# National College of Ireland

# Project Submission Sheet

**Student Name:** Aishwarya Subramani, Ashok Kumar Ghunalan, Divyansh Anand, Jaiprakash Chandraker, Vipin Sharma

**Student ID:** 22238077, 22193561, 22240217, 22213546, 22207406

**Programme:** MSc in Data Analytics **Year:** 2023-2024

**Module:** Data Governance and Ethics (H9DGE)

**Lecturer:** 21st July 2024
**Submission Due Date:**

**Project Title:** Data Governance and Ethics CA1

**Word Count:** 5394

**I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.**
**ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.**

**Signature:** Aishwarya Subramani, Ashok Kumar Ghunalan, Divyansh Anand, Jaiprakash Chandraker, Vipin Sharma

**Date:** 20th July 2024

**PLEASE READ THE FOLLOWING INSTRUCTIONS:**

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

| **Office Use Only** | |
|---|---|
| Signature: | |
| Date: | |
| Penalty Applied (if applicable): | |

# AI Acknowledgement Supplement

## Data Governance and Ethics (H9DGE)

| Your Name/Student Number | Course | Date |
|---|---|---|
| | | |

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

## AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

| Tool Name | Brief Description | Link to tool |
|---|---|---|
| | | |
| | | |

## Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

| [Insert Tool Name] | |
|---|---|
| [Insert Description of use] | |
| [Insert Sample prompt] | [Insert Sample response] |

## Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

## Additional Evidence:

[Place evidence here]

# Data Governance and Ethics CA1

Aishwarya Subramani
*Master of Science in Data Analytics*
*National College of Ireland*
Dublin, Ireland
x22238077@student.ncirl.ie

Ashok kumar Ghunalan
*Master of Science in Data Analytics*
*National College of Ireland*
Dublin, Ireland
x22193561@student.ncirl.ie

Divyansh Anand
Master of Science in Data Analytics
National College of Ireland
Dublin, Ireland
x22240217@student.ncirl.ie

Jaiprakash Chandraker
*Master of Science in Data Analytics*
*National College of Ireland*
Dublin, Ireland
x22213546@student.ncirl.ie

Vipin Sharma
*Master of Science in Data Analytics*
*National College of Ireland*
Dublin, Ireland
x22207406@student.ncirl.ie

## I. DATA GOVERNANCE AND MANAGEMENT (EASYCARE)

### *A. Reasons for Data Governance program*

EasyCare has offices in multiple locations, including Dublin, Brussels, Madrid & Athens which makes it tough to keep data reliable and up-to-date. Offices may collect, enter, and manage data differently These discrepancies often create inconsistency and errors in the data. For instance, one office may use disparate date or currency formats or discrepancies in customer information can lead to confusion and inaccuracies when the data is aggregated or scrutinized at a corporate level. This inconsistency can affect the trustworthiness of reports, analytics, and thus business decisions.

This lack of cohesion can be alleviated by the centralized standards, policies, and procedures that a data governance program enforces across all locations. Because they have standardized the way data is entered in EasyCare, all their notes will be recorded consistently. By, Adopting uniform templates for consumer data, transaction records will avoid redundant details being entered in different styles. EasyCare can reduce variance in the collected data through compliance with such standards and validation checks so that the data collected in Dublin will be of the same standard as the data collected in Madrid. This makes business intelligence and analytics more dependable and accurate, which in return aids in the right decision-making and ultimately helps in increasing the efficiency of the business operations. EasyCare is a rapidly growing company focusing on expanding to new locations across Europe, which means that the sheer amount and richness of the collected data will grow immensely. [1] Their emergence is either a strength or a weakness to the growth of the firm: New growth opportunities New threats rivals From the concept of new growth, new opportunities avail themselves to the growth of the firm as presented in the figure below; From the perspective of new threats rivals, the growth of the below rivals threaten the growth of the firm as presented in the figure below; Lack of specifically set data management plan leaves EasyCare vulnerable to problems such as data being isolated based on its creators' preferences, data quality lacking a uniform standard, and potential violations of regulatory requirements. An effective data governance program will offer structured procedures and objectives that will govern data within an organization for precision, availability, and safety. Moreover, it shall enhance decision making processes for the benefit of the stakeholders, as it shall afford them accurate, and concise data information relating to the customers so as to enhance their satisfaction levels. Regarding the theoretical findings, it should be noted that, irrespective of the industry in question, the presence of efficient management systems is imperative in order to maintain compliance and optimal performance of an organization.

