UNITED ARAB EMIRATES:
ETISALAT CUSTOMER DATA EXPOSURE

CASE STUDY REPORT

Submitted by

AFREED P MAJEED (VML24AD011)
DON P TOM (VML24AD056)
MUHAMMAD SHAZ PP(VML24AD080)
SHEBIN MUTHALIB (VML24AD107)
SABIN SANTO(VML24AD098)

As part of the Case Study under Continuous Internal Evaluation in the course

PEADT412-DATA SCIENCE PRIVACY AND ETHICS

Vimal Jyothi Engineering College, Chemperi
(JANUARY 2026)

DECLARATION

We, the undersigned, hereby declare that the case study report entitled **"United Arab Emirates:etisalat customer data exposure "**, submitted as part of the **Case Study under Continuous Internal Evaluation** for the course **PEADT412 – Data Science Privacy & Ethics**, is a **bonafide work** carried out by us.

This submission represents our **original work**, and the ideas expressed are in our **own words**. Wherever ideas, data, or words of others have been included, they have been **properly cited and referenced**.

We further declare that we have strictly adhered to the principles of **academic honesty and integrity**, and that this report has **not been submitted previously**, either in part or in full, for the award of any degree, diploma, or title at any University or Institution.

We understand that any violation of the above declaration may result in **disciplinary action** as per the rules and regulations of the Institution and the University.

PLACE: CHEMPERI

DATE: 14/01/26

NAME & SIGNATURE

AFREED P MAJEED

DON P TOM

SHEBIN MUTHALIB

MUHAMMAD SHAZ

SABIN SANTO

VIMAL JYOTHI ENGINEERING COLLEGE, CHEMPERI

CERTIFICATE

This is to certify that the case study report entitled **"United Arab Emirates:etisalat customer data exposure "** submitted by **AFREED P MAJEED(VML24AD011), DON P TOM(VML24AD056), SHEBIN MUTHALIB (VML24AD107), MUHAMMAD SHAZ (VML24AD080), SABIN SANTO (VML24AD098)** in partial fulfillment of the requirements for the **Case Study under Continuous Internal Evaluation** for the course **PEADT412 – Data Science Privacy & Ethics** is a **bonafide record of work carried out by them during the academic year 2026**.

This report has **not been submitted to any other University or Institute** for the award of any **degree or diploma**.

Faculty in Charge **Head of Department**

Ms Anju AJ **Dr Manoj V Thomas**

ABSTRACT

The rapid expansion of digital communication services has led telecommunication companies to process and store vast volumes of personal and sensitive customer data. In the United Arab Emirates (UAE), Etisalat operates as a major telecommunications provider, handling critical information such as customer identity details, billing records, call detail records, location data, and internet usage data. This extensive data processing environment increases the risk of customer data exposure resulting from cyberattacks, system vulnerabilities, insider threats, or inadequate security controls. To address such risks and safeguard individual privacy, the UAE enacted the Personal Data Protection Law (PDPL), which establishes a comprehensive legal framework governing the collection, processing, storage, and protection of personal data.

This case study critically examines a customer data exposure scenario involving Etisalat through the lens of the UAE PDPL. The study analyzes the nature of personal data handled by telecom operators, identifies potential causes and consequences of data exposure incidents, and evaluates Etisalat's responsibilities as a data controller under PDPL provisions. Particular emphasis is placed on PDPL principles such as lawful and transparent processing, purpose limitation, data minimization, security safeguards, breach notification, and the protection of data subject rights. The ethical implications of data exposure, including privacy violations, erosion of customer trust, and potential misuse of personal information, are also explored.

Furthermore, the study highlights the legal, operational, and reputational impacts of customer data exposure on both individuals and organizations within the telecom sector. It underscores the importance of implementing robust cybersecurity measures, privacy-by-design practices, and organizational accountability to ensure PDPL compliance. By analyzing the Etisalat case, this study aims to demonstrate how effective data governance and regulatory compliance can mitigate risks, protect customer privacy, and strengthen trust in digital communication services in the UAE.

Contents

Introduction

The rapid growth of digital communication and information technologies has significantly increased the volume of personal data collected and processed by telecommunication service providers. In the United Arab Emirates (UAE), Etisalat is one of the largest telecom operators, offering a wide range of services such as mobile communication, internet access, digital payments, and cloud-based solutions. To deliver these services efficiently, Etisalat processes large amounts of customer data, including personal identification information, billing records, call details, location data, and internet usage patterns.

