Journal of Posthumanism
2025
Volume: 5, No: 2, pp. 1449–1469
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i2.528

Administrative Measures for Protecting Personal Data in Saudi Law An Analytical and Practical Study

Salih Alsamhan[1],

Abstract

This research evaluates Saudi Arabia's efforts in protecting personal data, with a focus on the steps taken in alignment with Vision 2030. The study addresses the Kingdom's adoption of advanced administrative measures for personal data protection, which surpasses many other countries, thus warranting academic exploration. Additionally, the diversity of protection measures necessitates an in-depth clarification of their interplay. The significance of this research lies in highlighting the supervisory role of the Saudi Authority for Data and Artificial Intelligence (SDAIA) in overseeing personal data protection measures, as well as clarifying its relationship with entities involved in data control and implementation. The study aims to define the legal concept of personal data, determine its legal nature, outline forms of legal protection, and explore the distinctions between administrative protection and other legal protections provided by Saudi law. Furthermore, the research identifies administrative violations of the right to privacy concerning personal data and investigates administrative accountability for breaches. The findings reveal that Saudi Arabia has established a robust legal framework for protecting personal data, adhering to privacy policies, assigning responsibility to entities for data handling, processing, and supervision, and enforcing penalties for violations. The study also includes practical applications through both domestic and international cases.

Keywords: *Administrative measures, Personal data protection, Saudi Authority for Data and Artificial Intelligence (SDAIA)*

Introduction

The legislative efforts of Saudi Arabia have been directed towards aligning with the ambitious goals of Saudi Vision 2030. One significant milestone in this regard was the establishment of the Saudi Authority for Data and Artificial Intelligence (SDAIA) through Council of Ministers Resolution No. (292) dated 27/4/1441 AH, which was later amended by Resolution No. (195) dated 15/3/1444 AH. Complementing these efforts, the issuance of the Personal Data Protection Law under Royal Decree No. (M/19) dated 9/2/1443 AH, along with its Executive Regulations, marked a crucial step toward safeguarding data and ensuring its ethical management. Acknowledging these advancements, this research aims to explore the administrative measures for personal data protection within the Saudi legal framework. By analyzing the provisions of the Personal Data Protection Law and its Executive Regulations, alongside comparative insights from other legal systems, the study seeks to contribute to the ongoing legislative and regulatory discourse. This approach aspires to enhance the legal understanding and practical application of personal data protection in alignment with the broader objectives of Vision 2030.

Research Problem

This study addresses the administrative measures adopted by Saudi Arabia to protect personal

[1] Law Department, University of Hafr Al-Batin, Saudi Arabia. Salih.alsamhan@uhb.edu.sa.

data as part of its Vision 2030. These measures, overseen by the Saudi Data and Artificial Intelligence Authority (SDAIA), are implemented using various legal frameworks and tools. The central research question is: What administrative measures has Saudi Arabia implemented to protect personal data?

To address this central question, the study explores the following sub-questions:

a. What is the legal concept and nature of personal data?

b. What are the forms of legal protection available for personal data?;

c. What are the supervisory roles of SDAIA, and how does it relate to other entities involved in data management and enforcement?

d. What are the primary administrative violations of privacy concerning personal data, and how are these violations accountable?

e. Which authority is responsible for addressing violations of privacy in personal data?

f. How do administrative protections compare with other legal protections for personal data under Saudi law?

By answering these questions, the study seeks to provide a comprehensive understanding of the administrative framework for the protection of personal data in Saudi Arabia and its alignment with the broader objectives of Vision 2030.

Significance of the Research

This research is significant for several reasons:

a. It sheds light on Saudi Arabia's major efforts to protect personal data through specialized bodies for supervision, control, and execution.

b. It investigates the role of SDAIA in overseeing personal data protection and its interaction with other relevant entities.

c. It clarifies the differences and relationships between administrative and other legal protections for personal data.

d. It facilitates the process for individuals to assert their privacy rights by identifying the authorities responsible for enforcement.

e. It addresses the gap in existing studies regarding the administrative measures for personal data protection in Saudi Arabia.

Research Objectives

The study aims to address the research problem by:

a. Defining the legal concept and nature of personal data.

b. Exploring the forms of legal protection available for personal data.

c. Comparing administrative protections with other legal protections under Saudi law.

d. Investigating SDAIA's supervisory roles and its relationships with entities responsible for data management and processing.

e. Identifying administrative violations and accountability measures concerning privacy breaches.

f. Determining which authorities are responsible for addressing privacy violations.

g. Highlighting the administrative aspect of personal data protection within the broader legal framework.

Previous Studies

A comprehensive review of research databases indicates a lack of studies specifically focusing on the administrative measures implemented by Saudi Arabia to safeguard personal data. This highlights a significant gap in the existing literature, emphasizing the need for this study to address this overlooked area and contribute to the growing discourse on personal data protection within the Saudi legal framework.

Research Framework

To achieve the aforementioned objectives, the study comprises four main sections:

- Section One: Theoretical Framework of the Study, which includes:
  a. The legal concept of personal data.
  b. The legal nature of personal data.
  c. Forms of legal protection for personal data.
- Section Two: Administrative Regulations for Personal Data Protection, which includes:
  a. Establishing a System for Regulating Personal Data Handling Rules
  b. Assigning Competent Entities for Personal Data Processing and Control
  c. Designating a Supervisory Body to Implement and Enforce the Law
- Section Three: Distinguishing the Scope of Administrative Measures in Protecting Personal Data, which includes:

a. Administrative Jurisdiction in Protecting Personal Data

b. The Jurisdiction of Administrative Control in Personal Data Protection

c. Administrative Violations of Privacy Rights in Personal Data

d. Administrative Accountability for Violating the Right to Privacy in Personal Data

- Section Four: Practical Applications in Local and International Cases, which includes:
  a. Applications in Local Cases
  b. Applications in International Cases

Theoretical Framework of the Study

This chapter explores the legal concept and nature of personal data. The discussion is structured into three *main* sections to provide a comprehensive analysis of these aspects.

The Legal Concept of Personal Data

The Saudi legal system has addressed the concept of personal data in terms of its material reality and has examined personal data from other perspectives of equal importance, independent of its material concept, although still related to it in some aspects. Therefore, this section will first discuss the material definition of personal data, then address its comprehensive concept, concluding with a satisfactory opinion on the matter.