Navigating complex regulations across different countries (e.g., GDPR in the EU). It is necessary to comply with data protection laws such as GDPR considering that it can result in substantial fines and damage to reputation.

EasyCare faces the major challenge of navigating through the complex maze of regulations observed by different nations like GDPR for instance European Union. The importance of following strict data protection rules cannot be overstated because if ignored may attract heavy penalties, and damage its reputation. To address this problem, EasyCare should create a strong data governance framework that would maintain compliance with both local and international statutes thus reducing legal risks. Such a framework must include comprehensive compliance monitoring processes and regular audits conducted to verify compliance of all data processing activities with respect to relevant legislation. By constantly revising internal policies and procedures whenever new regulatory guidelines are approved, EasyCare will always stay compliant hence there will be no chances for legal breaches. The appointment of a dedicated officer or team responsible for compliance purposes ensures a focus on these matters as well as timely resolution of any issues that may arise in the future. Additionally, regular training programs targeted at employees raise awareness about the significance of keeping personal information safe and secure thereby embedding it into their daily work routine.

Incomplete record keeping because different departments use different systems or lack of integration of systems. Integrated record keeping systems help reduce double attempts, inefficiency in carrying out tasks, and sometimes even in getting the information needed in conducting tasks.

Thus, proper organization of data flows can become an important factor in the further augmentation of the infrastructure that would be beneficial for EasyCare's efficiency. There is an opportunity to achieve it by following the example of a single data platform that provides a clear integration of data from all offices. It is only through such a platform that information gathered from Dublin, Brussels, Madrid, and Athens can be compiled meaning that duplication of efforts is discouraged. Through consolidating information, it becomes easier to provide to employees the necessary and correct information so that they can make sound decisions within the shortest time possible. This symbiotic approach not only enhances the organization's operational efficiency but also increases its overall adaptability of the organization to changes within the market and the customer's needs as appreciated in EasyCare. Also, the shared information environment contributes to improved cooperation of the different divisions and branches, which results to enhancement of the integrative operation setting in Easy Care Company.

Poor data quality has an effect on strategic planning and forecasting since it brings difficulty in making any informed business decision and predicting future trends.

EasyCare's analytics, and business intelligence capabilities can be improved by using good-quality data. This is turn supports strategizing based on fully informed decisions. With the introduction of robust databases, EasyCare will improve its ability to perform extensive market analysis as well as detect emerging trends. It also assists the firm in identifying where they need to make investments with confidence of a positive return. The reliable figures about forecasts are useful for understanding the market demands during future periods that should be accommodated or supported by strategic adjustments made by EasyCare. Therefore, this would help guide well-informed actions in line with the long-term goals and objectives of the organization thereby promoting growth and competition advantage attainment. By emphasizing on data quality, there is strength in the overall strategic planning process at EasyCare while driving an evolution towards being data-driven across all organizational levels.

Customer's trust can be lost because of data breaks and misrepresentations. Security and accuracy are the two major aspects that customers look forward to in their personal and financial information.

Moreover, it greatly builds up data security as well as privacy measures which are important in creating customer trust. By having strong policies on data protection coupled with transparent practices, EasyCare can assure them that their personal details and financial information is being managed securely without any form of inaccuracies. This should involve airtight encryption of data, periodic security audits, and a clear understanding of how customer data is used and safeguarded. These steps serve two purposes; one they prevent breaches as well as inaccuracies while at the same time showing the commitment of Easy Care to keeping customer information safe. As consumers' confidence in the company's ability to secure their information increases, so does their overall satisfaction and loyalty towards EasyCare increase. The foundation for long-term relationships with customers built over time is based on this trust such that repeat business comes about due to this trust through positive word-of-mouth referrals thereby enhancing corporate reputation and resulting in success in the marketplace.

### *B. Relevant roles which should be considered in Data Governance Program*

*1) Data Governance Council:* Data Governance Council supervises data governance program, establish guidelines and standards, and guarantee alignment with business goals. Council members are made up of senior officials plus vital stakeholders from different business units to provide a policy direction and address any disputes. Data governance is one of the important fields that defines the strategies, procedures, and solutions, essential for the proper management of information resources in an organization.[2]

*2) Chief Data Officer (CDO):* CDO heads the data governance program ensuring it fits into those grand strategies given by the entire corporate body. The CDO develops the framework for governing all these activities through securing executive support and overseeing its implementation.