With the increasing dependence on digital platforms, the risk of customer data exposure has also grown. Data exposure incidents may occur due to cyberattacks, system vulnerabilities, insider threats, or inadequate security controls. Such incidents can lead to serious consequences, including privacy violations, financial fraud, identity theft, and loss of customer trust. Recognizing the importance of protecting personal data, the UAE introduced the Personal Data Protection Law (PDPL) to regulate how organizations collect, process, store, and protect personal data.

The UAE PDPL establishes clear principles and obligations for organizations acting as data controllers and data processors. These include lawful and transparent data processing, purpose limitation, data minimization, implementation of appropriate security measures, and timely notification of data breaches. For telecom companies like Etisalat, compliance with PDPL is critical due to the sensitive nature and scale of customer data they handle.

This case study examines customer data exposure risks associated with Etisalat in the context of the UAE PDPL. It aims to analyze how customer data is processed, identify potential causes and impacts of data exposure, and evaluate the ethical and legal responsibilities of telecom operators under PDPL. The study also highlights the importance of strong data governance, cybersecurity practices, and regulatory compliance to ensure customer privacy and maintain trust in the UAE’s digital ecos

Problem statement

Telecommunication service providers such as Etisalat handle vast amounts of sensitive customer data, including personal identification details, communication records, location information, and billing data. The large-scale collection and processing of such data increase the risk of customer data exposure due to cyberattacks, system misconfigurations, insider threats, or inadequate data security practices. Any unauthorized access, disclosure, or misuse of customer data can result in serious privacy violations and loss of public trust.

Although the UAE Personal Data Protection Law (PDPL) provides a comprehensive legal framework for safeguarding personal data, ensuring effective compliance remains a significant challenge for organizations operating complex digital infrastructures. For telecom operators, the challenge lies in balancing efficient service delivery with strict data protection requirements, transparency, and accountability. Failure to implement adequate technical and organizational safeguards can lead to non-compliance with PDPL obligations, exposing organizations to legal penalties, reputational damage, and operational disruption.

The core problem addressed in this case study is the potential exposure of Etisalat customer data and its implications under the UAE PDPL. The study focuses on identifying the causes of data exposure, examining the ethical and legal responsibilities of Etisalat as a data controller, and assessing the impact of such incidents on customers and the organization. It also highlights the need for robust data protection strategies, effective incident response mechanisms, and continuous compliance monitoring to mitigate risks and ensure the protection of customer privacy in the UAE's telecommunications sector.

ETISALAT AND CUSTOMER DATA HANDLING

Etisalat, as one of the leading telecommunications service providers in the United Arab Emirates, manages an extensive digital infrastructure that supports millions of customers across mobile, internet, and digital services. To deliver reliable communication services, Etisalat collects, processes, and stores large volumes of customer data on a continuous basis. This data is essential for service provisioning, billing, network management, regulatory compliance, and customer support.

The types of customer data handled by Etisalat include personal identification information such as names, Emirates ID details, contact numbers, and addresses. In addition, Etisalat processes financial and billing information, including payment records, transaction histories, and subscription details. Telecom-specific data such as call detail records (CDRs), message logs, internet usage data, and location information is also collected to ensure accurate billing, network optimization, and service quality. Due to the sensitive nature of this data, it is classified as personal and, in some cases, sensitive personal data under the UAE PDPL.

Etisalat relies on advanced information systems, databases, and cloud-based platforms to manage customer data efficiently. Data is typically processed across multiple stages, including collection at the point of service registration, storage in centralized or distributed databases, analysis for operational and business purposes, and sharing with authorized third parties such as regulatory bodies or service partners where legally permitted. Each stage of data handling introduces potential risks if adequate technical and organizational safeguards are not implemented.

To protect customer data, Etisalat employs cybersecurity measures such as access controls, encryption, authentication mechanisms, and monitoring systems. Only authorized personnel are permitted to access sensitive data, and role-based access controls are implemented to reduce the risk of unauthorized exposure. However, despite these measures, risks remain due to system complexity, evolving cyber threats, and human error. Data exposure incidents may arise from software vulnerabilities, misconfigured systems, phishing attacks, or insider misuse.

