The Extra-Territorial Effect of the Saudi Data Protection Law and the EUGDPR-A Comparative Analysis

Anas Mohameden
Senior Legal Counsel, Riyadh, Kingdom of Saudi Arabia
DOI: 10.55662/CYLR.2025.4101

Abstract

The primary aim of promulgating the General Data Protection Regulation (GDPR) was to establish a suitable privacy deterrent for individuals' rights across the EU. Therefore, a substantial obstacle to conformity for overseas businesses that process the personal data of European Union citizens and expatriates is addressed through this enactment. This article highlights the new norms governing the extraterritorial realms of securing sensitive data and explains the principles of data protection. In addition, it examines the scope of the GDPR's application, highlighting its territorial reach and the entities to which the law applies. Furthermore, this highlights the impact of GDPR on international law, encompassing subsequent jurisdictions. Qualitative research methodology employs document analysis from various data sources throughout the development of this article. Those sources include regulations, conventions, books, journal articles, etc. Hitherto, the article explores the significance of data privacy. In the digital age, exploring personal data protection law in Saudi Arabia is timely and essential. This law is designed to protect the privacy and rights of individuals, ensuring that their personal information is collected, processed, and stored in a lawful and transparent manner. This article examines the specific provisions, extraterritorial aspects, and implications of the Personal Data Protection Law (PDPL) 2021, with a focus on its alignment with Shariah principles. Additionally, it highlights the significant role played by the Saudi Data and Artificial Intelligence Authority (SDAIA), mainly through the National Data Management Office, in safeguarding personal data. By

This work is licensed under CC BY-SA 4.0.

thoughtfully comparing Saudi policies to the European Union's General Data Protection Regulation (GDPR), we also identify areas for improvement. The insights provided here aim to assist Saudi legislators in reevaluating the Personal Data Protection Law and encourage the development of proactive strategies to address and manage data incidents and breaches. Fulfilling trust and security for all citizens is vital to enhancing commitment to privacy in the rapidly evolving digital landscape.

Keywords: *Kingdom of Saudi Arabia, EUGDPR, Personal data, Extraterritorial Effect, International law.*

Introduction

The history of data protection law dates back over 40 years, beginning with the adoption of the first data privacy act in Germany in 1970. A distinction can be made between the development of data protection at the national and regional levels, particularly in the EU. At the national level, data protection initiatives began in Germany with the Hesse Act in 1970, followed by Sweden in 1973, and then Norway and Denmark in 1978. These early steps laid the groundwork for a broader commitment to privacy rights. In 1981, the European landscape took a significant stride forward by adopting the EC Convention 108, which aimed to safeguard individuals' fundamental freedoms and privacy by ensuring that automated personal data processing respects their rights.

As technology advanced, so did our approaches to data collection and protection. In 1995, the EU established a Data Protection Directive that set essential minimum standards for member states. The dialogue around improving these protections lasted for years, culminating in the adoption of the General Data Protection Regulation (GDPR), which came into effect on May 25, 2018, and represents a significant leap forward in our approach to data protection. Today, the EU stands proud as a global leader in establishing the most rigorous and influential data protection framework. Treating personal data as a fundamental right in the EU Charter showcases a profound commitment to individual privacy, fostering trust in our ever-evolving digital landscape.[i]

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

This vital evolution underscores our collective responsibility to protect personal dignity and privacy, empowering everyone in this rapidly changing world. Article 16(1) TFEU serves as a reminder that our rights are at the forefront of this initiative.

Personal data retention is essential in shaping the scope and effectiveness of our legal protections. It empowers individuals to control their information while holding organizations to a high standard of responsibility to protect it from unauthorized access, use, or disclosure. With decades of experience dating back to the 1980s, the EU has laid the groundwork for many countries to journey toward a future where privacy takes center stage and is held in high regard. The General Data Protection Regulation (GDPR) is an inspirational model for crafting robust data protection legislation worldwide.[ii] Notably, the Kingdom of Saudi Arabia (KSA) closely aligns its definition of personal data with that outlined in Article 4(1) of the GDPR.[iii]

Under the GDPR framework, "personal data" refers to any information relating to an identified or identifiable individual. This means a person can be recognized directly or indirectly through their name, identification number, location data, or distinctive traits that reflect their identity.[iv]

In KSA, personal data is thoughtfully classified into three categories. The first is regular personal data, which includes general, non-confidential information that does not reveal sensitive personal details. This entails information such as names, providing a solid foundation for privacy protection in today's digital world. It is crucial to prioritize the protection of individual identities and cultivate a culture rooted in respect and safeguarding personal privacy. Sensitive information, such as dates of birth, social status, and educational levels, must be handled with the utmost care.[v]

The alignment of the KSA's definition of personal data with the GDPR's definition is paramount. This alignment establishes a unified terminology and mutual understanding, which are essential for effective international communication and cooperation in data privacy matters. It reflects KSA's unwavering commitment to internationally recognized standards and best practices in data protection, fostering legal consistency and harmonization.[vi]

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

Moreover, classifying personal data into regular and sensitive categories within KSA law emphasizes the critical need to categorize data based on sensitivity. This classification is instrumental for organizations as it directs them to implement appropriate protection and security measures for varying data types. Additionally, KSA is committed to harmoniously balancing the utility of data and the protection of privacy rights. This determination is crucial for organizations operating in the KSA, particularly those with international connections. Embracing data protection measures that align with GDPR standards is essential to ensure compliance with local laws. This alignment establishes a solid framework for responsible data handling and promotes smooth international data flows while protecting the rights of natural persons.

Protecting individual privacy is a vital commitment for any nation, and I am excited to share how the Kingdom of Saudi Arabia (KSA) is making significant strides in this area! Sensitive personal data encompasses various types of information that can reveal a great deal about an individual, including their racial or ethnic background, political beliefs, religious or philosophical views, family history, and even health conditions. By prioritizing these crucial aspects, the KSA fosters a secure data environment that not only upholds but actively protects individual privacy across all sectors, especially in healthcare, where safeguarding health information is paramount. Additionally, biometric data—like facial recognition and fingerprint information—plays a pivotal role in personal identification. With the measure, The growing reliance on the Internet and various technological tools has significantly transformed the collection and dissemination of personal data. This evolution has led to the processing of personal data that transcends national borders, presenting considerable challenges for domestic lawmakers. A key development in this area is the General Data Protection Regulation (GDPR), which came into effect On May 25, 2018.

The GDPR introduces critical regulations that can majorly impact corporations globally, particularly those that handle the personal data of individuals in the European Union. Extensive research has been conducted to highlight the new risks that data processors may face. The implementation of GDPR compliance has become a significant concern for businesses worldwide. This regulation applies to companies based in the EU. It extends to non-EU businesses that provide goods or services to EU residents, highlighting its significant

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

influence in today's digital environment.

This article explores the extraterritorial application of GDPR and the associated challenges. One key aspect is how data controllers operating in different countries, subject to various jurisdictions, can effectively navigate GDPR requirements. Collaborating with the jurisdictions where these data controllers reside is essential to address the complexities of applying this regulation beyond its natural borders. Therefore, enforcing GDPR should not be viewed as a unilateral initiative; rather, it necessitates international cooperation and agreements.

A crucial question arises: Does the EU possess the necessary tools to ensure universal compliance with the GDPR? If not, what strategies can be developed to bolster compliance with GDPR beyond EU borders? This article aims to explore various relevant issues across its sections, addressing critical questions and examining potential pathways for the effective enforcement of the General Data Protection Regulation (GDPR) on a global scale or specifically within the European Union's jurisdiction.