### *C. Important features of a Data Governance model*

*1) Policy and standards development:* This area is responsible for setting out guidelines that ensure data management practices are consistent and comply with regulations. Policies should touch on topics like data privacy, quality, access and usage while standards will touch on how to gather, keep, process or even share the same.

*2) Data quality management:* Data profiling, cleaning and enrichment processes need to be put in place in order to continuously monitor and improve the quality of data. Regular checks are important because they minimize chances of business being affected by bad data.

*3) Data stewardship:* The major role played by these stewards is to ensure that data is used correctly and accurately maintained. Data stewards play a very crucial role in ensuring there is no compromise on the correctness of information held as well as finding solutions to any problems related with it. They facilitate communication between business units and IT.

*4) Compliance and risk management:* Mitigate risks by ensuring all activities dealing with data are as per legislative requirements. This includes among other things implementing measures for protecting ones' own personal data collecting regular audits as well as maintaining comprehensive records about their processing activities.

*5) Performance Measurement:* It defines metrics and KPIs to evaluate the appropriateness of the data management program and know which areas to improve. Performance metrics should be about data quality, compliance, data utilization, and overall program effectiveness Regular reviews and continuous improvement initiatives help enhance the data governance framework.

*6) Data Architecture and Integration:* Develop a holistic data architecture that supports a company's integration needs across systems and platforms. Well-designed data architectures make sure that information is accessible, consistent and secure. They also enable interoperability between different sets of information thus establishing seamless flow of data across an organization.

### *D. John Ladley's Eight-phase approach for implementing data governance*

*1) Phase 1 - The Program and Project Initiation:* It is crucial to address stakeholders concerns by establishing clear goals and involving top management. This phase involves defining the boundaries, goals and benefits of data governance program. Securing an executive sponsorship is as important as creating a project time table that includes the necessary milestones, resource allocation & schedules. Additionally, in order to ensure that the stakeholders accept the programme, it is useful to apply convincing business arguments to show that the programme is to the benefit of business.

*2) Phase 2 - Organizational Commitment:* To address stakeholder concerns in this phase, it is important to establish a council for data governance and delegate specific roles to its members. Developing a robust communication system is a key to keep stakeholders informed and engaged. Additionally, conducting workshops and meetings is important to highlight the importance of data governance in relation to commercial activities.

*3) Phase 3 - Data Governance Framework Development:* This phase involves the process of establishing a framework that will cover all the aspects of the Data Governance program. To address the concerns of stakeholders, this phase entails developing strategies, standards, and guidelines that define how information should be processed. There is a need to define processes, several roles, and responsibilities that are associated with data governance and to define how enterprise-wide rules should be managed. These steps include, but are not limited to the development of quality assurance policies, stewardship protocols and oversight systems to monitor compliance in case of deviations from the set quality benchmarks.

*4) Phase 4 - Data Management and Stewardship:* This phase focuses on ensuring that data stewardship and management are efficient. This entails appointing data stewards and implementing data quality management as ongoing practices. Additionally, assessment templates for managing data and training the employees on how to use them are important steps in this phase. Moreover, there is a need to establish methods for improving the quality of data which is vital for achieving Data Management and Data Stewardship objectives.

*5) Phase 5 - Data Governance Implementation:* This phase deals with a smooth implementation and adoption process to meet the stakeholders' concerns. This phase requires initiating the governance framework, informing stakeholders, and providing support throughout the process. To manage information consistently, there should be a proper plan of implementing data governance across the organization and all its divisions. Some of the recommendations for implementation include: Progress should be closely monitored to allow timely rectification of any barriers to the process.

*6) Phase 6 - Data Quality Management:* This phase ensures high quality in data holdings to respond to stakeholder demands. During this phase, measures are put in place for every company system in order to meet the quality and usability of data. Procedures for establishing the framework for evaluating the quality of the data are important and should be instituted to facilitate monitoring by different stakeholders. Moreover, it is essential to control the quality of information to be used in decision-making by having regular audit checks on the quality of the relevant information which should be followed by improvement plans in case of gaps identified during the audit.

