Data Governance and Ethics (H9DGE)

Akimuddin Aslam Shaikh
School of Computing
National College of Ireland
x22123245

Mohammed Musthafa Keloth Poyil
School of Computing
National College of Ireland
x23162112

Ebin Sujin
School of Computing
National College of Ireland
x23205814

Alan Thomas
School of Computing
National College of Ireland
x23188944

I. Question 1: Data Governance and Management for EasyCare

EasyCare, a growing insurance and financial planning company needs a robust data governance program to ensure following government data policies, data integrity, safeguard customer trust, and support its operational and strategic goals. A data governance program will provide a structured approach for managing data across departments, allowing EasyCare to align its data practices with regulatory standards, improve data quality, and enhance operational efficiency. By establishing clear policies, roles, and controls, this program will help EasyCare utilize data as a strategic asset while maintaining customer privacy and legal compliance.

A. The need for data governance

A data governance program is essential for EasyCare due to the complexity and sensitivity of the data it handles in the insurance and financial planning industry [1]. Below are the key data challenges EasyCare faces and how a data governance program would address them:

1) Data Security and Risk Management

EasyCare deals with the sensitive data of customers that may prone to unauthorized access or potential security breaches. To overcome this issue, data governance program, such as data encryption, role-based access, multi-factor authentication, and continuous monitoring of security measures can be established. This approach will allow EasyCare to safeguard sensitive customer information effectively.

2) Regulatory Compliance and Data Privacy

EasyCare is required to comply with the General Data Protection Regulation (GDPR) and other local data protection laws in European countries. Non-compliance can result in hefty fines and damage to the company's reputation. To resolve this, data privacy policies need to be established that align with GDPR requirements. It ensures secure collection, storage, and processing of customer data, limiting data access based on roles. Data stewards and a compliance monitoring team will oversee these practices, helping EasyCare maintain regulatory compliance across its entire data lifecycle.

3) Building Customer Trust

EasyCare's growth is highly reliant on customer trust, particularly when managing personal and financial data. Customers need assurance that their data is safe and transparent. By implementing a data governance program with transparent data policies, high security standards, and reliable data handling practices, EasyCare can improve its reputation for protecting customer data.

B. Roles and responsibilities in the Organisation

Easycare needs to established well-defined roles within organisation that will contribute to various aspects of data management [2].

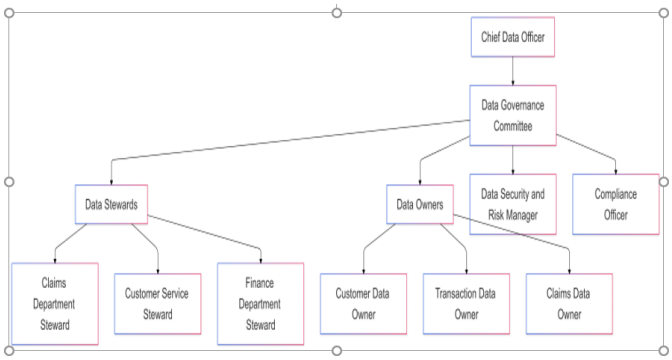

Fig. 1. Role and Responsibilities.

The prominent responsiblities lies on the shoulder of Chief Data Officer as they set the strategic vision for data management, ensuring alignment with EasyCare's business objectives and lead the development of policies, supervise data-related functions, and ensure regulatory compliance as depicted in Fig. 1. Being the head they ensures that EasyCare's data assets are governed, protected, and utilized securely across departments. The data governance committee needs to be established that include representatives from IT, Legal, Compliance, Finance, Marketing, and Customer Service to ensure all perspectives are considered. Initiating data governance program accross department will ensures that policies meet organizational needs and comply with industry-specific requirements. The role of data stewards would include managing the data quality and integrity in their respective department(e.g., claims, customer service, finance). The are responsible for maintaining high data standard accorss the department, ensuring that data used for business operations and decision-making is reliable. The role of Data owners will include accountabilty for specific data assets, such as customer data, transaction data, or claims data. They determine access

permissions, approve data sharing, and ensure data complies with relevant policies. They are responsible for safeguarding data and controlling access, aligning with EasyCare's need for secure, regulated data use. Data Security and Risk Manager roles are to safeguard EasyCare's data assets from unauthorized access and breaches. Responsibilities include developing and enforcing data security policies, managing access controls, and conducting regular security audits. This role is critical to protecting customer data given the sensitivity of the financial and personal data.

C. Data Governance Operating Model

A data governance operating model should provide a structured approach that meets both business and technical requirements [3].

1) Data Governance Framework and Structure

A well-defined governance structure includes features that outlines roles, responsibilities, and hierarchical reporting. The main reason is that it Establishes accountability and authority at each level, and this framework enables coordination across departments, aligning data management efforts with business goals. Chief Data Officer, Data Governance Committee, Data Stewards, and department-specific Data Owner are the key players that ensures policies meet both regulatory and business needs.