Under the UAE PDPL, Etisalat acts primarily as a data controller and is responsible for ensuring that customer data is processed lawfully, transparently, and securely. This includes limiting data collection to specified purposes, retaining data only for necessary durations, and implementing appropriate safeguards to prevent unauthorized access or disclosure. Failure to adequately manage customer data can lead to violations of PDPL provisions, resulting in legal consequences and loss of customer trust.

UAE Personal Data Protection Law (PDPL)

The United Arab Emirates Personal Data Protection Law (PDPL) was introduced to establish a comprehensive legal framework for the protection of personal data in the UAE. Enacted under Federal Decree-Law No. 45 of 2021, the PDPL aims to safeguard the privacy of individuals while regulating how organizations collect, process, store, and share personal data. The law aligns the UAE with global data protection standards and reflects the country's commitment to fostering trust in its digital economy.

The PDPL applies to personal data processed electronically or by other means, covering organizations operating within the UAE as well as those outside the country that process personal data of UAE residents. Telecom service providers such as Etisalat fall directly under the scope of the PDPL due to the extensive volume and sensitivity of customer data they handle. The law defines key roles such as data subjects, data controllers, and data processors, and clearly outlines their responsibilities.

Under the PDPL, personal data includes any information relating to an identifiable individual, such as name, contact details, identification numbers, location data, and communication records. Certain categories of data, including biometric, health, and financial information, are considered sensitive and require enhanced protection. The law emphasizes lawful processing, transparency, accountability, and security, making it particularly relevant to sectors like telecommunications where data misuse can have serious consequences.

7.1 Key Principles of UAE PDPL

The UAE PDPL is built on a set of fundamental principles that govern the processing of personal data. These principles ensure that organizations handle data responsibly and ethically.

The principle of **lawfulness, fairness, and transparency** requires that personal data be processed in a lawful manner and that individuals are informed about how their data is collected and used. Organizations must clearly communicate the purpose of data processing through privacy notices or policies.

Purpose limitation mandates that personal data should be collected for specific, explicit, and legitimate purposes and should not be processed in a manner incompatible with those purposes. For example, telecom customer data collected for billing should not be used for unrelated marketing without consent.

Data minimization requires organizations to collect only the data that is necessary to achieve the intended purpose. Excessive or irrelevant data collection increases the risk of exposure and violates PDPL principles.

The principle of **accuracy** ensures that personal data is kept up to date and corrected when inaccurate. Inaccurate customer data can lead to billing errors and service issues.

Storage limitation requires that personal data be retained only for as long as necessary to fulfill the purpose for which it was collected. Once the purpose is achieved, data should be securely deleted or anonymized.

Finally, **integrity and confidentiality** require organizations to implement appropriate technical and organizational measures to protect personal data from unauthorized access, disclosure, alteration, or destruction. This principle is critical for telecom providers managing sensitive communication data.

7.2 Rights of Data Subjects

The PDPL grants individuals, referred to as data subjects, several rights to maintain control over their personal data. These rights strengthen transparency and accountability in data processing activities.

Data subjects have the **right to access** their personal data and obtain information about how it is being processed. This allows customers to understand what data Etisalat holds about them.

The **right to rectification** enables individuals to request correction of inaccurate or incomplete personal data. This is essential for ensuring fair treatment and service accuracy.

The **right to erasure**, also known as the right to be forgotten, allows individuals to request deletion of their personal data when it is no longer necessary for the original purpose, subject to legal and regulatory requirements.

Data subjects also have the **right to restrict processing** in certain circumstances, such as when data accuracy is disputed or processing is unlawful.

The **right to object** allows individuals to oppose certain types of data processing, particularly direct marketing or automated decision-making.

Additionally, the PDPL provides rights related to **data portability**, enabling individuals to obtain their data in a structured and commonly used format. For telecom customers, these rights empower individuals to exercise greater control over how their personal information is handled.

7.3 Obligations of Data Controllers and Processors

The PDPL places significant responsibilities on data controllers and data processors to ensure lawful and secure data handling. Telecom companies like Etisalat typically act as data controllers, as they determine the purposes and means of processing customer data.

Data controllers are required to implement appropriate technical and organizational measures to ensure compliance with PDPL principles. This includes adopting cybersecurity controls, conducting risk assessments, and maintaining records of processing activities.

Controllers must ensure that personal data is processed based on a lawful basis, such as consent, contractual necessity, or legal obligation. They are also responsible for ensuring transparency and responding to data subject requests within specified timeframes.