*7) Phase 7 - Compliance and Risk Management:* This phase aims at addressing stakeholder concerns on compliance with regulations and risk minimization. This phase includes the formulation of the necessary policies and procedures for review and implementation of compliance as well as the handling of any arising problems during the review period. It is also important to determine and formulate different approaches on how to address and prevent possible data risk factors. Also, documentation of all information processing activities is required in order to create transparency and ensure that accountability has been achieved.

*8) Phase 8 - Performance Measurement and Continuous Improvement:* This phase involves identifying and responding to stakeholder concerns regarding the success and continuous improvement of the data governance program. This focuses on setting performance targets and tracking them with regard to effectiveness and the areas that require corrections. Here, it is important to point out that Data Governance Framework is constantly reviewed to allow for improvement. Moreover, it is important to obtain and incorporate stakeholders' views to make changes based on these views that are essential to maintain order within organizations of the corporate sector.

## II. Data Governance and Management (EasyCare)

### *A. Most significant legal requirements*

Pursuant to my role as Clever Soft's Data Protection Officer (DPO) it is my responsibility to guarantee complete adherence to Ireland and the EU's highly protective data and privacy legislation. Being an organization located in Dublin, Ireland, Clever Soft has to follow the General Data Protection Regulation (GDPR) requirement as a company that processes the personal data of EU citizens, regardless of the company's location in the Global. PWD mentions that personal data should be processed in a legal manner, and in a manner that is neither unfair nor unjustly compromising to the data subject. In the data minimization principle, it propounds that collection of data should only be done if there is a lawful, genuine need to do it. Most importantly, personal data has to be processed in a way that it is secure from accidental loss or damage or even from being accessed by unauthorized persons.

Supporting the GDPR, specific legislative acts of Ireland – Data Protection Acts 1988 to 2018 – contain national specific requirements and restrictions. [3] These include the data subjects' rights that include rights to the data, right to obtain copies and to edit the data, right to erasure of the data, and right to limit processing of the data and right to data portability. The implementation and regulation of such laws in Ireland is done by Data Protection Commission (DPC) which also deals with complaints concerning data protection.

With regards to the above highlighted legal frameworks, it is critical that Clever Soft institute an effective Data Protection Policy. It can be considered as an essential legal act including the company's adherence to the GDPR and describing specific actions in the case of the collection, processing, storage, and disposal of personal data. It defines the meaning of personal data and the types of processing activities that take place in the organization; defines the roles and duties of the employees such as the Data Protection Officer in relation to data, and requires organizations to apply the security measures such as encryption, pseudonymization, and access control to prevent data breaches.

An effective management of data processing activities involves assessment of data processing activities which is done through recording of processing activities (ROPA) that involves the records you have kept about the personal data, how it is processed, to which parties it is disclosed, and for how long it will be stored. However, for the activities that would be considered as significantly risky to the data subjects, Clever Soft carries DPIAs to establish and control the risks as follows.

Data subjects under GDPR are given several rights such as the right to request their data and its rectification, erasure if the data is not required for processing, stuck in a transferable form. Presently, Clever Soft has put in place measures to deal with Data Subject Access Requests (DSARs) in the most efficient way possible and within the one-month GDPR provision. The company also guarantees that consent for data processing is acquired voluntarily, precisely, and unambiguous with the permission of the individuals, also, it offers chance for the individuals to revoke their consensus at any time.

It is important to note that Clever Soft provides data security measures relating on the technologies and organizational procedures for personal data protection. Some of them include conducting orientation of all the organization's employees on the principles of data protection and security measures to be followed and drawing up and implementation of a response plan to act in the event of data breach.

This is done through elaborately drafted data processing agreements that both parties sign and which hold the third-party processor to GDPR compliance and clearly map of the roles and duties of all the associated parties. Clever Soft has guidelines in cases of data breaches that include the identification of the breach, reporting the issue, as well as handling it. This also involves reporting the breach to the DPC within 72 hours of the organization's notification of the breach and communicating to the affected data subjects within 72 hours if the breach is likely to result in high risk to their rights and freedoms.

Other main provisions of law under https://gdpr-info.eu/, [4] which include lawfulness of processing (Article 6 GDPR), rights of data subjects (Articles 12-23 GDPR), as well as the data protection by design and by default (Article 25 GDPR), also helps Clever Soft in the implementation of data protection laws. These provisions require that legal bases for data processing have to be stated, that processes for assessing and managing data subjects' requests have to be made clear, that privacy considerations have to be incorporated into the design process in the product and that the privacy default settings must be the best.

