process for individuals to request the erasure of their file sharing data, including the required information and the format for submitting requests. Additionally, the policy should specify the steps for verifying the identity of the requester and the process for securely erasing the file sharing data from all relevant systems.

d) Password Policy

- **Compliance**: The Password policy is compliant as it establishes minimum standards for selecting and protecting passwords.
- **Recommendation**: Our Recommendation is that the policy should include specific procedures for handling data erasure requests related to password protection. It should outline the process for individuals to request the erasure of their password data, including the required information and the format for submitting requests. Additionally, the policy should specify the steps for verifying the identity of the requester and the process for securely erasing the password data from all relevant systems.

e) Privacy Policy

- **Compliance**: The Privacy policy is compliant as it sets out how Clark uses and protects any information provided to Clark.
- **Recommendation**: Our Recommendation is that the policy should include specific procedures for handling data erasure requests related to personal information. It should outline the process for individuals to request the erasure of their personal data, including the required information and the format for submitting requests.

Additionally, the policy should specify the steps for verifying the identity of the requester and the process for securely erasing the data from all relevant systems.

f) Remote Access Policy

- **Compliance**: The Remote Access policy is compliant as it states the requirements for remote access to computing resources.
- **Recommendation**: Our Recommendation is that the policy should include specific procedures for handling data erasure requests related to remote access. It should outline the process for individuals to request the erasure of their remote access data, including the required information and the format for submitting requests. Additionally, the policy should specify the steps for verifying the identity of the requester and the process for securely erasing the data from all relevant systems.

2.Security Awareness Training and Testing

Our Recommendation are as follows for Security Awareness Training and Testing

- Introducing specific procedures for handling data erasure requests in the training program. It should outline the training requirements for employees regarding data erasure requests, including the importance of timely responses and the proper procedures for handling such requests. Additionally, the policy should specify the steps for verifying the identity of the requester and the process for securely erasing the data from all relevant systems.
- Implementing regular audits of data erasure requests to ensure compliance with GDPR requirements.
- Enhancing existing policies to include specific procedures for handling data erasure requests in compliance with GDPR, such as providing clear guidance on verifying requests and erasing data.

3. Flexibility and Procedures:

The flexibility of Clark University in handling data erasure requests may be limited by the absence of a dedicated policy.

Our Recommendation are as follows

- Provide flexibility in the process for submitting data erasure requests, such as offering multiple channels for submission.
- Allow individuals to submit data erasure requests through an online portal, email, or in person.
- Develop a flexible process for handling data erasure requests that accommodates different preferences and ensures timely responses.

4. Response Time and Process:

Non-Compliant: The policies may not specify response times for data erasure requests, leading to potential delays in processing requests.

Our Recommendation are as follows

- Define clear response times for data erasure requests to ensure timely processing.
- Our recommendation is to Set a policy of responding to data erasure requests within 30 days of receipt.
- Establish standard response times for data erasure requests and communicate them to individuals submitting requests.

5. Contact Points:

- **Non-Compliant**: The policies may not clearly identify who within Clark University is responsible for handling data erasure requests.

Our Recommendation are as follows

- Clearly identify contact points for data erasure requests to ensure requests are directed to the appropriate individuals.
- Designate a specific department or individual as the point of contact for data erasure requests.
- Clearly communicate contact information for data erasure requests in relevant policies and on the university's website.

Clark University's policies demonstrate a commitment to GDPR compliance regarding data erasure requests. By implementing the recommendations outlined in this report, the university can enhance its processes for handling data erasure requests and ensure compliance with GDPR requirements.

Project Outcomes	Measure of Success
• Provide technical recommendation, such as software or workflow, to support continuous monitoring and auditing processes to ensure ongoing GDPR privacy compliance.	• Implementation of technical recommendations, such as software or workflows, supporting continuous monitoring and auditing processes to ensure ongoing GDPR privacy compliance.

In an organization or Institutions of Higher Education, it is very important in terms of data management to see that they comply with GDPR. This involves continuous monitoring and auditing to see that they are maintaining GDPR Compliance to support continuous monitoring and auditing processes to ensure ongoing GDPR privacy compliance. So, we are going to discuss the need for such tools for achieving compliance with GDPR.[22]

Non-Compliance Scenario

Let’s talk about a scenario where a university is facing challenges with its current data management practices, potentially leading to GDPR non-compliance. A major issue is the absence of a comprehensive system for continuous monitoring and auditing. Without such a system, the Institutions of Higher Education struggles to track data usage, access, and potential breaches. This absence of control increases the risk of data misuse or unauthorized access, which could result in severe penalties under GDPR.