Data processors, who process data on behalf of controllers, must follow documented instructions and implement adequate security measures. Controllers must ensure that processors comply with PDPL requirements through contractual agreements.

In the event of a personal data breach, data controllers are obligated to notify the relevant authority and affected individuals when the breach poses a risk to privacy or rights. Failure to comply with breach notification requirements can result in penalties.

Overall, the PDPL emphasizes accountability, requiring organizations to demonstrate compliance through documentation, audits, and continuous monitoring. For Etisalat, fulfilling these obligations is essential to prevent data exposure incidents, maintain regulatory compliance, and protect customer trust.

ETHICAL AND LEGAL IMPLICATIONS OF DATA EXPOSURE

Customer data exposure in the telecommunications sector raises serious ethical and legal concerns due to the sensitive nature of personal information involved. Telecom operators such as Etisalat collect and process large volumes of customer data, including identity details, communication records, and location information. When such data is exposed due to security failures, unauthorized access, or misuse, it can result in significant harm to individuals and organizations alike. Beyond technical failures, data exposure represents a breach of ethical responsibility and legal obligations under the UAE Personal Data Protection Law (PDPL).

From an ethical perspective, organizations that process personal data are entrusted with safeguarding individual privacy and acting in the best interests of their customers. Data exposure undermines this trust and violates the fundamental ethical principle of respect for individual autonomy. Legally, such incidents can trigger regulatory action, penalties, and reputational damage. Therefore, understanding both ethical and legal implications is essential for responsible data governance in the telecommunications industry.

8.1 Ethical Concerns (Privacy, Trust, Transparency)

Privacy is one of the most significant ethical concerns arising from customer data exposure. Telecom data often includes highly sensitive information such as call records, internet usage, and location data, which can reveal personal habits, relationships, and movements. Unauthorized exposure of such data constitutes a direct violation of an individual's right to privacy. Ethically, organizations have a moral duty to ensure that customer data is collected and used only for legitimate purposes and protected against misuse.

Trust is another critical ethical issue. Customers trust telecom providers to handle their personal information responsibly and securely. A data exposure incident can severely damage this trust, leading to customer dissatisfaction, loss of confidence, and long-term reputational harm. Once trust is lost, it is difficult to rebuild, especially in industries where customers have limited alternatives. Ethical data handling is therefore essential not only for compliance but also for sustaining customer relationships.

Transparency plays a key role in ethical data governance. Customers have the right to know how their data is collected, processed, stored, and shared. In the event of a data exposure, organizations are ethically obligated to

communicate clearly and honestly with affected individuals. Failure to disclose incidents or provide accurate information undermines accountability and can worsen the ethical impact. Transparent communication demonstrates responsibility and respect for affected customers.

8.2 Legal Consequences under UAE PDPL

Under the UAE Personal Data Protection Law (PDPL), organizations are legally required to protect personal data through appropriate technical and organizational measures. A customer data exposure incident may constitute a violation of several PDPL provisions, particularly those related to data security, lawful processing, and accountability.

One major legal consequence of data exposure is **regulatory action**. Authorities may investigate the incident to determine whether the organization complied with PDPL requirements. If negligence or non-compliance is identified, the organization may face administrative penalties, fines, or corrective orders. These actions aim to enforce accountability and prevent future violations.

Another significant legal obligation involves **breach notification**. The PDPL requires data controllers to notify the relevant authority and affected data subjects when a data breach poses a risk to individual rights and freedoms. Failure to notify in a timely and transparent manner can result in additional penalties and increased regulatory scrutiny.

Data exposure may also lead to **civil liability**, where affected customers seek compensation for damages such as financial loss, identity theft, or emotional distress. For telecom companies like Etisalat, large-scale data exposure could result in multiple claims, increasing legal and financial risks.

In summary, the ethical and legal implications of customer data exposure are substantial. Ethically, organizations must protect privacy, maintain trust, and ensure transparency. Legally, compliance with the UAE PDPL is mandatory, and failure to meet its requirements can result in penalties, legal action, and reputational harm. These implications highlight the importance of robust data protection practices, ethical governance, and continuous compliance monitoring in the telecommunications sector.