Under GDPR, companies are required to designate a Data Protection Officer (DPO) if the organization's processing activities are relating to the offering of goods and services and comprised of large scale, systematic monitoring of data subjects. Clever Soft has its DPO to coordinate compliance and provide recommendations when there is a question of data protection responsibilities or contact with the Data Protection Commission.

Data transfers to third countries outside the EU are regulated in accordance with GDPR's Chapter V and imply an assessment of the transfers and implementation of the relevant guarantees for the transfer of data to third countries, including standard contractual clauses or binding corporate rules adopted by Clever Soft.

Therefore, GDPR and Ireland's data protection laws should by followed by Clever Soft to ensure that the privacy of individuals is protected, trust be established between the organization and its clients and partners as well as to avoid compromising the damaging impact if data breaches are to occur. As a result of proper policies and procedures in policy formulation, implementation, and compliance, Clever Soft manages personal data prudently and with adequate safety and as provided by the laws and standards in data protection.

### *B. Roles and responsibilities of a data controller and a data processor*

CleverSoft is planning to hire a data processor, so it is important to understand the different roles and responsibilities of both data controller and data processor according to General Data Protection Regulation (GDPR) [5]. These roles handle how the personal data managed and make sure both the parties follow legal requirements to protect data privacy.

- ***Data Controller***

A Data controller is an organization that defines the purpose and methods of processing data. The data controller determines why personal data is collected and how it will be used [5]. Below are the responsibilities of data controller.

*1) Security Measures:* Data Controller must ensure all the data are processed by following GDPR. It is responsible to secure legal justification for data processing, such as consent, contracts and legitimate interest [6]. Data Controllers are resposible for maintaining Contractual Agreements with data processors, which guides the data processing activities and responsibility to ensure it is following GDPR [5].

*2) Risk Management:* If the processing of data poses risks to individuals, the data controller is responsible to conducting Data Protection Impact Assesments (DPIA to estimate and mitigate potential risk [6].

*3) Retention & Record Keeping:* Data Controllers must maintain logs for data processing activities and able to explain the purpose and retention period [6].

- ***Data Processor***

A Data Processor is an entity that processes personal data on behalf of Data Controller. It does not determine the purpose of processing but acts under the control of Data Controller [6]. In CleverSoft's case, if the company decides to engage Data Processor, this entity will handle data according to controller's specifications. Below are the responsibilities of a data processor.

*1) Processing Data on Instructions:* Data processor should strictly follow the instruction provided by the Data

Controller for processing the data, if any deviation proper authorization is required from data controller [5].

*2) Security Measures:* Data Processor is responsible to protect personal data from unauthorised access, loss or breach. This enables access control, encryption and security audits [5].

*3) Sub-Processors:* Incase any sub-processors are involved in assisting with data processing, written approval should get from controller in prior and also it should follow GDPR [5].

*4) Data Return & Deletion:* Once the processing contract is expired, the processor must return or discard the personal data as per the contracts signed with controller [5]. This make sure the data is handled properly after processing.

In summary, CleverSoft should clearly define the roles and responsibilities of data controller and processor to ensure the data protection practices, which builds trust & security in handling personal data.

### *C. Lawful Data Transfers for Cleversoft*

CleverSoft plans to transfer data to the United States and the United Kingdom, it must follow the General Data Protection Regulation (GDPR), which implies rules for collecting, processing, storing and transferring personal data. Ireland's Data Protection Act 2018 complements the GDPR and to transfer data outside the borders of European Economic Area (EEA) are permitted only if they comply with the data protection standards [7]. Also, it is recommended to explore the legal mechanisms and the potential implications for the company to legally transfer the data.

#### *a. Data Transfer to the United States*

- *Mechanisms for Lawful Data Transfers*

CleverSoft can use the below mechanisms to ensure the compliance with GDPR standards to transfer data lawfully to the United States.

*1) Adequacy decision:* It is the basic mechanism to consider when transferring personal data to International Organisation, which was invalidated in 2020. The European Commission is working on new framework called EU-U.S. Data Privacy Framework, which helps to address the privacy concerns and simplify data transfers. In the absence of Adequacy decision, GDPR allows the transfer based on the safeguards like Standard Contractual Clauses (SCC) and Binding Corporate Rules (BCR) [8].