The Legal Bindings of an Extra-Territorial Scope as Enshrined in the EU GDPR

The European Union is recognized for its proactive approach to establishing laws that safeguard the rights of its citizens, demonstrating a commitment to upholding the fundamental rights of all individuals across its member states. A cornerstone of this endeavor is the Charter of Fundamental Rights of the European Union, adopted in 2000, which enshrines a broad spectrum of rights universally applicable to all individuals. Among these fundamental rights is the imperative to protect personal data, a critical aspect of individual privacy in the digital age. The Charter explicitly states, "Everyone has the right to the protection of personal data concerning them," highlighting the significance placed on data privacy.[vii]

In addition to the protections afforded by the Charter, certain fundamental rights are established through statutes and treaties agreed upon by member states, collectively referred to as 'primary law' within the EU legal framework. The General Data Protection Regulation (GDPR) represents a pivotal regulatory mechanism, one of its standout features being its

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

extraterritorial reach, which ensures that personal data is protected regardless of where it is processed. This broad territorial scope strengthens data protection standards and fosters a cohesive legal framework that spans global boundaries, actively safeguarding privacy rights within and outside the EU.[viii]

According to Article 3(2), these EU rules apply to non-EU entities that handle the data of EU individuals in two key scenarios: first, when they offer goods and services to people in the EU, and second, when they monitor the behavior of individuals within the EU. This intentional design empowers individuals by upholding their rights and enhancing data security.

Additionally, Article 2 outlines that the GDPR covers processing personal data through automated means and the manual processing of personal data. This comprehensive scope reflects a strong commitment to safeguarding personal information, reinforcing the importance of privacy in an increasingly interconnected world. With these regulations in place, we can look forward to a more secure and respectful environment for personal data, benefiting everyone involved in the filing system or are intended to form part of a filing system. It also applies to personal data processing in the context of establishing a controller or a processor in the Union; regardless of where processing occurs, the General Data Protection Regulation (GDPR) provides essential guidelines for anyone handling personal data. In the following paragraphs, we will examine how the GDPR applies to operators located outside the EU, highlighting its global significance.[ix]

Like other data protection regulations worldwide, the GDPR introduces specific rules and principles that must be followed when handling personal data. Article 5 of the Regulation outlines these core principles, which we will examine in more detail. Organizations and individuals impacted by the GDPR have a significant responsibility to ensure they follow these principles closely when processing data that can identify individuals.[x]

Among these principles, the notion of lawfulness stands out. Article 6 emphasizes that lawful processing hinges on obtaining explicit consent from data subjects for specific purposes. Additionally, transparency is key—data controllers must openly apply the notion. Organizations must clearly outline the types of data they collect in their privacy policies.

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

Adhering to these guidelines fosters a respectful and secure environment for managing personal data, which is essential in today's digital landscape.[xi]

A key principle is purpose limitation: personal data should only be gathered for a specific purpose, and data controllers should only collect what is necessary to achieve that purpose. Additionally, the GDPR provides greater flexibility for data processing when it serves archival purposes, scientific research, or historical insights. The regulation clarifies that personal data must be collected for explicit and legitimate purposes, ensuring that any further processing aligns with these original intentions.

Moreover, the principle of data minimization emphasizes that organizations and data controllers should only handle personal data, which is essential for achieving specific objectives. This approach protects individuals' privacy and enhances the overall efficiency and integrity of data management practices. By adopting these practices, we play a crucial role in creating a digital environment that prioritizes trust and respects personal data. There are significant advantages to this approach! For instance, in the unfortunate event of a data breach, unauthorized individuals will only access a limited amount of information. Additionally, embracing data minimization enhances security and simplifies maintaining accurate and current data.

Let us discuss accuracy, which is crucial in safeguarding our data. This principle encompasses three key components: correctness, currency, and completeness. The General Data Protection Regulation (GDPR) emphasizes the importance of accuracy, stating that every reasonable effort must be made to eliminate or rectify incomplete or inaccurate data without delay. Personal information must be:

1. Accurate and, when necessary, kept up to date.
2. Erased or rectified promptly if found to be inaccurate. Organizations should implement a robust storage limitation policy to maintain the relevance and security of our data. It is essential to securely delete information that is no longer necessary. By doing so, these organizations can play a vital role in protecting our digital lives, fostering a collaborative effort to ensure that our data remains secure and trustworthy.

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

The principles of integrity and confidentiality, as outlined in the GDPR, emphasize the importance of security in handling personal data. The GDPR requires that personal data be processed to ensure the implementation of appropriate security measures, thereby safeguarding against unauthorized access, unlawful processing, and the accidental loss, destruction, or damage of data through effective technical and organizational measures.[xii]

The EU remains dedicated to enacting laws that protect its citizens by upholding the fundamental rights of all individuals. This commitment is reflected in initiatives such as the Charter of Fundamental Rights of the European Union, first published in 2000, which codifies numerous rights that apply universally to everyone.[xiii] We can work towards a safer and more equitable world by reinforcing these principles.[xiv] The EU Charter recognizes personal data protection as one of the fundamental rights. It explicitly states that "everyone has the right to the protection of personal data concerning him or her."[xv]

Certain fundamental rights are established by statutes and treaties among member states, constituting the 'primary law' of the EU. For example, the General Data Protection Regulation (GDPR) ensures that primary laws are upheld. The territorial scope of the GDPR aims to prevent violation of personal data violations jurisdiction. This scope encompasses two aspects: the first pertains to personal data processing with a connection, and the second covers any processing within the European Union. The Regulation applies to personal data processing that is conducted wholly or partly by automated means, as well as to the non-automated processing of personal data that is part of a filing system or is intended as this Regulation governs the processing of personal data in the context of establishing a data controller or a processor, ensuring that personal data is handled with the utmost care and legality.

Offering of Goods and Services

"The act of targeting will make you targeted."
According to Article 3(2)(a) of the General Data Protection Regulation (GDPR), the regulation applies not only to operators within the European Union (EU) but also extends its reach to operators based outside the EU. Specifically, it encompasses those instances in which the

This work is licensed under CC BY-SA 4.0.

personal data of individuals residing in the EU is processed by these external operators, particularly when it pertains to the "offering of goods or services" to those individuals—even if the offerings are provided free of charge.

This framework for jurisdiction is well established; however, it raises significant controversies in the digital landscape. For example, the principle of jurisdiction is echoed in the Brussels Regulation. Here, it is stated that if a professional (business or entity) actively directs its activities toward consumers residing in a specific Member State, those consumers are entitled to the protective and non-negotiable principle at play here, which suggests that "you are subject to EU law if you actively target residents within the EU." This highlights the complex relationship between globalization and regulatory compliance, emphasizing the challenges businesses face when operating in the EU market. Thus, the foundation for this jurisdiction is quite understandable.[xvi]

However, the rationale can become more nuanced in online sales and universally accessible websites. It raises the question: "Who is targeting whom in these transactions?" For instance, does the consumer seek out the website, or is the website actively appealing to the consumer? Recital 23 of the GDPR clarifies that such targeting should be "apparent." To demonstrate this intention, factors such as the website's ability to facilitate orders in the language or currency of specific Member States or explicit references to EU customers can be significant. Additionally, the case law under Brussels 1 Further outlines very relevant aspects of targeting, including the international nature of the activity and the mention of itineraries from other Member States. This comprehensive understanding can assist businesses in navigating the intricacies of compliance in an increasingly interconnected feature; discussing the international nature of certain activities, we can see clear indicators such as itineraries from various Member States, the presence of international telephone codes, and the use of top-level domain names that differ from the Member State where the trader is established.

An intriguing question is whether courts will necessitate "active dis-targeting" from the operators. If we draw from the US legal landscape, a US court asserted jurisdiction over a Canadian website when American users used it. The website did not actively block access; instead, it merely relied on users to identify as Canadian residents to gain entry.

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

As Svante wisely suggests, leveraging geolocation technologies could provide a promising solution. While it may not be used solely for monitoring, gaining consent from users is always essential when accessing their information. Considering data processing within the European landscape, it is crucial to emphasize the importance of transparency and respect for individual privacy. This approach fosters trust and understanding, especially as we navigate complex legal frameworks.[xvii]

A pertinent question arises regarding the forms of processing EU data exempt from the GDPR: what falls outside its scope? There are only a limited number of answers to this significant inquiry.