The Material Concept of Personal Data

The Saudi legislator defines personal data as: "Any information that could lead to identifying an individual specifically, or makes their identification possible directly or indirectly." **[1]**

Personal data serves as a means of identifying an individual whether this refers to a natural person or a legal entity. Furthermore, such data is not limited to immediate identification but extends to means enabling identification over time, whether directly or indirectly, regardless of the time frame required for identification.

Article 1 of the relevant regulations identifies various examples of personal data, such as credit data, sensitive data, genetic data, and similar categories. A review of this article reveals that the concept of personal data encompasses multiple forms, including those confined to the material concept of personal data and others incorporating.

additional meanings. Forms that adhere to the material concept include**[16]**:

a. Data directly linked to an individual, regardless of their legal status or profession, such as personal names—whether the proper name of a natural person or the name of a company or legal entity for a juridical person **[1]**.

b. Data reflecting the individual through their activity or profession, such as professional titles appended to proper names, including descriptions and restrictions in the names of public bodies and commercial names for companies or private sector institutions **[1,17]**.

c. Digital data, which specifically identifies an individual with precision, making it impossible for two persons to share the same information. Examples include identification numbers, commercial registers, bank account details, and other private document data, including personal identifiers across various digital platforms **[18]**.

d. Data representing an individual through their appearance or visual identity, encompassing all types of personal photographs for natural persons, logos of public bodies, and trademarks for companies or private institutions.

A Comprehensive Perspective on Personal Data

To achieve comprehensiveness in addressing the concept of personal data, it is noted that the legislator's definition and its outlined examples relate solely to the material aspect of personal data. However, they do not encompass the concept in its entirety. The legislator has addressed the material reality and general examples of personal data, yet requires further elaboration from a categorical perspective that remains consistent with the aforementioned examples but expands the concept to a broader dimension. This dimension involves considering forms of personal data in terms of **[1]**:

a. Risk level: Evaluating the sensitivity of personal data to the individual, such as data related to religious or ideological beliefs and political affiliations.

b. Source and lineage: Assessing whether personal data pertains to an individual's origin or extends to their descendants, such as genetic data related to physiological traits.

c. Health status: Including identifiers from an individual's medical files at healthcare facilities.

d. Creditworthiness: Covering aspects like credibility, personal stability, or financial solvency, including data on the individual's obligations to public or private granting entities, such as relevant authorities or private financial institutions.

The Researcher's Opinion

From the foregoing discussion, the researcher concludes that the concept of personal data includes two main aspects: a material aspect and a descriptive aspect. The material aspect adheres to one of two criteria:

a. The personal data itself leads to identifying the individual, such as names or exclusive personal attributes.

b. The personal data can be used to identify the individual, either directly or indirectly, such as the individual's personal address or the official location of their business center. The concept also includes a descriptive aspect, arising from the addition of a criterion to the previous two: The data is a description associated with one of the forms mentioned in the material aspect, and this description may indicate the individual's intellectual approach, religious beliefs, political affiliation, or health status, as well as creditworthiness, and this description may extend beyond the individual to include their family members.

These criteria combine to define the meaning of "personal" in personal data, which is its indication or potential indication— even in the distant future—of a specific individual and no one else.

The Legal Nature of Personal Data

The legal nature of personal data is based on the origin of the creation of personal data, its standing in the organizer's consideration towards the individual, and what personal data serves in the relationship between the individual and the state, or rather the function of personal data in the relationship between the organizer and the individual. The researcher will discuss this in the subsections of this requirement through explaining the legal nature of personal data according to each influencing factor.

The Origin of the Creation of Personal Data

If we consider the origin of the creation of personal data, it becomes clear that it is regarded—depending on its specific nature—as the starting point for the actual existence of the individual. For a natural person, personal data—especially those related to identity—marks the beginning of the legal existence of the individual in the country's system [2]. Other personal data concerning the same individual marks the start of their existence in the domain relevant to that data. As for legal entities, the same principle applies: the origin of creating personal data for legal entities marks the beginning of their actual existence in the relevant market and in the organizer's consideration [3,19].

The Standing of Personal Data in the Organizer's Consideration Towards the Individual

After reviewing a number of texts, it is evident that the system (state) relies on personal data to distinguish between individuals [16]. Based on this data, it assigns tasks to individuals and

arranges penalties for violations based on each individual's data. Furthermore, personal data varies according to the aforementioned concept. On another note, the state arranges legal effects for actions performed by the individual using their personal data [3], such as contact numbers, bank account details, and social media identifiers. Actions taken by the individual—whether issuing orders or receiving them through such data—are considered valid in the organizer's view, and the individual is held responsible for them and their consequences.

The Function of Personal Data in the Relationship Between the Individual and the State

Based on the above, personal data serves as a means of communication between the individual and the state. Through it, the individual connects with the state to fulfill their rights towards it. In return, the state connects with the individual to grant privileges, impose duties, assign tasks, and in certain cases, enforce penalties [4,5].

Thus, the legal nature of personal data is that personal data are legal tools representing the actual existence of the individual, depending on the situation. On the other hand, they are legal means of communication between the individual and the state. Through personal data, the individual is held accountable for any tasks assigned to them by the state using their verified personal data, as well as for violations identified according to their personal data. Conversely, the individual is entitled to the privileges granted by the state to the general public, which correspond to their personal data.

Forms of Legal Protection for Personal Data

The previous discussion indicates that the privacy underlying personal data is protected by the organizer. There are several manifestations of this protection, which we address in this requirement.

Civil Protection

Civil protection refers to the legislative manifestations that establish the right to privacy in personal data. The texts that establish the informational privacy right for individuals provide protection for personal data from a civil type, as it is an inherent right protected by legal texts [20]. In the legislative phase, personal data itself does not have legal value for the individual, other than the right guaranteed by the text for the privacy of their personal data. The personal data protection system in the Kingdom of Saudi Arabia includes this type of protection, as Article 12 stipulates that the controlling entity must adopt a privacy policy. This policy should include the purpose of collecting personal data, the content of the data to be collected, how it will be collected, stored, processed, and disposed of, the rights of the data subject in relation to their data, and how they can exercise these rights. [1] The system also grants the individual the right to request the deletion of personal data held by the controlling entity once it is no longer needed. Other provisions reinforce the civil protection of personal data, deriving its strength from the Basic Law of Governance, which stipulates in Article 40 that correspondence, postal, and telecommunications are inviolable and cannot be confiscated, delayed, or accessed except in cases defined by the law.