*2) Standard Contractual Clauses (SCC):* It is an substitute contract for Adequacy decision, proposed by the European Commission to ensure the data is transferred outside the borders of EU [7]. Contracts between CleverSoft and its US based partners should include SCC, both the parties should obey GDPR compliant data protection practices.

*3) Binding Corporate Rules (BCR):* It is an internal policy adopted by the multinational companies that allow intra group companies to transfer their personal data across borders. [8] Cleversoft can develop and implement BCR for its affiliates and US subsidiaries, assuring that every company in their corporate group follows the same data security standards.

- *Some implications for CleverSoft to Transfer Data to United States*

*1) Legal and Compliance Cost:* To implement SCC and BCR for CleverSoft considerable amount of administrative cost and legal works are associated. Regular audits and compliance checks are required to ensure adherence [7].

*2) Data Security & Privacy Risk:* Invalidation of Adequacy decision shows the risks and uncertainties in transferring the data between EU and US. CleverSoft needs to stay updated with legal developments and ready to adapt to new rules which will be introduced in future [8].

*3) Operational Impact:* Data transfers may slow down because of careful review of contracts and compliance. It is important to upskill all the employees and make sure they understand and follow data privacy regulations [7].

#### *b. Data Transfer to the United Kingdom*

Data transfer from European Union to United Kingdom are allowed under the European Commission's Adequacy decision, it is the primary mechanism for data transfer. This decision recognizes the data protection standards are similar for the both. Despite Brexit, the data transfers are still permitted and the safeguards for these transfers have not changed [9]. Because of this adequacy decision, CleverSoft does not need to implement additional safeguard mechanisms like SCC or BCR for the data transfer between EU and UK [9].

- *Some implications for CleverSoft to Transfer Data to United Kingdom*

*1) Stability & Predictability:* The current adequacy decision provides a clear and trustable regulations for transferring data without legal and operational issues. Also, CleverSoft should always monitor any changes to the existing rules and be prepared to implement SCC and BCR if necessary [9].

*2) Continued Compliance:* CleverSoft must ensure that it follows the GDPR data standards, inspite of adequacy decision. Constant monitoring and assessments regarding the impact on data protection are needed to maintain compliance [9].

*3) Business Continuity:* CleverSoft can transfer the data without any interuptions to UK partners by using the adequacy decision. It also minimises the additional paper work and contractual protections [9].

In summary, to ensure the lawful data transfer from EU to non-EU countries like US and UK, CleverSoft must implement mechanisms like SCC and BCR. The adequacy decision simplifies the data transfer for UK. CleverSoft must remain proactive in monitoring the changes in data protection framework to ensure secure and legal way of handling personal data.

## III. Ethical Issues Pertaining to Data

In this world of rapid change and volatility, technology is catching up at great pace. It implies that businesses are gathering, preserving, and examining vast volumes of data. However, significant ethical questions around security, privacy, and the use of information accompany such practices. Maintaining people trust and ensuring that everyone benefits equally from technology requires more than simply executing by the law; it also requires to follow ethical standards. Businesses can navigate these challenging situations by applying and adopting ethical frameworks.

Let's dive into an important ethical philosophy which is associated with German philosopher, Immanuel Kant, called Deontological ethics. This philosophy emphasizes on following guidelines and obligations, irrespective of the result. When it comes to data management, it implies businesses must obtain full permission from people before utilizing their data and strictly respect their right to privacy. Being transparent is essential, businesses should disclose what information they gather, how they gather and use it, and with whom they share it. They should respect people privacy and independence by protecting personal information from unwanted access and breaches by placing a high priority on data security. This ethical approach translates into practical guidelines for businesses collecting data, they should make sure users are properly informed about the purpose and method of data collection. To give people awareness and control over their personal information, it is crucial to have clear permission processes and privacy regulations. By considering users as people and not just as data providers, this not only aligns with regulations but also promotes trust among the businesses and the users.

According to this theory, the main objectives should be justice and equitable opportunities for all members of society. Businesses must give a thought about how their data policies affect different groups when it comes to data management, mainly those who might be less powerful or privileged. Companies need to determine if the collection, archiving, and use of their data can accidently result in discrimination or increase disparities that currently exist.

Businesses need to make sure that everyone benefits equally from their usage of data to carry out the social justice strategy. They must ensure that everyone, not just a select few with privileged access, can benefit from new data tools and technology developments. Vulnerable population need to have their security and privacy protected, businesses should go beyond what is necessary to protect these groups and prevent misuse or data breaches.