Recommendation for Implementation

To address these non-compliance issues, the Institutions of Higher Education should consider implementing technical recommendations, such as software or workflows, to support continuous monitoring and auditing processes. One such recommendation is the adoption of a data governance platform that provides real-time monitoring of data access and usage. This platform should include features such as access controls, data encryption,

[22] (What Is Continuous Security Monitoring and Why Is It Important?, n.d.)

and audit trails to ensure GDPR compliance. Additionally, implementing automated workflows for data access requests and approvals can streamline the process and ensure that access to personal data is granted only to authorized individuals. This reduces the risk of unauthorized access and enhances GDPR compliance.

Benefits of Implementation

By implementing these technical recommendations, the Institutions of Higher Education can improve its data management practices and ensure ongoing GDPR privacy compliance. The continuous monitoring and auditing processes will provide the Institution of Higher Education with real-time insights into its data usage and access patterns, allowing for proactive identification and mitigation of potential compliance risks. Moreover, automated workflows will streamline data access requests, reducing the burden on administrative staff and ensuring timely responses to data subjects' requests.

Conclusion

In conclusion, implementing technical recommendations, such as software or workflows, to support continuous monitoring and auditing processes is crucial for ensuring ongoing GDPR privacy compliance. By addressing non-compliance issues and implementing these recommendations, universities can enhance their data management practices and mitigate the risks associated with data misuse or unauthorized access.

Some examples are as follows:

a) **Data Loss Prevention (DLP) Tools:** DLP tools can help monitor and prevent unauthorized access or sharing of sensitive data, ensuring compliance with GDPR data protection requirements such as processing of personal data, personal data breach to the supervisory authority, Communication of a personal data breach to the data subject and more. Examples include Symantec DLP, McAfee DLP, and Digital Guardian. These tools are for both small and large business with de-centralized based on the requirements of the organization to comply with GDPR.

Fig 13

b) **Security Information and Event Management (SIEM) Tools:** SIEM tools can centralize the collection, analysis, and monitoring of security events to detect and respond to potential data breaches or non-compliance incidents. Examples include Splunk (This is already in practice), IBM QRadar, and ArcSight.

Fig 14

c) **Data Mapping and Inventory Tools**: These tools help organizations map their data flow and maintain an inventory of personal data, which is essential for GDPR compliance. Examples include One Trust Data Mapping, Collibra, and Varonis.

Fig 15

d) **Identity and Access Management (IAM) Solutions**: IAM solutions help manage user access to systems and data, ensuring that only authorized individuals have access to personal data. Examples include Okta, Microsoft Azure Active Directory, and Ping Identity.

Fig 16

e) **Identity and Access Management (IAM) Solutions**: IAM solutions help manage user access to systems and data, ensuring that only authorized individuals have access to personal data. Examples include Okta, Microsoft Azure Active Directory, and Ping Identity.

Fig 17

6.DISCUSSION

6.1 Insights:

1. **Existing Compliance:** Clark University demonstrates a commitment to GDPR compliance through various policies addressing data collection, transfer, access, consent management, breach notification, privacy notices, and data minimization.
2. **Areas of Strength:** Some policies, such as the Data Security Policy, demonstrate alignment with GDPR principles, including secure data transfer and data minimization practices.
3. **Areas for Improvement:** Policies related to data erasure requests and consent management and some others could be strengthened to ensure compliance with GDPR requirements.

6.2 Recommendations:

1. **Cookie Consent Mechanism**: Implement a robust cookie consent mechanism that complies with GDPR requirements. This should include options for users to accept, reject, or customize cookie settings, as well as the ability to change their consent preferences at any time.
2. **Password Policy**: Strengthen the password policy by restricting the use of common words and patterns, increasing the minimum password length, and mandating regular password changes and prohibition of password reuse.(This is already in Use)
3. **Change Management Policy:** Enhance the Change Management Policy to explicitly address the protection of personal data and privacy, ensuring that all individuals affected by the policy are aware of how their personal information will be handled.
4. **Data Loss Prevention (DLP) System**: Implement a DLP system for the Outlook email system to prevent the inadvertent exposure of sensitive information, such as personally identifiable information (PII), through phishing attacks or accidental sharing.