IMPACT OF CUSTOMER DATA EXPOSURE

Customer data exposure in the telecommunications sector can have serious and wide-ranging consequences. Telecom service providers such as Etisalat store highly sensitive personal and communication data, and any unauthorized disclosure of this information can negatively affect both customers and the organization. The impact of data exposure extends beyond immediate technical or financial losses, influencing trust, legal compliance, and long-term organizational sustainability.

Data exposure incidents undermine confidence in digital services and raise concerns about the ability of organizations to safeguard personal information. In highly regulated environments like the UAE, such incidents also attract regulatory scrutiny and legal consequences. Understanding the impact of customer data exposure is essential for developing effective data protection strategies and maintaining ethical and legal standards.

9.1 Impact on Customers

The exposure of customer data can cause significant harm to individuals. One of the most serious consequences is **loss of privacy**. Telecom data, including call records, location data, and internet usage, can reveal sensitive personal details about an individual's daily activities, relationships, and behavior. Unauthorized access to such information constitutes a direct violation of privacy rights.

Another major impact is **financial risk**. Exposed personal and billing information can be misused for fraud, identity theft, or unauthorized transactions. Customers may suffer financial losses and may need to spend considerable time and effort resolving such issues. In severe cases, data exposure can also lead to blackmail, harassment, or social harm.

Data exposure can also cause **psychological distress**. Knowing that personal information has been compromised can create anxiety, fear, and loss of confidence in digital services. Customers may become reluctant to share information or use online services, affecting their overall experience.

Additionally, data exposure reduces **trust in service providers**. Customers expect telecom operators to handle their data securely. When this expectation is not met, customers may choose to switch providers or limit their use of digital services, leading to long-term dissatisfaction.

9.2 Impact on Organization and Reputation

For organizations such as Etisalat, customer data exposure can result in severe **reputational damage**. Public disclosure of data breaches can lead to negative media coverage and loss of customer confidence. Reputation is especially critical in the telecommunications sector, where trust is fundamental to customer retention and brand value.

Data exposure can also lead to **legal and regulatory consequences**. Under the UAE PDPL, organizations may face investigations, penalties, and mandatory corrective actions if they fail to protect customer data. Compliance failures increase operational and financial burdens.

From a business perspective, data exposure can cause **financial losses** due to fines, compensation claims, increased cybersecurity costs, and loss of customers. Organizations may need to invest heavily in system upgrades, audits, and employee training following a breach.

Operational disruption is another significant impact. Responding to a data exposure incident requires resources for investigation, system recovery, and communication with regulators and customers. This can divert attention from core business activities and affect service quality.

CONCLUSION

The case study on Etisalat customer data exposure under the UAE Personal Data Protection Law (PDPL) highlights the critical importance of data protection in the telecommunications sector. As a major telecom service provider, Etisalat processes vast amounts of sensitive customer data to deliver essential communication services. While such data processing is necessary for operational efficiency, it also creates significant ethical and legal responsibilities related to privacy, security, and accountability.

The study demonstrates that customer data exposure can occur due to technical vulnerabilities, human error, or inadequate security practices. Such incidents have serious consequences, including privacy violations, financial risks for customers, loss of trust, and reputational damage for organizations. Under the UAE PDPL, telecom operators are legally obligated to implement strong technical and organizational measures to protect personal data and respond effectively to data breaches.

Furthermore, the ethical implications of data exposure emphasize the need for transparency, trust, and respect for individual rights. Customers expect their personal information to be handled responsibly, and any failure to do so undermines confidence in digital services. Compliance with PDPL is therefore not only a legal requirement but also a fundamental aspect of ethical data governance.

In conclusion, preventing customer data exposure requires a proactive and comprehensive approach that includes robust cybersecurity controls, clear data governance policies, employee awareness, and continuous compliance monitoring. By aligning operational practices with the principles of the UAE PDPL, telecom organizations like Etisalat can protect customer privacy, maintain public trust, and ensure sustainable growth in the UAE's digital ecosystem.

REFERENCES

- UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (Personal Data Protection Law – PDPL).

- UAE Data Office, *Personal Data Protection Law – Overview and Compliance Guidelines*, Government of the United Arab Emirates.

- Etisalat Group, *Privacy Policy and Data Protection Practices*, Etisalat Official Publications.

- Al Shamsi, A., "Data Protection and Privacy Law in the UAE: An Overview of PDPL," *International Journal of Law and Information Technology*, 2022.

- European Union, *General Data Protection Regulation (GDPR): A Comparative Reference*, Official Journal of the European Union, 2018.

.