Companies must carry out ethical audits of their data management procedures to ensure they are operating ethically. A deontological ethics audit would verify that they have effective security measures in place, that their consent procedures are clear and informed, and that their privacy policies are compliant with the law. And alternatively, an audit with a social justice focus would evaluate their data practices to see whether they are equitable, if they help all groups equally, and if they might accidentally harm underprivileged groups.

Firms should begin their audits by examining and amending their privacy policies to ensure that privacy policies clearly state the types of data being collected, how they will be used, and the rights users have over their data, firms should begin these audits by examining and maybe amending their privacy policies. For consumers to make educated decisions, businesses must communicate clearly and provide information in a way that is simple to comprehend for all.

Businesses must also constantly review and upgrade their security protocols to safeguard customer information from emerging threats and hazards. This supports their responsibility to protect the privacy of individuals.

Audits must determine if data practices increase or decrease societal inequality from a social justice standpoint. Businesses should take steps to guarantee that their data strategies do not accidentally discriminate against any group and should actively attempt to give people equal access to and benefits from the use of data. This entails carefully evaluating how their data approaches impact various groups and modifying their approaches to encourage equality and inclusivity.

It is important to provide specific protection to communities that are excluded. Organizations should implement additional measures to reduce the risks that these groups face, ensuring that their data practices avoid worsening pre-existing vulnerabilities. By concentrating on safeguarding those who are most in need, businesses demonstrate that they take their ethical responsibilities seriously and contribute to the development of a more equal and just technology environment.

In conclusion, there are a considerable number of ethical issues raised by the rapid rate at which technology is developing. Businesses can successfully handle these issues by including the perspectives of social justice and deontological ethics into their data practices. Deontological ethics stresses about following laws and responsibilities, particularly when it comes to maintaining privacy and about being open how data is used. And with the inclusion of the social justice approach dedication to equity and providing equal opportunities for everyone is achieved, and businesses must consider the effects of their data practices on various groups and seek to eliminate any inequalities thereafter.

Companies shall make sure their data practices not only conform with legal requirements but also maintain high ethical standards by conducting comprehensive ethical audits based on these principles. This methodology encourages user trust, promotes for equal distribution of data benefits as well as promotes a more just and moral technological environment. In the end, businesses can ethically use technology to further their corporate objectives and the interests of society at large by adopting ethical data management practices as aforementioned above.

## References

[1] "Inventory Management System for Self-Governance of a poultry slaughterhouse," IEEE Conference Publication | IEEE Xplore, Aug. 09, 2023. Available: https://ieeexplore.ieee.org/abstract/document/10276894?casa_token=PT6-_JxzQIAAAAAA:Q00HXIInWjb5I5e0L7Q8wJdBiJXuevc10MhCvLe2OmUJ21pfd1pXKz2ZlbkDbrDjeeH1qohIGIo

[2] Navigating data governance in the telecom industry. (2023, November 15). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/10414472

[3] V. Timon, Z. Deasy, S. O'Donnell, and J. Drennan, "Data Protection Laws and Regulations Ireland 2023-2024," International Comparative Legal Guides International Business Reports, Jul. 20, 2023. Available:

https://iclg.com/practice-areas/data-protection-laws-and-regulations/ireland

[4] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects | European Data Protection Board. (n.d.). https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en

[5] Data Privacy Manager, "Difference Between Data Controller and Data Processor," Data Privacy Manager, [Online]. Available: https://dataprivacymanager.net/difference-between-data-controller-and-data-processor/ [Accessed: 19-Jul-2024].

[6] GDPR.eu, "Data Controllers and Processors," GDPR.eu, [Online]. Available: https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/ [Accessed: 19-Jul-2024].

[7] Data Protection Commission, "Transfers of Personal Data to Third Countries or International Organisations," Data Protection Commission, [Online]. Available: https://www.dataprotection.ie/en/organisations/international-transfers/transfers-personal-data-third-countries-or-international-organisations [Accessed: 19-Jul-2024].

[8] GRCI Law, "EU-US Privacy Shield Ruled Invalid: What Now?" GRCI Law, [Online]. Available: https://www.grcilaw.com/blog/eu-us-privacy-shield-ruled-invalid-what-now [Accessed: 19-Jul-2024].

[9] European Commission, "Brexit," European Commission, [Online]. Available: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/brexit_en. [Accessed: 19-Jul-2024].