The concept of monitoring encompasses a range of definitions. It includes instances where natural persons are tracking online education, which may involve the successive use of personal data processing techniques, such as profiling. Profiling refers to the analysis and prediction of personal preferences, behaviors, and attitudes based on collected data, leading to decisions made about individuals. According to this definition, most data processing activities involving EU citizens will trigger the application of GDPR when conducted by businesses. However, the Regulation must not apply to non-EU entities conducting such activities; the definition granted to "personal data" highly affects the limits of the concept of "monitoring." They comprise, but are not limited to, the user's preferences, interests, location, and movements. The regulation states that online identifiers, such as IP addresses and cookie identifiers, can serve to identify natural persons and thus be considered personal data. Therefore, the monitoring does not significantly concern social networks, email providers, or search engine operators but targets the vast majority of websites that collect clickstream data (surfing behavior), either through the use of cookies, ad banners, or JavaScript.[xviii]

Conversely, Article 3(2) significantly expands the scope of European Union data protection norms unilaterally, to a greater extent than any other jurisdiction has done to date. Even if it is related to the alleged voluntary ethics of the operator to justify the application of the regulation, in practice, the application of the regulation almost "follows" the EU data. The question of which legal basis underpins the legitimacy and authority of the regulation invites

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

significant scrutiny. If we assume that the abrupt enforcement of EU rules on a multitude of websites worldwide is indeed permissible, we must delve deeper into the complexities involved.

Examining the Challenges of Legal Basis and Legitimacy in Extraterritorial Applications of the EUGDPR

The internet's inherently borderless nature underscores the need for comprehensive regulation, particularly regarding the unilateral extension of EU law to non-EU operators. The internet, operating beyond geographical constraints, necessitates a corresponding borderless approach to legal enforcement. The efficacy of data protection in a digital context starkly contrasts with the limitations of traditional territorial jurisdiction.[xix]

In this ambitious endeavor, the EU is pushing the envelope further than any other jurisdiction has dared to venture, establishing some of the highest global standards for data protection. However, this formidable regulatory framework tests the essence of state sovereignty and places a disproportionately heavy burden on international businesses. Companies worldwide face the daunting prospect of adhering to stringent EU regulations while managing the escalating risks of hefty administrative fines for non-compliance.

A crucial question emerges as we navigate this complex landscape: on what legal grounds can the EU justifiably extend its authority over entities not based within its borders? Operators justify or legitimize these new self-acquired powers in the eyes of the world. The unilateral expansion of jurisdiction outside the boundaries is a phenomenon that is commonly recognized by most countries. In criminal matters, extraterritorial claims must adhere to specific guidelines to ensure compliance and respect for jurisdictional boundaries. This is particularly relevant within the context of the European Union, where member states must navigate these complex legal frameworks.[xx]

Exemption from the Scope of Application of the EU GDPR

When considering the material scope of the General Data Protection Regulation (GDPR), Article 2, Section 2 outlines four critical exceptions where the regulation does not apply. One

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

key exception pertains to security policies and criminal prosecution, recognizing that certain data processing activities in these domains may necessitate different regulatory considerations.[xxi]

From an economic perspective, the most significant exemption is delineated in subsection ©, which states that the GDPR does not apply to the processing of personal data by an individual engaged in activities that are purely personal or of a household nature. This exception emphasizes the need for clarity in how we interpret the boundaries of personal data usage.

To elaborate, this concept encompasses many activities typically associated with private life—such as processing data for leisure pursuits, engaging in hobbies, planning vacations, or participating in entertainment events. It also includes using social networking platforms and managing personal information collections, like addresses, birthdays, and notable dates, including anniversaries.

However, it is critical to note that this exemption does not extend to instances where the data processing overlaps with business information. If the processing involves any business-related data, the GDPR provisions become applicable, emphasizing the necessity for individuals to distinguish between their personal and business activities to comply with data protection.[xxii]

Regulations Effectively

By grasping the subtleties of the GDPR framework, individuals and organizations can more adeptly navigate the complexities of data protection while recognizing the limitations regarding the regulation's applicability in personal contexts.

International Law through the EUGDPR

The GDPR's extraterritoriality significantly expands the applicability of EU data protection law beyond its borders. However, an obstacle within international law is that even with the newly implemented consistency mechanism, the pros and cons of international and EU law may remain unresolved.

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

The Jurisdictional Aspirations of EUGDPR

The GDPR features a broad jurisdictional assessment. Specific principles under international law determine when a state's extraterritorial reach is permissible.[xxiii]

Bases for significantly expanding national Law

Several traditional bases have been employed to establish jurisdiction, including the principle of territoriality, the nationality principle, the passive personality principle, and the protective principle. To be more specific regarding online conduct, states have increasingly exercised jurisdiction based on variations of established principles, such as the objective territoriality test and the effects doctrine.[xxiv]

Territoriality and Nationality

Territoriality and nationality are the principles most frequently invoked. States can thus affirm jurisdiction over acts committed both within their borders and by their nationals, even if those acts occur outside of the state's physical territory. A notable variation of the traditional concept of territoriality is the "objective territoriality principle," which permits a state to assert jurisdiction over actions initiated abroad but completed within its territory, mainly when a key element of the conduct occurred within the state. The jurisdictional test outlined in the Directive appears to embody the objective territoriality principle, as it enables European regulators to assert jurisdiction over foreign websites or online service providers based solely on the location of their equipment or servers within the EU.[xxv]

Passive Persona Jurisdiction and the Protective Principle

States not only establish jurisdiction over acts committed abroad by their nationals but also have the ability to assert jurisdiction for acts committed against their nationals by foreigners. This is referred to as the passive personality principle, which allows states to exercise authority based on their connection to the victim of unlawful conduct. While this principle has typically been applied to serious crimes, such as terrorist attacks or assassinations, there have been instances where it has been used in civil law contexts as well. Although traditionally cautious about employing this principle, recent developments in U.S. courts have seen it adopted in specific cases, particularly concerning acts of terrorism.[xxvi]

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

Additionally, the protective principle broadens this concept by enabling the state to safeguard itself from harmful actions outside its borders.

The Effects Doctrine

Moreover, under the "*effects doctrine,*" states can establish jurisdiction when conduct outside their territory has significant repercussions within their borders. This principle allows for a proactive approach to jurisdiction, ensuring states can effectively address and mitigate external threats inside the state. This notion is narrowly associated with the "objective territoriality idea"; however, it does not involve any element of the conduct being regulated within the state's territory. The effects doctrine is generally based on establishing jurisdiction under international law, which is controversial. Even though it's faced with some pushback from legal experts, it's become a standard approach when it comes to actions that happen online.[xxvii]

When asserting international jurisdiction, simply meeting one of the bases doesn't automatically make the action acceptable. According to the current understanding of international law, the party that wants to claim jurisdiction must explain why it makes sense to exercise extraterritorial jurisdiction based on the specified bases. The Third Restatement of Foreign Relations Law lists various factors courts should consider in decision-making. It reflects a trend restricting jurisdiction use in U.S. domestic law, which has now become a principle of international law. Several factors contribute to this trend, including (1) the degree to which the activity is connected to the country attempting to regulate it, particularly whether it has a "substantial, direct, and foreseeable effect"; (2) the relationships between that country and the individual involved; (3) the nature of the activity, its significance to the regulating state, and the extent to which other states also regulate it; (4) the existence of justified expectations that may be either protected or harmed by the regulation; (5) the significance of the regulation to the international system; (6) the alignment of the regulation with the traditions of the global system; (7) the extent to which other states may have a vested Interest in regulating the activity and the probability of conflicts with regulations established by other states are key considerations. If evaluating these factors suggests that the extraterritorial application of the relevant law would be unreasonable, courts are likely to rule against such application.[xxviii]

This work is licensed under CC BY-SA 4.0.

The principles outlined in the Restatement closely align with the concept of comity, often described as the "golden rule" among nations – that is, each state should respect the laws, policies, and interests of other states in the same way it would like its own rules to be respected. Comity generally dictates that states should refrain from applying their laws extraterritorially against foreign citizens when those laws conflict. When two states hold concurrent jurisdiction over when determining jurisdiction in data protection and internet-related cases, a balancing test should identify which state has more substantial interests. Key factors include where the data controller is based, where data is processed or stored, where the wrongful act occurred, the residence of the data subject, and the use of cookies in another state. Typically, jurisdiction is presumed based on the location of the data controller or where a marketing email is received, aligning with the territorial principle and effects doctrine. However, weaker connections, like using a single intricate landscape of data protection regulation, particularly regarding the General Data Protection Regulation (GDPR) and its extra-territorial application, have attracted considerable scrutiny, especially for non-European Union (EU) media companies. When evaluating claims of jurisdiction, regulators typically concentrate on the whereabouts of the data controller, which serves as a cornerstone for asserting their authority.[xxix]

For a media company outside the EU, it is crucial to leverage various legal principles such as the objective territoriality principle, the passive personality principle, and the effects test when determining the applicability of GDPR. Each of these legal frameworks presents a nuanced approach to jurisdiction. However, a compelling argument suggests that such claims may be deemed unreasonable under the frameworks outlined in the Third Restatement, potentially infringing upon the principles of comity recognized in international law.[xxx]

To effectively challenge the enforcement of the GDPR, a non-EU media company would need to present a strong case demonstrating that compliance would clash with existing U.S. laws or regulations. For instance, invoking the First Amendment, which safeguards free speech and press, could illuminate the publisher's paramount interests in free expression. This argument posits that these interests should take precedence over the European Union's commitment to protecting the privacy rights of its citizens.