2) Data Policies and Standards

Data policies are the top priority that includes data handling, storage, access, and sharing practices. These standards help align operational needs with legal requirements, like GDPR. It can be done by developing specific policies for data privacy, security, quality, and retention, enforced by department heads and Data Stewards that meets legal requirement.

3) Data Stewardship and Ownership

Data governance standards should enforce Defined stewardship and ownership roles across departments. It ensures data accountability and promotes data quality at the departmental level. Department-specific Data Stewards monitor data handling and quality within their areas. Data Owners ensure policies are followed, addressing both operational and technical needs.

4) Data Security and Access Controls

Role-based access and security protocols should be established to protect sensitive financial and personal data. The primary reason is to prevents unauthorized access, ensuring data security and compliance with industry regulations. IT and Data Security teams should manage encryption, multi-factor authentication, and access permissions based on employee roles.

D. John Ladley's 8-phase Approach

To implement a data governance program, John Ladley's 8-phase approach provides a comprehensive roadmap that address key stakeholder concerns at each phase [1].

1) Phase 1- Strategic Alignment

Building stakeholder consensus on the data governance value and its alignment with companies business objectives by conducting workshops and briefings with stakeholders across departments.

2) phase 2- Planning and Funding

Gain funding approval from senior leadership by linking investments to compliance and risk mitigation. Emphasize the long-term ROI of compliance, reduced data errors, and efficiency gains.

3) phase 3- Program Development

Form the Data Governance Committee and assign data-related roles to establish the foundational structure and framework of the data governance program. Ensuring that governance standards are feasible and aligned with current practices will alleviate these concerns about the impact on the workflows.

4) Phase 4- Communications and Change Management

Host training sessions and workshops to increase awareness of data governance policies that will develop a communication strategy to promote the program within the organization.

5) Phase 5 - Governance Framework and Data Management Processes

Set up a Data Quality Management System, using automated tools that implement data management processes including data quality checks, access control, and regular audits. Implementing phased rollouts with pilot programs will ease the worry about the complexity and cost of new processes.

6) Phase 6- Operationalization and Execution

Launch a Data Stewardship Program in each department to monitor data adherence, oversee data usage, and resolve issues. Ensure each department understands the value of compliance for their operational needs.

7) Phase 7- Sustainment and Monitoring

Develop a Data Governance Scorecard to track key metrics and report progress to conduct regular reviews and audits to monitor compliance with governance policies. Assure stakehoders by showing measurable improvements in data quality, compliance, and risk reduction.

8) Continuous Improvement and Program Evolution

Establish a Governance Feedback and Improvement Cycle to ensure the program evolves with EasyCare's business needs, regulatory changes, and technological advancements.

II. Question 2: Data Protection Requirements for IT Systems

***Abstract*—This paper outlines some of the major legal requirements for data protection that ITSystems needs to observe while designing its framework for data management. Being an IT services provider operating from Ireland and offering services to the EU region, IT Systems is bound by the laws of the region and thus, GDPR and the Irish Data Protection Act 2018 are the ORG requiring the consent and defining the mechanics of withdrawal. This report outlines the duties and obligations of ITSystems if the organization contracts a cloud provider as the data processor together with analyzing adequate methods of transferring data to third nations. Finally, the guidelines on how to maintain continued compliance in the constantly changing data protection environment are provided.**

A. Introduction

IT Systems is an IT service provider located in Dublin hence Its operations are legally bound by the Irish and the laws governing the European Union on data protection. Observance with these regulations is essential not only from legal point of view but also from the perspective of trusting activities with clients and for the sake of protecting personal data which are processed by ITSystems. This paper proposes to analyze and explain GDPR and Irish Data Protection Act obligations to an organization deciding on a cloud solution, the controller-processor relationship as the working model with a cloud provider, and the legal tactics for international data relocation beyond the EU.

B. Overview of Legal Requirements for Data Protection

Data protection needs for IT Systems are primarily drawn from GDPR and the Irish Data Protection Act 2018. They provide main guidelines that concern the collection, processing, storage, and sharing of personal data.