5. **Designate Data Protection Officer (DPO):** While not legally obligated, consider designating clear responsibilities to the Information Privacy and Compliance Analyst to oversee all activities similar to those of a DPO, ensuring alignment with strategic objectives and enhancing data privacy and compliance efforts.
6. **Data Handling with Third Parties**: Ensure compliance with GDPR and other relevant laws by avoiding disclosing unnecessary or irrelevant information to third parties and justifying data sharing based on legitimate interests, explicit consent, or special data protection clauses in contracts.
7. **Identify Overlaps and Conflicts**: Explore overlaps and conflicts between GDPR and other relevant data privacy laws (such as PIPL, DPDP, and FERPA) to ensure alignment and consistency in compliance efforts.
8. **Dedicated Data Erasure Policy:** Develop a standalone internal policy outlining procedures for handling data erasure requests, ensuring consistency and clarity in compliance efforts.
9. **Enhanced Consent Management:** Improve the Email Policy to include detailed procedures for obtaining and documenting consent, aligning with GDPR standards.
10. **Regular Audits and Training:** Conduct regular audits annually of data protection practices, including data minimization, and provide training to staff on GDPR requirements.
11. **Automated Monitoring:** Implement automated systems for continuous monitoring and auditing of data processing activities to ensure ongoing GDPR compliance.
12. **Improved Communication:** Clearly communicate data erasure request processes and contact points for such requests to ensure timely responses and compliance.
13. **Vendor Management Practices**: Implement robust vendor management practices, including vendor data transfer agreements and regular assessments of vendors' compliance with GDPR requirements.
14. **Privacy Impact Assessments (PIAs):** Conduct individual PIAs for new software solutions to assess their impact on privacy and ensure compliance with GDPR.
15. **Continuous Improvement:** Establish a process for continuous improvement of data protection practices, including regular reviews of policies and procedures to align with changing regulatory requirements.(This is currently in practice)

The above recommendations can enhance its data privacy practices, improve compliance with relevant laws, and ensure the protection of personal data.

7.CONCLUSION

7.1 Summary of key findings and their implications:

The analysis of Clark University's current data privacy policies and practices has revealed several key findings and implications for GDPR compliance and data protection.

The evaluation highlighted areas of non-compliance, particularly concerning the handling of cookies and password policies. Issues like installing the cookies without the data subjects' consent and not having a strong password will impose these penalties under GDPR. For any serious violations, organizations can face fines of up to €20 million or 4% of their global annual turnover, whichever is higher.[23]

This penalty is also for violating the personal data of the data subject without consent, or failure to fulfill data subject rights. For less severe infringements, organizations can face fines of up to €10 million or 2% of their global annual turnover, whichever is higher.

The assessment identified gaps in privacy protocols, especially regarding the protection of personal data during change management processes and the absence of a designated Data Protection Officer. These gaps could result in privacy breaches and non-compliance with GDPR requirements.

Furthermore, the analysis emphasized the importance of continuous monitoring and auditing processes to ensure ongoing GDPR compliance. Recommendations for implementing technical solutions, such as DLP systems and cookie consent mechanisms, were provided to enhance data protection measures.

7.2 Suggestions for Future Research or Actions:

1. Our recommendation is to conduct a comprehensive review of all policies and procedures related to data privacy to ensure alignment with GDPR and other relevant laws.

[23] (Fines / Penalties - General Data Protection Regulation (GDPR), 2021)

2. Our recommendation is to implement a robust data protection framework that includes regular audits, privacy impact assessments, and staff training programs.

3. Our recommendation is to enhance the university's data protection measures by investing in advanced technologies such as AI-driven security solutions and encryption tools.

4. Our recommendation is to establish a clear roadmap for GDPR compliance, including milestones, responsibilities, and monitoring mechanisms.

In conclusion, achieving compliance with the General Data Protection Regulation (GDPR) requires a comprehensive approach that attends technical, organizational, and legal aspects of data protection. By precisely implementing the detailed recommendations outlined in this report and maintaining a persistent commitment to data privacy, organizations can strengthen their compliance efforts and ensure the protection of personal data in accordance with GDPR and other relevant laws. This involves not only implementing technical measures such as encryption and access controls but also establishing clear policies and procedures, conducting regular audits, and providing ongoing training to staff.

To conclude, we want to highlight that Compliance with GDPR is an ongoing process that requires continuous monitoring and adaptation to new challenges and regulatory requirements.