Administrative Protection

Administrative protection refers to the rules governing the secure handling of personal data and the policies set by control entities [21]—whether government agencies, institutions, or private companies—that impose restrictions on their employees in receiving, storing, and processing personal data. This includes administrative oversight systems concerning practices that violate

the provisions of the system and general rules mentioned above.

The personal data protection system in the Kingdom includes several provisions that grant administrative protection to individuals. Article 10 stipulates that personal data may only be collected directly from its owner, and the same article prohibits processing the collected data except for the purpose for which it was gathered. Article 15 also prohibits disclosing personal data except in specific cases that do not harm the data subject. Additionally, the system obligates control entities to take all necessary organizational, administrative, and technical measures to ensure the protection of personal data. To reinforce administrative protection, the personal data protection system requires control entities to appoint one or more persons responsible for data protection [1].

Criminal Protection

Criminal protection refers to the accountability rules related to privacy violations in personal data, with malicious intent towards the data subject, activating civil protection. This falls under the judicial authority responsible for studying violations of personal data protection systems to verify the elements of liability [22].

A distinction can be made between these forms of protection from a procedural perspective. Civil protection takes precedence over other forms of protection in terms of application. While regulatory texts related to each form of protection may be established during the legislative phase, practical practices related to civil protection certainly precede, followed by administrative protection, and then criminal protection, with overlap between the latter two, as both involve penalties for violations. However, they differ in terms of their goals, the authority to impose penalties, and the nature of the penalty, particularly in terms of whether it can be revoked.

Administrative Regulations for Personal Data Protection

The Kingdom of Saudi Arabia has made significant efforts and implemented various measures to protect personal data. These efforts include enacting laws and regulations, designating entities responsible for safeguarding, processing, controlling, and storing this data, and appointing a supervisory body to oversee data handling processes and ensure compliance with the established regulations. In this chapter, I will address these aspects in detail through the following sections:

Establishing a System for Regulating Personal Data Handling Rules

Saudi Arabia is among the few countries that have implemented a dedicated system for protecting personal data, reflecting its forward-thinking vision and commitment to data privacy and the protection of its citizens' personal information. The Personal Data Protection Law was issued on 9/2/1443H (16/9/2021) under Royal Decree No. (M/19) and Council of Ministers Resolution No. (98), dated 7/2/1443H.

The law comprises 43 articles, comprehensively addressing all aspects related to personal data handling, including data processors, controllers, and supervisory entities. It guarantees the rights of data subjects, prioritizes individual and societal interests, and adopts a data privacy policy.

Assigning Competent Entities for Personal Data Processing and Control

The Personal Data Protection Law obligates data controllers—whether public or private entities, individuals, or legal persons—to define the purpose of processing personal data and how it is carried out, whether directly or through a data processor. The latter refers to any entity processing personal data on behalf of the controller.

The law mandates these entities to maintain data confidentiality, prohibits disclosure, and restricts data processing or purpose alteration without the subject's consent. It also requires data destruction once the purpose of collection has been fulfilled. These provisions underscore the legislator's emphasis on personal data protection and privacy, fostering trust and reassurance among data subjects [1].

Designating a Supervisory Body to Implement and Enforce the Law

The government has assigned the Saudi Authority for Data and Artificial Intelligence (SDAIA) as the supreme regulatory and supervisory authority responsible for implementing personal data protection measures. This section discusses the legal basis for assigning these tasks to SDAIA, its relationship with data controllers and processors, and the rules governing its supervisory role.

Establishing SDAIA's Reference Role in Personal Data Protection

Royal Decree No. (M/19) dated 9/2/1443H states: "The competent authority shall be the Saudi Authority for Data and Artificial Intelligence for a period of two years, during which the application of the provisions of the Personal Data Protection Law and its executive regulations will be evaluated based on the maturity of the data sector. Following this period, the supervisory mandate may be transferred to the National Data Management Office."

This article establishes SDAIA as the supreme administrative authority responsible for implementing the law. Upon analysis, SDAIA's technical nature and relationship with artificial intelligence suggest that not all forms of personal data necessarily require its supervision. Some types of personal data align more naturally with the administrative roles of other entities[35].

The legislator specified a two-year period for SDAIA's supervisory role to evaluate the law's implementation and sector maturity. This indicates that certain forms of personal data—or potentially all personal data—may later be assigned to a different supervisory entity, as highlighted by the legislator's mention of the National Data Management Office taking on this role after the two-year period.

Nature of SDAIA's Relationship with Controllers, Processors, and Governing Rules

This section examines SDAIA's relationship with entities under its supervision, including the rules it applies in delegating authority to controllers and processors.

Council of Ministers Resolution No. (98) dated 7/2/1443H states:

"The competent authority shall, when preparing the executive regulations for the Personal Data Protection Law, establish provisions and regulations for organizational, administrative, and technical measures related to storing personal data with controllers..."

Drafting Executive Regulations

The legislator emphasizes SDAIA's responsibility for drafting executive regulations for the law. These regulations must:

a. Include provisions and measures for storing personal data with controllers[8].

b. Coordinate with relevant entities—such as the Ministry of Communications and Information Technology, Ministry of Foreign Affairs, Communications and Information Technology Commission, National Cybersecurity Authority, Saudi Health Council, and Saudi Central Bank—before issuing the regulations[1].

Approvals and Licensing for Activities Related to Data Protection, or for Auditing and Inspection Activities

The system assigns the Saudi Data and Artificial Intelligence Authority (SDAIA) the task of setting requirements for the practice of commercial, professional or non-profit activities related to personal data protection in the Kingdom, in coordination with the relevant authorities. It also grants SDAIA the responsibility of issuing licenses to entities that issue accreditation certificates for data controllers and processors, along with the authority to establish the rules governing this process.

The system also entrusts SDAIA with the task of granting licenses to entities responsible for auditing or inspecting personal data processing activities, giving it the authority to establish the requirements and conditions for issuing these licenses and to establish the relevant regulations[1].

This provision reinforces another aspect of the SDAIA's supervisory role in personal data protection. Clarifies that the authority to approve and license any commercial activity related to personal data protection is vested exclusively in SDAIA. This includes the authority to license entities that issue accreditation certificates for data controllers and processors. Naturally, this provision also establishes a time frame for the supervisory tasks assigned to SDAIA, set at two years. Therefore, the authority's licensing and approval functions, as outlined in this provision, follow the original tasks assigned to the authority which are bound by this time limit.