This work is licensed under CC BY-SA 4.0.

In parallel, the extra-territorial scope articulated in the Saudi Personal Data Protection Law of 2021 signifies a global transition towards more stringent data privacy measures. As the conversation surrounding data protection intensifies in contemporary discourse, the complexities of international compliance pose significant challenges for organizations operating across borders.

Various jurisdictions have enacted data protection laws to safeguard personal information, including names, addresses, and identity numbers. Protecting this data is crucial, as it can be misused by malicious actors and unauthorized individuals to achieve their objectives. Consequently, governments and regulatory bodies have recognized the importance of data in the modern landscape and the necessity of its protection.[xxxi]

In Saudi Arabia, while there were existing laws aimed at protecting individual data, notable gaps remained. To address these shortcomings, the Personal Data Protection Law (PDPL) was introduced in September 2021. This article seeks to discuss the provisions of the PDPL in Saudi Arabia, utilizing a descriptive and analytical approach. This article dives into the essential components of the new Personal Data Protection Law (PDPL) and evaluates its effectiveness in safeguarding personal data. We'll explore the law's provisions and analyze its adequacy and efficiency. Notably, the PDPL shines in some key areas, such as extending protections to deceased individuals, which is commendable. Additionally, its rigorous stance on data transfers outside the Kingdom demonstrates a strong commitment to ensuring adequate protection for everyone.[xxxii]

As we embrace this exciting digital transformation era, technology seamlessly integrates into every facet of our lives. From cashier-less stores like Amazon to instant communication through platforms like WhatsApp and Twitter, it's fantastic to see how interconnected we are! While these advances embrace exciting opportunities in our digital age, it's essential to remain mindful of the challenges, especially regarding privacy and protecting our personal information.

The introduction of the Personal Data Protection Law (PDPL) marks a pivotal advancement in addressing these vital concerns. With such thoughtful legislation in place, we can approach

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

the digital landscape with renewed confidence and optimism. It ensures that our rights are not just acknowledged but also actively safeguarded.[xxxiii]

Data protection has emerged as a crucial topic today, especially following the enactment of various personal data protection laws across different jurisdictions. We often overlook that our names, addresses, and identity numbers are forms of personal data that require diligent protection. Understanding this is vital, as unauthorized access can lead to misuse by individuals with ill intentions.

Recognizing the importance of data in our modern lives, governments and regulators worldwide have acted swiftly. It's fantastic to see the ongoing efforts to protect personal data, which is crucial in our digital age! In September 2021, Saudi Arabia took a significant step forward by launching its Personal Data Protection Law (PDPL). This law highlights the nation's dedication to securing individuals' privacy and establishing a safer digital environment. With 43 thoughtfully crafted sections, the PDPL will officially come into effect 180 days after its publication in the official gazette, demonstrating a proactive approach to privacy protection.

Before the enactment of the PDPL, it's important to note that individuals' data were not without protection. Saudi Arabia has several existing laws safeguarding personal information. This article will delve into how these laws provide varying levels of security for individuals, showcasing the foundation upon which the new law is built.

The Basic Law of Governance

It was primarily introduced in 1992 and serves as a cornerstone for these efforts. It recognizes the right to privacy as paramount, affirming its significance across different contexts. Together, these measures reflect a strong commitment to fostering and enhancing privacy for all citizens in Saudi Arabia.

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

Article 37 states:

"Dwellings are inviolate. Access is prohibited without their owners' permission. No search may be made except in cases specified by the Law."[xxxiv]

Furthermore, Article 40 of Basic Law recognizes the protection of personal communication in this digital age. It states:

"The privacy of telegraphic and postal communications, as well as telephone and other means of communication, shall be inviolate. There shall be no confiscation, delay, surveillance or eavesdropping, except in cases provided by the Law".[xxxv]

This article is essential because it covers all means of communication, including modern means such as email and new chat apps.

Law of Criminal Procedures (2013)

The Law of Criminal Procedure confirms the protection of privacy provided by the Basic Law of Governance. It provided more detail. Article 41 states:

"The privacy of persons, their dwellings, offices, and vehicles shall be protected. Privacy protects his body, clothes, property, and belongings. The privacy of a dwelling covers any fenced area or any other place enclosed within barriers or intended to be used as a dwelling".[xxxvi]

It broadens the protection afforded to homes to encompass the workplace and means of transportation. It defines "homes" as "any place enclosed within barriers or intended to be used as a dwelling."

Moreover, the article further states:

"Mail, cables, telephone conversations, and other means of communication shall retain personal

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

communications, like phone calls and messages, are meant to be private and should not be monitored or accessed without an apparent legal reason and for a limited time. This means that law enforcement can only look into these communications if they have a specific order explaining why they need to"[xxxvii]

The laws regarding what constitutes a *"home"* and what personal belongings fall under that protection are ambiguous. Neither specific laws nor past legal cases clearly define what constitutes personal belongings, which can create confusion. For instance, some laws prohibit the invasion of someone's private communications; however, they do not necessarily protect all the information stored on a person's phone or device. This leaves certain areas vulnerable, as these laws may not provide enough protection against unauthorized access.

The Anti-Cybercrime Law, established in 2007, aims to protect personal information from various online threats such as fraud and spying. It addresses issues such as using computers for deceitful purposes and misusing camera devices for defamation. These laws are intended to keep people's private information safe, but gaps still need to be addressed for better protection. Crimes such as hacking. As this research focuses on protecting personal data and privacy in general, the discussion here will concentrate on the provisions that pertain to individuals' privacy.[xxxviii]

Article 3

Primarily, article 3 states:

"Any person who commits any of the following cybercrimes shall be subject to imprisonment for a period not exceeding one year and a fine not exceeding 500,000 riyals, or either penalty: (1) Spying on, or interception or reception of data transmitted through an information network or a computer without legitimate authorization. (2) Unauthorized access to threaten or blackmail any person into compelling first paragraph prohibits various actions regardless of the security status of the data if there is no lawful authority present. It highlights the prohibition against spying and intercepting data that may be transmitted. The second paragraph makes it a criminal offense to gain access to a computer with the intent to blackmail or threaten another party. Such unauthorized access typically

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

targets sensitive and valuable information, so the law criminalizes unauthorized entry into someone's private space. It is a serious matter that we must address with care."[xxxix]

The fifth paragraph takes an essential step in protecting personal information by criminalizing the misuse of technology to defame or harm others. A significant libel case highlighted this when a woman made defamatory statements with serious consequences. The fourth paragraph emphasizes the critical role of privacy as we navigate our rapidly advancing technological landscape.

In his dissertation, Almebrad posed insightful questions about the clarity of this paragraph. What exactly defines an invasion of privacy? Is the legal framework limited to privacy violations via a mobile phone, or does it extend to other devices like cameras, recording devices, or GPS? While answers may generally come from a limited number of published cases, one example is a case involving a defendant who took and shared a picture of an 11-year-old girl in a store, which the court ruled as an apparent invasion of privacy.[xl]

Moving forward, Article 4 establishes that anyone engaging in cybercrimes related to these issues could face imprisonment, reinforcing our commitment to protecting privacy rights. of three years or less and a fine not exceeding 2,000,000 riyals, or either penalty:

"*Illegal access to bank or credit data, or data about the ownership of securities to obtain data, information, funds, or services offered.*"

This article protects individuals' banking and credit information. It criminalizes mere illegal access, regardless of whether the accused has stolen money from his illicit access.[xli]

Article 5

Article 5 states that anyone involved in any of the following cybercrimes shall be imprisoned for a period of four years or less and a fine not exceeding 3,000,000 riyals, or either penalty:

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

1- "*Unauthorized access to cancel, delete, to destroy, to leak, to damage, to alter, or to redistribute---*

A significant discussion is underway regarding the definition of "private data," and Almebrad has raised an essential question regarding its implications. Unfortunately, we have yet to receive clear guidelines on what qualifies explicitly as private data, which leaves some ambiguity about the information that falls within this category.