1) GDPR Compliance:

GDPR establishes a wide range of rules with strict specifications as to the processing of personal data within the scope of the EU. Key obligations for ITSystems include:

i Lawful Basis for processing: ITSystems must ensure that the founding of data processing activities is legal and which entails the consent of the data subjects, carrying out of obligation arising from the contract, compliance with legal requirements or pursuit of legitimate interest [4]. Every basis has its conditions; for example, consent has to be unambiguous, active, and informed where personal data relating to a sensitive matter is been processed.

ii Data subject rights: GDPR provides the following rights to data subjects where they have the right to request a copy of the data, to rectify the data, to have it erased, to port it from one data controller to another [5]. ITSystems has to be having measures to address the requests in proper way and also in the said time-frame according to each right.

iii Data minimization and purpose limitation: Data minimization needs to be complied with by ITSystems so that only data essential to its defined and reasonable objectives is processed. The purpose limitation principle forbids the use of collected data for purposes other than the cited one unless a new legal ground will be provided and possibly data subject information.

iv Security of processing: Regarding to the GDPR's Article 32, ITSystems has certain duties to use technical and organizational security measures to protect processed data. These may include, dataencryption, access controls, regular-security assessments, secure storagesolutions [6]. ITSystems should also have a data access control policy to help with processing of data and the systems should also regularly be audited.

v Breach notification: GDPR requires that in case of a data breach, ITSystems notify the Data Protection Commission (DPC) within 72 hours [7]. This means that ITSystems has to have an incident response plan and that an assignment of essential tasks in the dependency of an incident is necessary to be able to handle these vulnerabilities.

2) Irish Data Protection Act 2018:

The other is the Irish Data Protection Act 2018 which augments GDPR and outlines other specific regulation standards for firms in Ireland. It establishes particular rules and sanctions for the Data Protection Commission (DPC) [5]. IT systems are obliged to respect the requests of the DPC and collaborate on investigations or audits.

3) Implementing Compliance Measures:

ITSystems can adopt the following best practices to ensure compliance with GDPR and Irish regulations:

i Privacy by design and default: Data protection should therefore be incorporated into the architecture of ITSystems by default. This approach entails that data protection is a factor even before systems are designed and constantly throughout operations.

ii Data Protection Impact Assessments (DPIAs): DPIAs are important in the assessment of risk in relation to high risk processing activities. With DPIAs, ITSystems can detect privacy risks in good time, particularly whether new technologies or services are used.

iii Staff training: It can be noted that constant training for employees help to familiarize all workers of the company with the principles of data protection. Staff should be aware of GDPR of the given requirements and trained on policies that they met, for example on data breach or on data subject's rights.

C. ROLES AND RESPONSIBILITIES OF DATA CONTROLLER AND DATA PROCESSOR

Whenever ITSystems outsource data processing to a cloud provider they need to identify roles and responsibilities with respect to GDPR.

1) Data Controller

ITSystems works as a data controller which means that it defines guidelines about the ways and purposes of personal data

processing. This responsibility entails the following; adherence to the GDPR principles regarding the processing of personal data, and respect of the data subject rights [4]. ITSystems has to determine the lawful ways of data processing, data protection and management of the breaches.

2) Data Processor

A cloud provider, as a data processor, processes data on the ITSystems side and shall observe GDPR directions on the protection and confidentiality of data. The processor also must act upon the instructions given by the controller, ITSystems, and cannot process the data for their own benefits [6].

3) Data Processing Agreement (DPA)

To regulate this kind of connection ITSystems ought to sign a Data Processing Agreement (DPA) with the cloud provider. The fact of that this is a business-critical, customer-facing service means that obligations for HSoV, including data handling practices, security requirements, incident reporting, and Interactions with ITSystems' data protection policies must be spelled out in this agreement. The DPA makes certain that both the companies involved are responsible for the protection of information.

D. LAWFUL DATA TRANSFERS TO THE UNITED STATES AND THE UK

While doing business, the ITSystems might have to migrate or share personal data to a country in the EU. There, for this reason, it is necessary to employ legal methods to work with data transfers that would coincide with GDPR standards.

1) Data Transfers to the United States

Transfers of data to the United States deserve special protection on the grounds that US privacy laws are not akin to the GDPR. ITSystems can employ SCCs, which are legal that offer legal requirements that the data processor must meet to protect personal data [7]. Also, for ITSystems it should be important to produce a Transfer Impact Assessment, which will point to the fact of possibility of the US authorities' surveillance due to the American laws. In essence, ITSystems can eliminate such risks by applying higher level of security measures like data encryption if depending on circumstances it becomes necessary.

2) Data Transfers to the United Kingdom

As of today the United Kingdom has an adequacy status in the EU which enables personal data to be transferred freely with further requirements. However, such adequacy status may vary in the future and therefore ITSystems should always consider the future changes in regulations. Where such a scenario arises, ITSystems may transition to the use of SCCs or other means through which data transfer is legal.

3) Implications of IT Systems

Data privacy compliance with legal disposition of trans-border data transfer needs constant review of the legal developments and periodic legal audit of the transfer mechanisms. ITSystems should have procedures of monitoring changes in regulations so as to adjust their policies.