Regarding the licensing of entities, if the entity receiving approval or licensing represents a data processor outside the Kingdom, SDAIA must specify the applicable licensing provisions in the regulations and outline the relationship between the foreign entity and the entity it represents. In cases where the license pertains to entities that issue accreditation certificates for data controllers and processors, SDAIA must establish the rules that govern the issuance of such certificates[1].

Handling Complaints of Legal Violations

The supervisory responsibilities of the Data Authority concerning personal data protection extend to its competence in receiving and processing complaints raised by data subjects. A data subject has the right to file a complaint with the competent authority within a period not exceeding ninety days from the date of the incident in question or from the date the data subject becomes aware of it. If the data subject submits the complaint after this period has passed, the authority has the discretion to decide whether to accept the complaint or not, based on the reasonable circumstances that prevented the data subject from submitting the complaint within the prescribed time-frame [1].

In all cases, and in line with this aspect of the authority's duties, it must define clear regulations for handling complaints in its guidelines. The competent authority is required to receive complaints through the method specified in the regulations, following procedures that ensure promptness and quality in handling them. All complaints submitted to the competent authority must be recorded in a special register prepared for this purpose.

Distinguishing the Scope of Administrative Measures in Protecting Personal Data

After discussing the concept and providing a brief overview of the legal protection of personal data, we now delve into examining the administrative aspect of the topic of study, specifically

regarding the forms of protection related to administrative jurisdiction, and then from the perspective of monitoring violations, based on administrative infractions that constitute violations of privacy in personal data, followed by the aspect of liability for violating privacy.

Administrative Jurisdiction in Protecting Personal Data

In this section, we discuss the aspects of protection from the perspective of government departments' jurisdiction over the preservation of personal data – each in its own capacity. This moves beyond the stage of creating personal data, as while the jurisdiction to handle it belongs to the executive authority (administration), the process of creating personal data itself does not directly imply protection in the strict sense.

The legislator has designated specific administrative bodies for the preservation of personal data, depending on the nature of the individual data subject. The Civil Status Departments, for instance, are responsible for registering and maintaining records of civil occurrences, personal identity cards, and family books[2]. These departments carry out their duties in designated regions, setting up specialized safes for the preservation of records pertaining to that region, and these records must be deposited for safekeeping within one month of closing the registration. The personal data under the jurisdiction of the Civil Status Department includes information that identifies an individual and confirms their existence or death. This includes the civil status card or national identity card, the family book, and the death certificate. It is mandatory for the death certificate issued by the registrar to be deposited along with the deceased's personal identity card and their name in the family book at one of the Civil Status Departments within fifteen days from the issuance of the certificate [1].

Regarding legal entities such as associations, institutions, and private companies, the system has assigned specific administrative bodies for the preservation of personal data related to these entities. For example, the Ministry of Social Affairs and the National Center for the Development of the Non-Profit Sector are tasked with preparing a specific register for associations and institutions [6,7]. This registry is responsible for maintaining data related to the association or institution and any modifications made to it whenever updates occur. As for private companies, the Ministry of Commerce is required to establish a specific register containing all commercial company data[9]. The founders of each individual institution or commercial company, or the partners, directors, or board members of a company, are obligated to register the company in the commercial register, along with the company's founding contract or its charter, and any subsequent amendments[3].

In light of the legislative direction within the framework of the Kingdom's Vision 2030, and delegating the task of organizing data protection procedures to the Saudi Data and Artificial Intelligence Authority (SDAIA), the legislator has grouped different entities, based on their operations, under a specific category concerning personal data—referred to as the "controller entity.[1]"

Upon further consideration, it becomes clear that this definition applies to all entities working under the umbrella of one of the entities whose data has been submitted, such as individual institutions, private companies, and even government institutions. The entities that are considered "controller entities" include: passport offices, hospitals, the central bank, and the courts. The legislator has entrusted the SDAIA with the oversight and supervision of all these entities' activities.

Additionally, the legislator has assigned each controller entity with specific responsibilities,

including:

a. Ensuring that the controller entity takes all necessary organizational, administrative, and technical measures to protect personal data. This responsibility is detailed in relation to all forms of processing that personal data may undergo, such as transfer, modification, correction, disclosure, destruction, and others. If any department (controller entity) delegates processing tasks to another entity, it must ensure that the chosen entity provides sufficient guarantees to implement the provisions of the system and regulations. Furthermore, the controller entity must continuously verify that the delegated entity complies with the instructions it receives regarding personal data protection [1].

b. Appointing one or more individuals within each controller entity to be responsible for ensuring the entity's compliance with the provisions of the system and regulations [1].

The Jurisdiction of Administrative Control in Personal Data Protection

The jurisdiction to protect personal data falls under the executive authority, with each department exercising its jurisdiction according to its responsibilities by issuing regulations and circulars that regulate the behavior of administrative members and public employees whose duties involve direct interaction with personal data [23].

On the other hand, the protection of personal data—under this meaning—takes various forms. It ensures the administrative jurisdiction controls the behavior of individuals outside civil service or employment with private institutions and companies. That is, after establishing policies and making organizational decisions to regulate the conduct of public employees in handling personal data, the administration, through law enforcement officers, must activate its authority in field tasks to monitor cases of personal data violations [24]. This framework of protection also includes the regulatory tasks of committees and administrative bodies specialized in investigations, specifically those concerning violations of personal data protection regulations and the resulting records [10].

Protection, in this sense, aims at preventing privacy violations regarding personal data. In nature, this protection differs from its intersection with criminal jurisdiction. The administrative scope, with its various aspects, differs from the criminal one in terms of its objective, the authority responsible for imposing penalties, and the punitive nature of the penalties [23].

In conclusion, protection from the administrative regulatory perspective is preventive, whereas from the criminal perspective, it is corrective. Later, we will explore the aspects of the administration's jurisdiction in protecting personal data that overlap with the criminal domain.

Administrative Violations of Privacy Rights in Personal Data

The procedures through which the administration exercises its regulatory jurisdiction in protecting personal data typically end with detecting suspicious practices as violations of protection rules, whether they are basic legislative rules or administrative regulations [10]. The administration's decision to issue a ruling on the violation is considered one of the most important manifestations of administrative protection for personal data. We will examine violations of privacy rights in personal data by examining the legislative foundation and presenting examples of material violations of administrative protection rules.