On a positive note, the E-Transaction Law is structured to establish a robust framework for electronic transactions and signatures. It provides vital guidance for navigating the complexities of our digital landscape. While the law does not explicitly define personal information, it lays down fundamental rules for processing electronic data, ensuring the reliability and integrity of all transactions conducted electronically.

Regarding data storage, the law and its associated regulations clearly outline essential guidelines for protecting electronic data. This is a crucial moment as we work together to enhance the security and trustworthiness of our digital interactions. We must stay informed and engaged to embrace these critical developments fully.

We must maintain clarity and focus regarding relevant laws, regulations, or procedures for storing traditional (non-electronic) data. However, no indication of which existing laws can be used for this one exists. Moreover, electronic data should be stored. The executive regulation outlines essential guidelines regarding the retention and access of electronic transaction data. It mandates that any data retention period specified by laws or regulations must be adhered to, with a requirement for secure storage throughout that duration. This ensures that all data related to electronic transactions is kept for at least the legally required timeframe.

Regarding data access, the regulation establishes clear conditions that institutions must follow when handling stored electronic data. Access to this data should be restricted to designated employees who require it for their work, thereby enhancing data privacy and security.

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

Furthermore, all employees must be bound by the institution's standards for protecting the confidentiality of data and documents.[xlii]

Additionally, institutions must implement appropriate technical measures to log in to any instances of access to or modification of electronic records. However, the regulation does not specify detailed instructions regarding the maintenance of these access logs or the duration they should be retained. These measures aim to safeguard electronic transaction data while ensuring compliance with relevant laws.

Conversely, the institution that maintains the records is not entitled to enable third parties to access the records without previous agreements between or among the parties.

The E-Transaction Law and its executive regulations provide essential legal protections for individuals' electronic data and records. These measures encourage organizations that handle electronic data to limit access to only a few authorized employees, diligently maintain logs for every access instance, seek consent before storing personal data, and strictly prevent unauthorized access by third parties without explicit permission or legal authorization.[xliii]

That said, there is still room for improvement. The current framework does not adequately distinguish between personal and sensitive personal data, resulting in a one-size-fits-all approach to data protection.

On a positive note, the Telecommunications Law and its executive regulations highlight the importance of safeguarding individual information as a key objective. Article 3 underscores the commitment to protecting both public and user interests while ensuring the confidentiality and security of telecommunications data. This focus provides a hopeful foundation for building a more secure digital environment where personal information is respected and protected. Together, these regulations pave the way for progress in data privacy, instilling confidence as we move toward a more considerate approach to electronic data protection.

Cemented protection for individuals' data privacy. First, under Article 56, legislators consider

This work is licensed under CC BY-SA 4.0.

service providers accountable for keeping customers' private information. The article provides clarifying information about how individuals can raise concerns or lodge complaints if service providers do not fulfill their responsibilities.

Additionally, Article 56 outlines the types of personal information that providers can share. It states that a service provider may only disclose the user's name, address, and listed telephone number with the user's written consent or, if required by law, for legitimate public authority.

This legislation protects users by prohibiting disclosing personal information beyond what's outlined, ensuring that privacy is prioritized. However, it's important to note that service providers can share a user's text that discusses the Law of Practicing Healthcare Professions (LPHP) in Saudi Arabia, which aims to protect an individual's health information. It emphasizes the importance of maintaining confidentiality by health practitioners, stating that they can only disclose information in specific cases, such as reporting criminal acts, communicable diseases, or preventing crimes. This framework seeks to balance user privacy with necessary communication in the digital landscape, helping individuals understand and safeguard their personal information.

The practitioner rebuts accusations about his competence or practicing his profession made by the patient or his family. B- If the patient agreed in writing to disclose the secret or if disclosure to the patient's family is helpful for his treatment. C- If so ordered by a judicial authority".[xliv]

Violators of confidentiality obligations may face a fine of up to 20,000 SR and additional disciplinary punishments such as the loss of a professional license. The severity or frequency of the offense can result in more significant sanctions.[xlv] However, according to Al Mebrad, although health information is essential and sensitive, the law in Saudi Arabia was still unclear as it was addressed using broad rules and principles.[xlvi]

Civil Affairs Law (1986)

The Civil Affairs Law provides extreme protection for individuals' records, and Article 11 embodies a commitment to safeguarding our records, emphasizing that "the records shall not be, in any case, transferred from the Civil Affairs Offices." This principle ensures that if a

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

judicial authority seeks to review specific records, it must be done with utmost respect and care, requiring a designated judge or investigator to visit the storage site directly.

Al Mebrad passionately argues that the law prioritizes the protection of individual records, placing significant importance on limiting access to these sensitive materials rather than merely categorizing information based on confidentiality levels. However, it is concerning that certain government agencies still unveil specific details from civil records. For instance, the execution courts publicly share specific rulings through local news articles, often including the sentenced person's full name. Including ID numbers in various practices highlights the complex relationship between transparency and protecting personal privacy. While such disclosures foster openness, they also expose vulnerabilities related to individual privacy rights. The lack of a comprehensive legal framework explicitly addressing these issues indicates an ongoing need for stronger privacy protections.

The E-Transaction Law and its accompanying executive regulations acknowledge the importance of safeguarding electronic data. However, they do not specifically enhance the legal protection of personal information. In contrast, telecommunications legislation offers more substantial safeguards, as it limits service providers' ability to collect, share, or use consumer data without explicit consent or legal justification.

Overall, it is clear that the landscape of personal data protection in Saudi Arabia remains ambiguous. This ambiguity allows for potential invasions of privacy without appropriate consequences; the introduction of a comprehensive legal framework for personal data protection in the region highlights a positive move towards safeguarding individual privacy. On September 24, 2021, Saudi Arabia took a significant step forward by enacting its first-ever comprehensive Personal Data Protection Law (PDPL), set to take effect on March 23, 2022. Excitingly, organizations will have a full year to ensure their operations align with this critical legislation!

For the first two years, the Saudi Data & Artificial Intelligence Authority (SDAIA) will oversee the implementation of the PDPL. After this initial phase, the National Data Management

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

Office (NDMO) will take on the supervisory role, ensuring continuous support and guidance for compliance.[xlvii]

The scope of the PDPL is both broad and empowering. It aims to protect "personal data," encompassing all forms of information that can identify a person—whether directly or indirectly—like names and personal identifiers. This law strengthens individual rights and fosters trust in the digital landscape. The future looks bright as we embrace these changes, ensuring a safer and more secure environment.[xlviii]

Sensitive personal data under this law are considered as: "every personal data that includes a reference to an individual's ethnic or tribal origin, or religious, intellectual or political belief or indicates his membership in nongovernmental associations or institutions, as well as criminal and security data, biometric data, genetic data, credit data, health data, location data, and data that indicates that both parents of an individual or one of them is unknown."

Additionally, the PDPL applies to the deceased's data if it may be used to identify the deceased or a family member. Notably, personal data processing for individual or family use is exempt from the scope of the PDPL if it is not shared or disclosed to others.

Furthermore, it is worth noting that the law applies to all personal data processing related to individuals in Saudi Arabia, regardless of the means used, including the processing of personal data of individuals residing in the Kingdom by any party outside the Kingdom's territorial jurisdiction.[xlix]

Definitions And Interpretations

Article 1 of the PDPL is dedicated to clarifying the terminology used in the law to make it more precise and accurate. Particular of those terminologies will be stated below as follows:

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

The authorized Legal Department: The authority will be determined by a decision made by the Cabinet.

Processing: This refers to any activity performed on personal data, whether through manual or automated means. It encompasses various methods such as collection, recording, archiving, indexing, formatting, storing, modifying, updating, merging, retrieving, utilizing, transferring, publishing, sharing, interconnecting, blocking, erasing, and destroying data.

Collection: The responsible entity gathers personal data according to the law. This data can be directly from the individual, their representative, legal guardian, or another authorized party.