8 REFERENCES

Art. 15 GDPR – Right of access by the data subject - General Data Protection Regulation (GDPR). (2018, March 28). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-15-gdpr/

Art. 17 GDPR – Right to erasure ('right to be forgotten') - General Data Protection Regulation (GDPR). (2017, June 12). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-17-gdpr/

Art. 33 GDPR – Notification of a personal data breach to the supervisory authority - General Data Protection Regulation (GDPR). (2018, March 29). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-33-gdpr/

Baig, A. (2022, September 2). GDPR Data Collection Requirements. Security. https://securiti.ai/blog/gdpr-data-collection/

Briefing, C. (2022, July 21). PIPL vs GDPR - Key Differences and Implications for Compliance in China. China Briefing News. https://www.china-briefing.com/news/pipl-vs-gdpr-key-differences-and-implications-for-compliance-in-china/

Chapter 2 – Principles - General Data Protection Regulation (GDPR). (2018, October 5). General Data Protection Regulation (GDPR). https://gdpr-info.eu/chapter-2/

Consent - General Data Protection Regulation (GDPR). (2021, October 22). General Data Protection Regulation (GDPR). https://gdpr-info.eu/issues/consent/

Fines / Penalties - General Data Protection Regulation (GDPR). (2021, October 22). General Data Protection Regulation (GDPR). https://gdpr-info.eu/issues/fines-penalties/

How universities have to adapt under the new EU General Data Protection Regulation (GDPR) | Full Fabric. (n.d.). https://www.fullfabric.com/articles/how-universities-have-to-adapt-under-the-new-eu-general-data-protection-regulation-gdpr

https://medicine.ecu.edu/studentaffairs/wp-content/pv-uploads/sites/238/2019/02/FERPA-Flyer.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/09/Appropriate-Use-of-Clarks-Information-Technology-System-Policy-v.2-1.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/09/Change-Management-Policy-v.2.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/09/Data-Classification-Policy-v.2.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/09/Data-Security-Policy-for-All-Faculty-Staff-and-Student-Employees-v.2.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/09/Data-Security-Policy-for-Supervisors-Data-Managers-and-Data-Custodians-v.2.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/09/Email-Policy-v.2.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/08/File-Sharing-and-Copyright-Policy.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/08/File-Sharing-and-the-Higher-Education-Opportunity-Act-Policy.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/08/Maintaining-Clark-Web-Sites-Policy.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/09/Privacy-Policy-v.2.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/09/Remote-Access-Policy-v.2.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/08/Security-Extension-to-Appropriate-Use-Policy.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2022/08/Clark-Website-Policy.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2023/03/Clark-Account-Policy.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2023/05/Document-Retention-and-Destruction-Policy-1.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2024/03/Physical-Access-to-Restricted-IT-Areas-Policy-ISPC-Review.pdf

https://www.clarku.edu/policies/wp-content/uploads/sites/295/2024/03/Security-Awareness-Training-Testing-Policy.pdf

Personal Information Protection Law of the People's Republic of China - PIPL. (2022, May 10). PIPL. https://personalinformationprotectionlaw.com/

Policies and Standards | Information Technology Services | Clark University. (2023, February 15). Information Technology Services. https://www.clarku.edu/offices/its/about-its/policies-and-standards/

Product Documentation | ServiceNow. (n.d.). https://docs.servicenow.com/bundle/tokyo-application-development/page/administer/integrationhub-store-spokes/concept/zendesk-spoke.html

S. (2021, July 27). GDPR Cookie Consent Website Examples. Cookie Law Info. https://www.cookielawinfo.com/gdpr-cookie-consent-website-examples/

Student Resources | Clark University. (2023, December 1). Clark University. https://www.clarku.edu/student-resources/

What is continuous security monitoring and why is it important? (n.d.). Vanta. https://www.vanta.com/resources/what-is-continuous-security-monitoring#:~:text=Continuous%20monitoring%20can%20also%20help,better%20adhere%20to%20these%20laws.

What is India's Digital Personal Data Protection (DPDP) Act? Rights, Responsibilities & Everything You Need to Know. (n.d.). Digital Guardian. https://www.digitalguardian.com/blog/what-indias-digital-personal-data-protection-dpdp-act-rights-responsibilities-everything-you#:~:text=The%20Digital%20Personal%20Data%20Protection%20(DPDP)%20Act%2C%20passed%20in,such%20data%20for%20lawful%20purposes.

Wolford, B. (2023, September 14). What is GDPR, the EU's new data protection law? GDPR.eu. https://gdpr.eu/what-is-gdpr/