Legislative Foundation of Administrative Protection for Personal Data

In this subsection, we will discuss the regulatory texts that establish the practical procedures for protecting personal data. The legislator has laid the foundations to activate the administrative role in protecting personal data, stipulating in the system that: "A committee (or more) shall be formed by a decision from the head of the competent authority, with no fewer than three members, one of whom shall be appointed as chairman. The committee must include a technical specialist and a legal advisor. The committee will review violations and impose warnings or fines as specified in paragraph (1) of this article, based on the type of violation, its severity, and its impact. The committee's decision must be approved by the head of the competent authority or by someone authorized by them. The head of the competent authority shall issue a decision outlining the committee's operating rules and specify the rewards for its members [1]."

Upon reflecting on the content of this article, it becomes clear that it addresses the legal protection of personal data from both the administrative and criminal sides, considering the legal nature of the penalties specified and the competent authority responsible for imposing them.

The administrative scope within the meaning of this article lies in the requirement for the competent authority (SDAIA) to form a specialized committee to review violations and impose the penalties outlined in the system. The committee's decision must be approved by the head of the competent authority or someone delegated by them **[1]**. The responsibilities of this committee have already been discussed in the context of the executive bodies through which the authority carries out its supervisory duties. This highlights the foundation of administrative protection for personal data, based on this article, especially since the committee is part of the policies of the Saudi Data and Artificial Intelligence Authority (SDAIA), which is entrusted with organizing, supervising, and overseeing all protection procedures.

Administrative decisions issued by the committee regarding the conviction of an employee for a violation must be based on a majority vote **[12]**. If a member of the committee has reservations, these reservations must be recorded in the investigation report, and the report must be substantiated. The violator who is convicted may file an appeal with the committee, the competent authority that issued the decision **[25]**, or before the competent court **[1]**.

Examples of Material Violations of Administrative Protection Rules

According to the provisions of Article 36 of the Personal Data Protection System, several forms of violations of administrative protection rules are considered violations of the established procedures for personal data protection. These may include actions taken by any competent authority, whether acting as a controller or a processor of personal data. Below are some of these manifestations, which can be classified into procedural violations and other violations in field implementation:

Procedural Administrative Violations

From an administrative procedural perspective, the following are considered violations of administrative protection rules **[1]**:

a. The absence of regulations by the competent authority governing the procedures for accrediting and granting certification to data controllers or processors, or the lack of coordination between the competent authority and the Digital Government Authority concerning licensing data controllers or processors.

b. The absence of regulations by the competent authority governing the licensing of entities responsible for auditing or inspecting personal data processing activities, as specified in paragraph (3) of Article 33 of the system, and the lack of coordination between the competent authority and the Digital Government Authority concerning licensing entities providing services on behalf of government entities. The violation in the two previous cases lies in the failure of the competent authority to establish specific regulations for organizing the activity of data control and processing, whether through licensing competent entities or establishing oversight policies to ensure compliance with safe data processing requirements and standards.

c. If a data controller or processor lacks a specialized committee responsible for reviewing violations and imposing penalties (warnings or fines) as stipulated in the system, this is considered one of the most significant violations of protection rules from an administrative perspective. The degree of the violation here lies in the procedural aspect of administrative protection for personal data.

Field Implementation Violations

In accordance with the provisions of the system, the following administrative behaviors or practices are considered violations of administrative protection rules:

a. The lack of alignment between the level of penalties and the type and severity of violations that the competent committee has decided to address **[1]**. The violation of administrative protection rules here lies in the shortcomings of the competent committee in its duties of imposing penalties for violations. The assessment of the appropriateness of the penalty in relation to the violation, and the determination of whether the committee's decision was correct or incorrect, falls within the jurisdiction of the judicial authority, which inherently belongs to the criminal aspect of personal data protection.

b. Disclosure by a public employee or member of a data controller or processor about confidential information related to their employer or any other information that undermines national security, including contents of mail received, which may include national security-related data or private entities' data with dealings with the state **[13]**. The data controller is prohibited from disclosing personal data except under strict conditions: when the personal data subject consents, or when disclosure is requested by a government entity for public interest, or to protect the life or health of specific individuals, or when the personal data was collected from a publicly accessible source, or when the disclosure is limited to processing in a way that does not reveal the identity of the data subject or any individual **[1]**.

c. The failure of specialized administrative bodies to carry out verification procedures aimed at preventing data duplication, especially for sensitive data categories like trade names, trademarks, etc **[1]**. To address this, the data controller must appoint one or more individuals to be responsible for ensuring compliance with the system and regulations. For personal data of private companies, the registrar is responsible for verifying the necessary regulatory requirements in registration applications. The registration decision must be made within ten working days **[9]**. Article 10 of the Trademark System states: "The competent authority in the Ministry of Commerce must decide on the registration application within sixty days of its submission, provided it meets the requirements and procedures stipulated in this system and its executive regulations." "If the competent authority deems that the application does not comply with this system's provisions, it must notify the applicant in writing and may

request that conditions be met or necessary amendments be made to accept the application **[14]**." This obligation aims to prevent duplication of commercial personal data (trade names).

The Personal Data Protection System further emphasizes that the data controller must ensure the chosen processing entity provides the necessary guarantees to implement the system and regulations, and continuously verify its compliance with the instructions regarding personal data protection, without conflicting with the system and regulations, and without affecting the data subject's or competent authority's responsibilities, as applicable.This indicates that the data controller is obligated to provide necessary guarantees for personal data protection, including protecting traders' personal data so it is not duplicated for another trader. If the data controller fails to fulfill this obligation, it is considered a violation of the procedural policies for registration **[1]**.

Administrative Accountability for Violating the Right to Privacy in Personal Data

This section aims to address the protection of personal data from the perspective of administrative accountability. It can be noted that this aspect of administrative protection is the most intertwined with criminal protection. Therefore, it is considered, on the one hand, as the

focal point of summarizing the administrative scope of legal protection for personal data.

The Discipline Regulation System stipulates: "Violating the provisions stated in these regulations exposes the violator to accountability and disciplinary and penal actions in accordance with the relevant regulations **[10]**."

"If a violation by an employee is discovered, the employee is referred to the committee for investigation, to consider imposing one of the penalties in accordance with the system. The committee raises its recommendations to the minister, and the decision is approved by him **[10]**."