Destruction: This involves actions that effectively remove personal data, ensuring it cannot be accessed or retrieved again.

Disclosure: This allows any individual other than the responsible entity to obtain, use, or access personal data through various means for any purpose.[1]

Transfer: This involves transferring personal data from one location to another for processing.

Publishing: This means sharing or making available personal data through written, audio, or visual publication formats.

Genetic Data: This term refers to any personal data associated with an individual's genetic or acquired characteristics uniquely identifying their physiological or health attributes. It is derived from analyzing a biological sample, such as nucleic acids.

Health Data: This encompasses all personal data related to an individual's health status, including physical, mental, and psychological aspects and data regarding health services.

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

Credit Data: This includes personal data relevant to an individual's request for or acquisition of financing, whether for personal or family purposes. It also pertains to data regarding their ability to obtain credit, repayment capability, and credit history.

Data Subject: An individual to whom personal data pertains, along with their representative or legal guardian.

Public Entity: Refers to any ministry, department, public institution, public authority, or any independent public entity within the Kingdom and its affiliated entities.

Controlling Entity: This could be a public entity, a private individual, or a legal entity that determines the purpose and means of processing personal data, whether performed directly or through a processing entity.

Processing Entity: An individual or legal entity, whether public or private, that processes personal data on behalf of the controlling entity.

Data Protection Principles: While the PDPL does not explicitly categorize its provisions into principles like the GDPR, it generally adopts similar principles across various articles.

1. **Lawfulness, Fairness, and Transparency:** The law requires that the controller's purpose for collecting personal data be lawful and compliant with existing legal provisions. Controllers are also required to implement a privacy policy that outlines the purpose of data collection, the types of data collected, collection methods, processing, destruction methods, data subject rights, and how these rights can be exercised.

2. **Purpose Limitation:** Personal data must be collected directly from the data subject and directly related to the purposes of processing as defined by the controller.

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

3. **Data Minimization:** Data collection should only encompass what is necessary for processing. Article 11 (3) of the PDPL mandates that collected personal data must specifically relate to the controller's purposes and be limited to what is essential.

4. **Accuracy:** Article 14 of the PDPL requires controllers to ensure that personal data remains up-to-date, accurate, complete, and relevant to its intended purpose.

5. **Storage Limitation:** Data retention is constrained to periods during which the data is deemed necessary. According to Article 11 (4), if data is no longer required for its original purpose, the controller must cease collection and promptly destroy the data previously gathered.

6. **Integrity and Confidentiality:** The PDPL mandates that controllers implement appropriate organizational, administrative, and technical measures for data protection, including during data transfers, as detailed in regulatory provisions.

Accountability: Controllers must select processing parties that provide necessary guarantees for legal compliance. They are obliged to monitor these entities' adherence to protection protocols regularly.

Data Subject Rights: The PDPL grants data subjects the following rights: the right to be informed, the right to access their data, the right to rectify any incorrect data, the right to request data erasure, the right to consent regarding data processing, the right to withdraw consent at any time, and the right to file complaints with authorized legal bodies.[li]

The Shariah Aspect of Data Protection

The sanctity of the deceased has been well considered in Shari'a. Prophet Mohammad (صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ) has been reported to have said: *"Breaking a dead man's bone is like breaking it when he is alive."*.[lii] Imam Ibn Hajar explained the meaning of this Hadith; he said that it can

This work is licensed under CC BY-SA 4.0.

be learned from this Hadith that the sanctity of the believer after his death remains as it was during his life.[liii]

The PDPL Imposes strict rules on transferring personal data outside Saudi Arabia. Controllers can only transfer data if they meet specified requirements, such as being part of an agreement that benefits the Kingdom or complying with executive regulations. Additionally, procedures must be followed to ensure that data transfers do not threaten national security or Saudi interests, and approval from the authorized legal department is required.

The law emphasizes the importance of prompt notification of breaches. Controllers must swiftly inform the authorized legal team when a data breach occurs. This quick action can significantly minimize potential damage, as the legal experts are ready to act decisively to secure any leaked information. Together, we can protect our data effectively!

The legal framework is notably stringent regarding penalties for non-compliance, which enhances protection for individuals. This rigorous approach will likely deter potential offenders from illegally processing sensitive data or transferring unauthorized data across borders. The Personal Data Protection Law (PDPL) further distinguishes between various offenses by imposing specific penalties, reinforcing its commitment to safeguarding personal information.

While it is natural for new laws to have some initial challenges, we can view these as opportunities for growth. The PDPL draws heavily from the GDPR, which sets a high standard for data protection. However, there are a few areas where further clarity could enhance individual protection. For instance, the PDPL does not specify the requirements for obtaining consent, an essential aspect of data processing. In contrast, the GDPR emphasizes that consent must be clear, informed, and explicit, ensuring robust protection for individuals. By addressing these gaps, we can work toward a framework that fully safeguards people's data rights while embracing the positive changes the PDPL brings. Together, we can advance and support a more robust data protection landscape.[liv]

This work is licensed under CC BY-SA 4.0.

Moreover, under the GDPR, "leverage" in the context of personal data processing refers to pseudonymization. This approach enables the processing of personal data without directly linking it to any specific individual. Such a technique offers significant advantages, providing enhanced protection for individuals as their identities remain concealed during data processing. In contrast, the PDPL does not incorporate this mechanism.[lv]

Unfortunately, the previous data protection measures were insufficient, prompting the Saudi legislature to introduce a new, comprehensive law. While the Personal Data Protection Law (PDPL) has room for improvement, it represents a significant step forward in safeguarding individuals' rights. With its enactment, all data processors will be held accountable, providing individuals with greater confidence in their data protection. Exciting times are ahead for enhanced privacy.[lvi]

Conclusion

Data protection is a key component in contemporary times, and post-personal data protection acts have been passed in different jurisdictions. Name, address, and identity number encompass the subsequent realms of personal data. Sensitive data must be protected from exposure to danger, as the general masses are still in oblivion, and unauthorized parties could misuse them to achieve their goals. However, considering the case of Saudi Arabia, the law enacted the PDPL in the last quarter of 2021.

The absence of a robust data protection law does not imply that individuals' data is inherently vulnerable. However, the newly proposed legislation is set to enhance data privacy measures by adopting key provisions from the GDPR, widely recognized as the benchmark for data protection law. Notably, this new legislation extends its applicability to the data of deceased individuals, marking a significant advancement. Additionally, the Personal Data Protection Law (PDPL) demonstrates a progressive approach to cross-border data transfer, underscoring its commitment to safeguarding individual rights. Despite these strengths, the law needs refinement, notably regarding consent mechanisms, which require greater transparency and explicit guidance for data subjects on providing consent and the circumstances under which it may be rendered void. Furthermore, the PDPL does not currently accommodate data

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

processing techniques involving pseudonymization, suggesting a need for further enhancements.

An in-depth exploration of the Kingdom of Saudi Arabia's (KSA) legal landscape reveals strengths and weaknesses that could impact the legal transplantation process, especially concerning its adaptation within the KSA framework. A fundamental hurdle in this substantive legislation analysis is the complex interplay between substantive and procedural laws within the KSA legal system. This paradox presents new challenges for legal practitioners in Saudi Arabia as they strive to effectively implement the five substantive enactments relevant to Personal Data Breach scenarios. Our research has pinpointed potential areas for enhancing KSA's legal infrastructure, particularly concerning administrative sanctions and specific procedural laws associated with Personal Data Breaches, Cybercrime, and Cyber Threats. Significant reforms have been initiated within the KSA legal framework, notably through full enforcement measures rolled out in 2022 and 2023, to establish comprehensive protocols that align institutional mechanisms with modern legislative requirements.

The Benchmarking analysis that compares the KSA PDPA with the EUGDPR indicates that the KSA has successfully integrated a comprehensive set of Personal Data Protection protocols encompassing prevention, mitigation, detection, and recovery phases. This is evident through its structured CIA (Confidentiality, Integrity, Availability) framework implementation, robust notification law, internal dispute resolution mechanisms, and diverse sanction categories. The foundational principles remain consistent despite some discrepancies between KSA regulations and EUGDPR guidelines. This similarity suggests that KSA's legal framework aligns with global information privacy standards as exemplified by the EUGDPR, positioning the region for future initiatives focused on "Regional Cooperation" in Data Protection.