E. CONCLUSION

In accordance with GDPR, the Irish Data Protection Act, and the legal data transfer mechanisms, it is crucial for IT-Systems . However, through implementing Privacy by Design, DPIAs, staff training, and having a proper data processing agreement with ITSystems data processors are effectively handled. Scarlett: Owing to the fact that the data protection laws are still being developed, ITSystems must remain keen.

III. QUESTION 3: ETHICAL FRAMEWORKS FOR IT SYSTEMS

A. Deontological Ethics (Duty-Based Ethics)

Based on the philosophy of Immanuel Kant, deontological ethics focus on the concepts of duty, obligation, and rules. An action is considered right only if it follows certain rules or principles, regardless of the consequences [8]. In data management, deontological ethics emphasize respecting the rights of data subjects and complying with data protection laws, such as the GDPR, which imposes prescriptive mandates on how data must be treated [9].

Example Use in an Ethical Audit: A deontological approach in an audit assesses if IT systems respect data subject rights consistently. For instance, there should be no failure in facilitating the right to consent, access, and be forgotten. Here, the audit evaluates whether robust data governance policies exist and are being enforced based on rule-based standards [10].

B. Utilitarianism (Consequentialist Ethics)

Utilitarianism, a form of consequentialism, determines right from wrong by focusing on outcomes. In data ethics, this means assessing decisions based on their impact on everyone involved, including customers, employees, and society. The goal is to make data-driven decisions that provide more benefits (such as improved services or policy insights) while minimizing harm, such as privacy violations or data commodification [11].

Audit of IT Systems: Utilitarian ethics would assess whether data is collected and used in a manner that benefits all parties. For example, data use should not lead to discrimination, profiling harm, or other negative impacts. This audit highlights potential harmful effects of AI algorithms, data analytics, and profiling, which could result in biases or privacy infringements [12].

C. Conduct an Ethical Unit Test with These Theories

1) Deontological Audit Components

- **Policies & Compliance:** Check if the IT systems have sufficient data governance policies and rules that align with GDPR and other applicable data protection legislation [9].
- **Upholding User Rights:** Verify whether mechanisms are in place to facilitate data subjects' rights, such as the ability to access or remove their data [10].
- **Consistency in Data Handling:** Assess whether approaches provide for consistent, ethical data use across departments and prevent arbitrary or unauthorized data use [13].

2) Utilitarian Audit Components

- **Stakeholder Impact Assessment:** Evaluate the effects of data use on stakeholders, analyzing potential risks and benefits for users [11].
- **Algorithm and Analytics Impact:** Examine if analytics and AI algorithms respect privacy rights and avoid harm. Regular checks ensure fairness and prevent bias in decision-making across sensitive categories [12].
- **Data Practices with Social Benefit:** Ensure data use benefits society by providing insights without compromising individual privacy. Data analysis should contribute to societal good [13].

D. Bridged Insights on Ethical Recommendations for IT Systems

- **For Deontological Ethics:** IT systems should advance data governance policies that strictly comply with legal data protection regulations. Policies should align data access, processing, and sharing with privacy rights and implement compliance across the organization [9].
- **For Utilitarian Ethics:** Regularly audit algorithms and data analytics tools to ensure they do not harm or introduce bias. Balance organizational goals of data practices with social responsibility by ensuring benefits for both users and society [12].

REFERENCES

[1] John Ladley. *Data governance: How to design, deploy, and sustain an effective data governance program*. Academic Press, 2019.

[2] Dama International. *DAMA-DMBOK: Data management body of knowledge*. Technics Publications, LLC, 2017.

[3] Sunil Soares. *The IBM data governance unified process: driving business value with IBM software and best practices*. MC Press, LLC, 2010.

[4] P. Voigt and A. von dem Bussche. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 2017.

[5] M. Goddard. The eu general data protection regulation (gdpr): European regulation that has a global impact. *International Journal of Market Research*, 59(6):703–705, 2017.

[6] W. G. Voss. European union data privacy law reform: General data protection regulation, privacy shield, and the right to delisting. *Business Lawyer*, 72:221–233, 2020.

[7] T. Z. Zarsky. Incompatible: The gdpr in the age of big data. *Seton Hall Law Review*, 47:995, 2016.

[8] Immanuel Kant. *Groundwork of the Metaphysics of Morals*. Harper Row, 1785.

[9] European Parliament. General Data Protection Regulation (GDPR), 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[10] Organisation for Economic Co-operation and Development. Privacy guidelines, 1980.

[11] Jeremy Bentham. *An Introduction to the Principles of Morals and Legislation*. 1789.

[12] M. Wachter-Boettcher. *Technically Wrong: Sexist Apps, Biased Algorithms, and Other Threats of Toxic Tech*. W.W. Norton & Company, 2017.

[13] Francine Berman and Vinton Cerf. Social and ethical responsibilities of computing. *Communications of the ACM*, 64(5):8–9, May 2021.