These provisions indicate the protection of personal data by establishing responsibility for employees' violations of the system's provisions, including the rules that determine the responsibility of administrative controllers and the controls they must observe for controlling and processing personal data.

As for the administrative aspect, this protection is considered from two perspectives: the authority responsible for accountability and imposing the penalty (formal aspect) and the degree of the violation subject to penalty (substantive aspect), and the legal nature of the penalty imposed on the violator **[1]**.

From a formal perspective, the data controller responsible for regulating the behavior of employees dealing with personal data is tasked—with the help of a specialized committee—with recommending the penalty. The final approval of this penalty lies with the minister. This decision is always entrusted to an executive administrative authority **[26]**.

From a substantive perspective, the violation in question does not rise to the level of a criminal offense, as there is no need to prove the mental element or criminal intent. These are violations that are limited to the responsibility for negligence related to the failure to implement the policies set by the data controller to ensure safe personal data processing.

As for the legal nature of the penalty, it results from both the formal and substantive realities described above. Since the penalty required here is merely a matter of negligence—and the legislator has entrusted its imposition to an executive authority—it must take on a disciplinary

nature and does not reach the level of judicial nature, as the latter is confined to the judiciary's jurisdiction.

Practical Applications in Local and International Cases

At the outset of this section, we note that the modernity of the texts related to personal data protection—particularly in its contemporary sense—makes the field of application somewhat limited in terms of the number of practical cases involving claims for the right to privacy in personal data. Nevertheless, in this section, we present some applications of the administrative scope of personal data protection, with examples drawn from both local and international cases.

Applications in Local Cases

In this subsection, we discuss applications based on judgments issued in cases examined within the Kingdom of Saudi Arabia, as follows:

Cases Where a Ruling Confirmed a Violation of Protection

Case of Request for Name Modification on ID Card

The plaintiff filed a lawsuit before the administrative court in Makkah, requesting the defendant to annul the negative decision of the defendant, which rejected the plaintiff's request to the Civil Service Agency for adding his tribe to his national ID card. The case was registered with the court under number 5842/10/Q/for the year 1439H. The court issued its judgment to annul the defendant's decision. The reason for the court's ruling was that the defendant did not respond to the plaintiff's request to add his tribe to the relevant committee as per the system. Article 82 of the Civil Status Law stipulates the establishment of a subcommittee within the ministry with the task of resolving requests for correction or modification of civil status records From the reasoning behind this judgment, it becomes clear that the data processor (defendant) was held responsible for the failure to take the necessary action to protect personal data by processing it as requested by the data subject. Moreover, the failure in protection here translates into the defendant violating the rules of delegation within its structure and violating Article 4(4) of the Personal Data Protection Law.

Intellectual Property Claim for Cancellation

The plaintiff filed a lawsuit challenging the defendant's decision to accept the registration of a trademark in Class (35), which was identical to the plaintiff's trademark, registered under Classes (29, 30, 31, 32) **[31]**. The defendant argued that the trademark in question was registered under the services class, not the products class, while the plaintiff's trademark was already registered under the class for food products, agricultural products, mineral water, and carbonated beverages. The legal prohibition against registering similar marks does not apply in this case because the defendant's trademark registration is in the services class.

The relevant court concluded that the purpose of the legal prohibition on registering identical marks is to prevent confusion among consumers of the services or products offered by the business, and such confusion arises when the two marks are identical, regardless of whether they are registered in the same or different classes. Therefore, the court ruled to annul the defendant's decision to protect the plaintiff's trademark.

Commentary

It is evident from this case that the original claim involves a violation of protection from an

administrative perspective. The annulment of the decision means holding the control entity (represented by the relevant department in the Ministry of Commerce responsible for examining and accepting trademark registrations) accountable for its failure to apply the rules for trademark protection, especially those concerning the examination of similarity between the registered trademark and those submitted for registration. The court intervened at the request of an interested party (the plaintiff) to apply the rule and activate the legislative protection for the plaintiff's trademark.

Cases Where It Was Ruled No Violation of Protection (No Offense)

First Application

A lawsuit challenging an administrative decision issued by the Committee for Violations of the Credit Information System **[32]**, which included a ruling that the plaintiff had erred by providing the Saudi Credit Bureau (SIMAH) with information about a consumer without obtaining his written consent, as required by the Executive Regulations of the Credit Information System **[15]**. After hearing the case and reviewing the defenses, the court found that the plaintiff had signed a contract with the consumer, which included a clause in which the consumer acknowledged the plaintiff's right to share his data with SIMAH whenever requested. This meant that the plaintiff's action was lawful and consistent with the regulations, as the contract clause constituted the consumer's written consent. Therefore, the court ruled that the plaintiff had not made an error in providing SIMAH with the consumer's credit information, and thus the lawsuit was accepted, and the decision of the committee was annulled.

However, despite this, it was noted in the court's judgment that the court rejected the plaintiff's lawsuit **[32]**, and the decision was upheld by the Court of Appeals.

Commentary

On the Facts of the Case and Interpretation of the Judgment

Upon reviewing the facts of the case in order to interpret the judgment rejecting the lawsuit, it became clear that the initial decision by the Committee for Violations of the Credit Information System was based on the plaintiff's error in providing SIMAH with information about the consumer while withholding other negative information, which could lead to misleading disclosure about the consumer's true credit status.

This suggests that the appellate court's ruling to uphold the committee's decision was correct, but the court's reasoning contained a flaw. The judgment overlooked the fact that the committee's decision was based on misleading actions, and thus the court's reasoning was flawed despite the judgment being correct in substance. The plaintiff did indeed make a mistake by providing SIMAH with some information and withholding others, which was a clear violation of the system's regulations.

On the Implications for Personal Data Protection

The core of the plaintiff's claim was based on the right established in the Executive Regulations of the Credit Information System, which stipulates that no entity may provide personal data to another without obtaining written consent from the data subject. This principle is reinforced by the Personal Data Protection Law in various sections **[1]**.

Second Application

A lawsuit filed to compel the Ministry of Civil Service to amend the plaintiff's date of birth for employment purposes **[33]**. The plaintiff sought to have his date of birth corrected from 01/07/1376H to 09/05/1380H based on a decision by the Civil Status Committee and the Minister's approval. The plaintiff presented a medical report from the King Faisal Hospital in Taif, estimating his age through dental examination, in support of his claim. The defendant argued that the employment regulations specified that the age of an employee at the time of appointment should be based on the date of birth in the official document, and that any changes after 01/07/1409H should not be considered for employment purposes.