Furthermore, echoing the observations of Xichen Zhang et al., "Technological advancement" constitutes a significant "Uncontrollable Factor" that perpetuates "Personal Data Breaches" within the realm of Cybercrime. The emergence of Artificial Intelligence (AI) has notably intensified the ramifications of data breaches, complicating the nature and extent of damages to affected individuals. The liability for malicious activities following such incidents necessitates further scholarly examination to formulate effective management and mitigation

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

strategies. Additionally, the proliferation of AI-derived technologies has led to adverse applications in Saudi Arabia, such as Identity Theft facilitated by Deepfake technology. The focus on Advanced Persistent Threats (APT) reflects the urgency with which KSA legal practitioners must approach these evolving challenges. As such, Saudi Arabia must maintain vigilance and develop comprehensive frameworks for addressing the implications of AI advancements in data protection.

In conclusion, this article provides a detailed comparative analysis of the GDPR and KSA Data Protection laws. While this comparison offers valuable insights, it highlights the necessity for a more extensive evaluation of global data protection frameworks to ensure a thorough understanding of international best practices in this domain.

Bibliography

Articles

Alshamisi, Mohammad Khamis, Normalini Md Kassim, and Yashar Salamzadeh. "FACTORS INFLUENCING INTENT TO USE AN EDUCATIONAL MANAGEMENT INFORMATION SYSTEM (EMIS): INSIGHTS FROM PRIVATE UNIVERSITIES OF THE UNITED ARAB EMIRATES." Community Practitioner 20, no. 8 (2023): 115-133.

AlMarzooqi, Mezna A. "Physical activity and attitudes toward social media use of active individuals during the COVID-19 pandemic in Saudi Arabia: cross-sectional survey." Frontiers in Psychology 12 (2021): 707921.

Alshaleel, Mohammed Khair. "The Extraterritoriality of the gdpr and Its Effect on gcc Businesses." Global Journal of Comparative Law 13, no. 2 (2024): 201-226.

Alhazmi, Ahmed, and Anas Daghistani. "Privacy practices of popular websites in Saudi Arabia." Journal of Umm Al-Qura University for Engineering and Architecture 16, no. 1 (2025): 19-29.

Abokhodair, Norah, and Sarah Vieweg. "Privacy & social media in the context of the Arab Gulf." In Proceedings of the 2016 ACM conference on designing interactive systems, pp. 672-683. 2016.

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

Abokhodair, Norah. "Transnational Saudi Arabian youth and Facebook: enacting privacy and identity." PhD diss., 2017.

Alsajjan, Sultan Saud. "The Proposition of A Public Governance Framework for The Real Estate Sector in Saudi Arabia." PhD diss., SP Jain School of Global Management (India), 2022.

Alotaibi, Hajed A. "The challenges of execution of Islamic criminal law in developing Muslim Countries: An analysis based on Islamic principles and existing legal system." Cogent Social Sciences 7, no. 1 (2021): 1925413.

Aissani, Rahima. "Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait." J. Legal Ethical & Regul. Isses 25 (2022): 1.

Ahmed, Syed Zubair. "An Evaluation of the Anti-Fraud Regime in Saudi Arabia from the Islamic Shariah Perspective." Universal Journal of Business and Management 1, no. 2 (2021): 94-120.

Almebrad, A. (2018). The sufficiency of information privacy protection in Saudi Arabia [Doctoral dissertation, Indiana University Maurer School of Law]. Maurer School of Law Digital Repository. https://www.repository .law.indiana.edu/cgi/viewcontent.cgi?article=1055&context=etd

Rosadi, Aden. "Islamic Jurisdiction System In Saudi Arabic." Al-Ahwal Al-Syakhsiyyah: Jurnal Hukum Keluarga dan Peradilan Islam 2, no. 1 (2021): 1-14.

Alzahrani, Reema Bakheet. "An overview of AI data protection in the context of Saudi Arabia." International Journal for Scientific Research 3, no. 3 (2024): 199-218.

Alyousof, Shahd Hosam. "The Impact of the Medical–Legal Partnership (MLP) Model on Public Health Students Regarding Screening of Social Determinants of Health: Qualitative Study." Master's thesis, Alfaisal University (Saudi Arabia), 2023.

This work is licensed under CC BY-SA 4.0.

Aloufi, Abdulrahman. "THE NEED TO ENHANCE ONLINE CONSUMER PROTECTION UNDER EXISTING SAUDI ARABAIN E-COMMERCE LAWS." PhD diss., Curtin University, 2023.

Al-Qahtani, Kholod Saaed, and MM Hafizur Rahman. "Data Governance and Digital Transformation in Saudi Arabia." In Proceedings of International Conference on Information and Communication Technology for Development: ICICTD 2022, pp. 95-106. Singapore: Springer Nature Singapore, 2023.

Alkhamsi, Norah Nasser, and Sultan Saud Alqahtani. "Compliance Framework for Personal Data Protection Law Standards." International Journal of Advanced Computer Science & Applications 15, no. 7 (2024).

Al-Marani, Abdul-Jabbar Hadi Abdullah, and Isyaku Hassan. "AN INVESTIGATION INTO THE MEANING AND USAGE OF "PERFECT HADITH" TERMINOLOGY FROM IBN HAJAR'S VIEWPOINT." Synesis (ISSN 1984-6754) 14, no. 1 (2022): 280-290.

Alhababi, Hamad Hamed. "Cross-Border Data Transfer between the gcc Data Protection Laws and the gdpr." Global Journal of Comparative Law 13, no. 2 (2024): 178-200.

Al-Khalifa, Hend, Malak Mashaabi, Ghadi Al-Yahya, and Raghad Alnashwan. "The Saudi privacy policy dataset." arXiv preprint arXiv:2304.02757 (2023).

Bentzen, Heidi Beate. "Context as key: the protection of personal integrity by means of the purpose limitation principle." In Research Handbook on EU Data Protection Law, pp. 381-404. Edward Elgar Publishing, 2022.

Bouderhem, Rabaï. "A review of Saudi e-commerce regulation under the scope of the GDPR." Arab Law Quarterly 1, no. aop (2024): 1-19.

Czerniawski, Michal, and Dan Svantesson. "Challenges to the Extraterritorial Enforcement of Data Privacy Law–EU Case Study." (2024).

This work is licensed under CC BY-SA 4.0.

Dove, Edward S., and Jiahong Chen. "What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9 (2)(e)." International Data Privacy Law 11, no. 2 (2021): 107-124.

Elfakharani, Ashraf. "Evaluation and comparison of the electronic contract in the context of legislations in Egypt and Saudi Arabia: An explanatory study." Law and Humanities Quarterly Reviews 1, no. 2 (2022).

Fontanelli, Filippo. "The European Union's Charter of Fundamental Rights Two Years Later." *Perspectives on Federalism* 3, no. 3 (2011).

Henseler, Simon, and Aurelia Tamò-Larrieux. "Reaching beyond its territory- An analysis of the extraterritorial scope of European data protection law." In Research Handbook on EU Data Protection Law, pp. 290-313. Edward Elgar Publishing, 2022.

Hustinx, Peter. "Data protection and international organizations: a dialogue between EU law and international law." International data privacy law 11, no. 2 (2021): 77-80.

Janeček, Václav, and Cristiana Teixeira Santos. "The autonomous concept of "damage" according to the GDPR and its unfortunate implications: Österreichische Post." Common Market Law Review 61, no. 2 (2024).

Kamminga, Menno. "Extraterritoriality." In The Max Planck Encyclopaedia of Public International Law. Oxford University Press, 2020.

Kanojia, Siddharth. "Ensuring privacy of personal data: a panoramic view of legal developments in personal data protection law in Saudi Arabia." J. Int'l L. Islamic L. 19 (2023): 270.

Kellerbauer, Manuel, Marcus Klamert, and Jonathan Tomkin. The EU Treaties and Charter of Fundamental Rights: a Commentary. Oxford University Press, 2024.

Knetsch, Jonas. "The compensation of non-pecuniary loss in GDPR infringement cases." Journal of European Tort Law 13, no. 2 (2022): 132-153.