After hearing the case and reviewing the defenses, the court confirmed the plaintiff's date of birth as 1380H and found that, based on the documents submitted, the date of 1376H was irrelevant. However, the defendant's refusal to amend the date for employment purposes was upheld due to the regulations in place, which do not permit any changes after the specified date (01/07/1409H). Therefore, the court rejected the plaintiff's claim and upheld the defendant's decision.

Commentary

It is noted that this case does not directly address a violation of personal data protection but rather involves a request for the modification of personal data (the plaintiff's date of birth) as outlined in the first section of the Personal Data Protection Law. The plaintiff's date of birth was amended from 01/07/1376H to 09/05/1380H, and this amendment was officially recognized. However, the lawsuit focused on the rejection of this modification for employment purposes, leading to a judgment rejecting the claim.

This outcome confirms the administrative protection of personal data, as the Civil Status authority responded to the plaintiff's request to modify his personal data and the court upheld this modification. However, the defendant's refusal to amend the data for employment purposes reflects the protection of the system's rules, ensuring that all public employees receive their rightful benefits based on their personal data.

Applications in International Cases

In this section, we discuss some cases related to the administrative scope of personal data protection, whether those related to the prohibition of violating the jurisdictional rules of the controlling entity (administration) in personal data processing or liability for negligence due to the failure to implement policies ensuring secure processing.

In Principle: One of the requirements for secure processing is the obligation of the processing entity, under the supervision of the controlling entity, to remove and destroy personal data as soon as the purpose for collecting it has ended, especially if the data subject requests such action **[1]**.

First Application

A lawsuit filed by a group of plaintiffs against Google before the Court of Justice of the European Union, requesting that the company remove and destroy personal data attributed to them from many years ago. The justification for this request was that the data was no longer valid or accurate in representing the individuals at the time of the lawsuit.

The Court of Justice of the European Union issued its judgment on May 14, 2014, obliging

Google to acknowledge the plaintiffs' right not to document personal data attributed to them from a long time ago. Instead, Google was required to remove this data from its search engines, considering this to be a legal duty under the rules of secure processing, especially when accompanied by a request from the data subject **[30,34]**.

Commentary

This case illustrates the practical depth in the Saudi system, where the data subject has the right to request the controlling entity to destroy their personal data. This is considered one of the primary cases in which the controlling entity must take action to process the data by deleting it from all storage units upon the request of the data subject.

Entities that control personal data, regardless of the nature of their relationship with the data, are generally subject to the oversight of the Saudi Data and Artificial Intelligence Authority (SDAIA), which is the highest administrative body responsible for supervising and regulating data protection measures **[1]**.

Second Application

In a similar case, an Italian woman filed a lawsuit against Google, requesting the removal of a news article about her husband's death, which contained her personal name. The article had been published ten years prior to the lawsuit. She requested that the company remove the article from the results of Google search engines **[36]**.

Commentary

This application clearly demonstrates a violation of personal data protection. However, it is important to note that the violation is not directly attributed to an administrative controlling entity. Instead, the violation was committed by an individual, and it occurred outside the framework of an administrative entity's operations. Nevertheless, if we consider the nature of the personal data in this case, the violation of data protection principles can be attributed to companies that manage and process such data. Specifically, the case suggests that the failure to remove or delete personal data once its purpose has ended constitutes a violation of personal data protection principles.

This aligns with the Saudi system, which allows data subjects to request that controlling entities delete their personal data once its purpose has been fulfilled **[1,28]**.

Applications of Cases Involving Acknowledgment by the Administration

As previously mentioned, the controlling entity is obligated to provide necessary safeguards to protect personal data. When choosing a processing entity, the controlling entity must ensure that it selects one that provides the same guarantees. This means that both the controlling entity and the processing entity are responsible for protecting personal data from breaches, hacking, and theft.

In this section, we discuss two incidents in which the processing entity acknowledged personal data theft due to breaches and hacking **[27,29]**:

First Application

In 2007, the British Tax Authority acknowledged that it had lost two CDs containing personal data of around 25 million people.

Second Application

In 2008, the North London Health Service Authority acknowledged losing CDs containing personal data of 18,000 patients when they were mistakenly sent by mail.

Commentary on the Two Applications

Both incidents are similar in that they involve the acknowledgment by controlling entities of the loss of personal data stored under their custody.

From the perspective of Saudi regulations and the procedures of the Saudi Data and Artificial Intelligence Authority in overseeing the implementation of personal data protection laws, these two incidents represent clear violations of the provisions of the Personal Data Protection Law and the safeguards established by SDAIA for secure data storage and processing. These violations resulted in the loss of personal data protection concludes with the application of theoretical frameworks. From the study, several findings can be summarized as follows:

a. Personal data refers to information that can identify an individual, either directly or indirectly. The concept includes both a material and descriptive aspect. The material aspect is present when the data leads to identifying an individual, while the descriptive aspect adds qualitative characteristics such as political beliefs, religious views, or intellectual orientation.

b. The legal nature of personal data is represented by its role as a legal instrument that affirms an individual's legal existence and serves as a communication tool between the individual and the state. It is through this data that responsibilities are assigned, and rights and privileges are granted.

c. The study addresses the reference role of the Saudi Data and Artificial Intelligence Authority (SDAIA) and its relationship with the administrative bodies that carry out tasks on its behalf, outlining the specific rules for its interaction with those bodies and the responsibilities assigned to each body.

d. The study briefly discusses the forms of legal protection, including civil, administrative, and criminal protection.

It is clear that the differentiation between forms of protection follows a sequential order: civil protection comes first due to its connection with the specific regulatory texts, followed by administrative protection, which pertains to practical applications, and finally, criminal protection, which focuses on data, as admitted by each controlling entity in their respective applications.

Conclusions

The study on monitoring and tracking administrative precautions for penalties and accountability, though they differ in their objectives and jurisdictions.

a. The study highlights that administrative protection measures manifest in several ways, restricting the authorities or processing entities by rules related to the handling of personal data, whether in storage or processing. Administrative protection comes from the jurisdiction over data handling, as well as in the form of administrative oversight and accountability for public employees.

b. Based on the findings, the researcher recommends the following key points to

enhance administrative protection:

c. Activating the role of the Data Authority in monitoring and inspecting control and processing bodies to ensure compliance with the system in practice.

d. Each authority should establish field inspection teams responsible for investigating and monitoring violations of the system.

e. The researcher supports the possibility of transferring the supervision of personal data protection to the National Data Management Office after the current term of the SDAIA, considering the relationship between SDAIA and specific forms of personal data.

f. Establishing precise regulatory standards to ensure accurate monitoring of system violations.

g. The need to activate the organizational role of the SDAIA in preparing executive regulations for the Personal Data Protection Law and setting specific rules and procedures for administrative and organizational measures.

References

Azikiwe, H., Bello, A. (1443/2/9H). Personal Data Protection Law, Royal Decree No. (M/19) dated 9/2/1443H (Article 1/4).

Azikiwe, H., Bello, A. (1407/4/20H). Civil Status Law, Royal Decree No. M/7 dated 20/4/1407H (Articles 34, 35, 36).

Azikiwe, H., Bello, A. (1443/12/1H). Saudi Companies Law, Royal Decree No. (M/132) dated 1/12/1443H.

Azikiwe, H., Bello, A. (1435/1/22H). Sharia Litigation Law, Royal Decree No. (M/1) dated 22/1/1435H.

Azikiwe, H., Bello, A. (1443/5/26H). Saudi Evidence Law, Royal Decree No. (M/43) dated 26/5/1443H.

Azikiwe, H., Bello, A. (1437/2/19H). Saudi Associations and Charitable Institutions Law, Royal Decree No. (M/8) dated 19/2/1437H (Article 34).

Azikiwe, H., Bello, A. (2023). Executive Regulations of the Associations and Charitable Institutions Law issued by the National Center for Nonprofit Sector Development, Decision No. (T/2/2023) dated 04/01/2023.

Azikiwe, H., Bello, A. (1443/2/7H). Cabinet Resolution No. (98) dated 7/2/1443H.

Azikiwe, H., Bello, A. (1446/3/19H). Commercial Registry Law, Royal Decree No. (M/83) dated 19/3/1446H.

Azikiwe, H., Bello, A. (1443/2/8H). Functional Discipline Law, Royal Decree No. (M/18) dated 8/2/1443H.

Azikiwe, H., Bello, A. (n.d.). Executive Regulations of the Functional Discipline Law, Royal Decree (M15).

Azikiwe, H., Bello, A. (1391/2/1H). Employee Disciplinary Law, Royal Decree No. (M/7) dated 1/2/1391H.

Azikiwe, H., Bello, A. (1406/2/21H). Postal Law, Royal Decree No. (M/4) dated 21/2/1406H. Version February 6, 2025 submitted to Journal Not Specified 19 of 19

Azikiwe, H., Bello, A. (1423/5/28H). Trademark Law, Royal Decree No. (M/21) dated 28/5/1423H.

Azikiwe, H., Bello, A. (1429/7/5H). Executive Regulations of the Credit Information Law, Royal Decree No. (M/37) dated 5/7/1429H (Article 40/1).

Bateh, A. (2024). Legal Protection of Information Privacy. Dar Al-Nahda Al-Arabiya.

Daoud, I. (2017). Legal Protection of Personal Data: A Comparative Analytical Study. Journal of Legal and Economic Research, Faculty of Law, Alexandria University, Issue 1.

Al-Tahami, S. A. (2013). Delictual Liability in Personal Data Processing According to the UAE Civil Transactions Law. Paper presented at the Civil Transactions Law Conference, February 27-28, 2013.

Ibrahim, M. G. (2024). Legal Framework for Data and Information Security in the Digital Transformation Era. 1st edition, Dar Al-Ahram.
Dib, A.W. (2023). The Right to Protect Personal Data. 1st edition, Halabi Legal Publications.
Ayoub, P. A. (2009). Legal Protection of Personal Life in Informatics: A Comparative Study. 1st edition, Halabi Legal Publications.
Farooqui, M. O., Qureshi, T., Kisswani, N., & Mishra, D. K. (2024). Artificial Intelligence: Legal and Ethical Perspectives in the Health Care Sector. Science of Law, 2024(4), 8-14. https://doi.org/10.55284/sol.v2024i4.152
Naim, S. (2022). Legal Protection of the Right to Information Privacy: A Comparative Study. 1st edition, Modern Publishing House.
Fadhli, S. M. A. (2017). The Role of Administrative Environmental Control in Protecting the Aesthetics of Cities: A Comparative Study. 1st edition, Arab Center.
Labad, N. (2004). Administrative Law. 1st edition, Vol. 1, Dali Ibrahim Printing.
Tanago, S. A. (2018). Administrative Grievances in the Saudi Legal System: A Comparative Study with the Egyptian Legal System. Journal of Law Faculty Research, Issue 2.
Tanago, S. A. (2014). Basic Principles in Obligation Theory: Sources of Obligation. 1st edition, Manashat Al-Ma'arif.
Al-Tahami, S. A. (n.d.). Legal Protection of Personal Data: A Study on French Law.
Rammal, S. A. (2018). Privacy in the Digital Age. 1st edition, Halabi Legal Publications.
Abid, M. K. (n.d.). Nature of Violation of Personal Data for Users of Websites and Scientific Applications. University of Babylon.
Court of Justice of the European Union (2014, May 13). Google Spain v. AEPD Mario Costeje Gonzalez, Case C-131/12, D. 2014.1092.
Diwan, M. (1438H). Judicial Rulings Collection, Diwan of the Public Grievances. Case No. 2322/1/Q, 1438H.
Diwan, M. (1441H). Judicial Rulings Collection, Diwan of the Public Grievances. Case No. 4529/1/Q, 1441H.
Diwan, M. (1435H). Judicial Rulings Collection, Diwan of the Public Grievances. Case No. 1658/10/Q, 1435H.
Court of Justice of the European Union (2014, May 13). Google Spain v. Mario Costeje Gonzalez, Case C-131/12, D. 2014.1092.
SDAIA. (n.d.). OfficialWebsite of the Saudi Data and Artificial Intelligence Authority. Retrieved from https://sdaia.gov.sa
Teremetskyi, V. I., Bodnar-Petrovska, O. B., Dir, I. Y., Petrenko, A. A., & Lien, T. V. (2025). European Union's Legal System: Essential Features and Tendencies of Modern Development. Science of Law, 2025(1), 1-6. https://doi.org/10.55284/sol.v2025i1.160
Aawsat. (n.d.). Article on Privacy and Data Protection.