Kuner, Christopher. "Data and extraterritoriality." In Research Handbook on Extraterritoriality in International Law, pp. 356-371. Edward Elgar Publishing, 2023.

This work is licensed under CC BY-SA 4.0.

Marengo, Federico. "The challenges of the General Data Protection Regulation to protect data subjects against the adverse effects of artificial intelligence." (2023).

Mulders, Stephan. "The relationship between the principle of effectiveness under Art. 47 CFR and the concept of damages under Art. 82 GDPR." International Data Privacy Law 13, no. 3 (2023): 169-181.

Nuseirat, Wael Mohammed. "Legal Protection of Personal Data Privacy in the Kingdom of Saudi Arabia." Manchester Journal of International Economic Law 1 (2024).

Oladoyinbo, Tunboson Oyewale, Samuel Oladiipo Olabanji, Oluwaseun Oladeji Olaniyi, Olubukola Omolara Adebiyi, Olalekan J. Okunleye, and Adegbenga Ismaila Alao. "Exploring the challenges of artificial intelligence in data integrity and its influence on social dynamics." Asian Journal of Advanced Research and Reports 18, no. 2 (2024): 1-23.

Peers, Steve, Tamara Hervey, Jeff Kenner, and Angela Ward, eds. The EU Charter of fundamental rights: a commentary. Bloomsbury Publishing, 2021.

Pormeister, Kärt. "Genetic data and the research exemption: is the GDPR going too far?." International Data Privacy Law 7, no. 2 (2017): 137-146.

Sarabdeen, Jawahitha, and Mohamed Mazahir Mohamed Ishak. "A comparative analysis: health data protection laws in Malaysia, Saudi Arabia and EU General Data Protection Regulation (GDPR)." International Journal of Law and Management 67, no. 1 (2024): 99-119.

Saqf Al Hait, Adel. "Cyber hacking: building a harmonised criminal legal framework for addressing cyber hacking in the Arab convention on combating information technology offences: a comparative study between Jordanian & Saudi cyber laws." PhD diss., Anglia Ruskin Research Online (ARRO), 2023.

Schellinger, Benjamin, Fabiane Völter, Nils Urbach, and Johannes Sedlmeir. "Yes, I do: Marrying blockchain applications with GDPR." e-government 19 (2022): 22.

Sunan Abi Dawud 3207, Book 21, Hadith 119.https://sunnah.com/abudawud/21/119

This work is licensed under CC BY-SA 4.0.

Torre, Damiano, Mauricio Alferez, Ghanem Soltana, Mehrdad Sabetzadeh, and Lionel Briand. "Modeling data protection and privacy: application and experience with GDPR." Software and Systems Modeling 20 (2021): 2071-2087.

Van den Bulck, Hilde, Steven Dewaele, and Karen Donders. "Signal integrity in EU Member States: Much ado about nothing?." In European Audiovisual policy in transition, pp. 221-238. Routledge, 2023.

Vardanyan, Lusine, Václav Stehlík, and Hovsep Kocharyan. "Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity." TalTech Journal of European Studies 12, no. 1 (2022): 159-185.

Voigt, Paul, and Axel von dem Bussche. "Scope of application of the GDPR." In The EU General Data Protection Regulation (GDPR) A Practical Guide, pp. 9-36. Cham: Springer Nature Switzerland, 2024.

Wang, Lipeng, Zhi Guan, Zhong Chen, and Mingsheng Hu. "Enabling integrity and compliance auditing in blockchain-based gdpr-compliant data management." IEEE Internet of Things Journal 10, no. 23 (2023): 20955-20968.

Zac, Amit, Pablo Wey, Stefan Bechtold, David Rodriguez, and Jose M. Del Alamo. "The Court Speaks, But Who Listens? Automated Compliance Review of the GDPR." Center for Law & Economics Working Paper Series 1 (2024).

Books

- Abu Dawood Suleiman bin Al-Ash`ath Al-Sijistani, Sunan Abi Dawud, almaktabat aleasriat , sayda - Beirut.
- Ahmed bin Ali bin Hajar Al-Asqalani, Fath Al-Bari sharh Sahih Al-Bukhari, dar almaerifat - Beirut, 1379.
- Paul Voigt and Taylor Wessing, THE EU General Data Protection Regulation (GDPR): A practice Guideline, SPRINGER International Publishing,2017, Berlin, Germany. Tom, Jake, Eduard Sing, and Raimundas.

This work is licensed under CC BY-SA 4.0.

- Voss, W. Gregory, Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later (March 1, 2014).

Journals

- Azzi, Adele. "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation." *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 9 (2018): 126.
- Regulation. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, *9*, 126
- Pelteret, Marc, and Jacques Ophoff. "Organizational information privacy strategy and the impact of the PoPI act." In *Information Security for South Africa (ISSA), 2017*, pp. 56-65. IEEE, 2017.Matulevičius. "Conceptual Representation of the GDPR: Model and Application Directions." In *International Conference on Business Informatics Research*, pp. 18-28. Springer, Cham, 2018
- Kurtz, Christian, and Martin Semmann. "Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors." (2018).
- Bennett, Colin J. "The European General Data Protection Regulation: An instrument for the globalization of privacy standards?" *Information Polity* 23, no. 2 (2018): 239-246.
- Teen, Omer, and Christopher Wolf. "Overextended: jurisdiction and applicable law under the EU general data protection regulation." In *Future of Privacy Forum White Article*. 2013.
- Journal of Internet Law (March 2014 -- Vol. 17, No. 9) -- Aspen Publishers Inc. -- Wolters Kluwer Law & Business.
- Voss, W. "Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later." (2014).
- ***Regulations***
- European Union Data Protection Directive (Directive 95/46/EC) of the European Parliament and the Council, 1995, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046
- European Commission on the General Data Protection Regulation (GDPR), Regulation EU 2016/679, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

This work is licensed under CC BY-SA 4.0.

- ***Websites***
- Elisa Cazoola, A brief history of GDPR, https://blog.claimable.com/a-brief-history-of-the-gdpr/, retrieved on 18th December 2018
- Kevin Marshall, General data protection: Data accuracy in practice, https://www.datenschutz-praxis.de/fachartikel/general-data-protection-regulation-data-accuracy-in-practice/, retrieved on 20th December 201
- https://www.lewik.org/term/13596/integrity-and-confidentiality-principle-gdpr/Lwik.A.R.O, last modified, 20 December 2018

Statutes

- The Basic Law of Governance 1992.
- The Law of Criminal Procedures 2013.
- The Anti-Cyber Crime Law 2007.
- E-transactions Law 2007.
- The Executive Regulation of the E-Transactions Law 2008.
- Telecommunications Law 2001.
- Executive Regulation for Telecommunications Law 2002.
- Law of Practicing Healthcare Professions 2005.
- Civil Affairs Law 1986,
- The Personal Data Protection Law (**PDPL**) 2021.
- General Data Protection Law (GDPR) 2016.

Dissertations

- Msfer Al-Qahtani, *Hmayat Alhayat Alkhasat lil'iinsan Watatyabaqatiha Alqadayiya (Alasrar-Almraslat-altqnyat Almeasr) Dirasat Mqarn* [Protecting the Privacy of Humans and its applications courts: (Secrets, Communication, New Technologies): A Comparative Article.] 68 (2014) (Ph.D. dissertation, Imam Mohamad Bin Saud University).
- Almebrad, A. " The Sufficiency of Information Privacy Protection in Saudi Arabia." (a Ph.D. dissertation, Indiana University, 2018).
- Elgujja, A. A. "*Adequacy of the legal safeguards of the patients' confidentiality right under the Saudi Arabian laws*" (Doctoral dissertation, University of Salford 2020).

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

Electronic sources

- Akhbaar24.Com, 'Imprisonment, Lashing, and Fine for a Woman in Her Thirties for Defaming a Citizen on the "WhatsApp," '(Mar. 16, 2015) (in Arabic) available at https://akhbaar24.argaam.com/article/detail/207989/
- *Mahkamat Altanfidh Bialriyad Tamahal Saad Alhariri 5 'ayam [Court of Execution in Riyadh Gave Saad Hariri Five Days to Implement a Judicial Decision], JAZAN NEWS, DEC. 15, 2016, at* http://www.jazannews.org/news.php?action=show&id=45333.
- https://cutt.ly/YIZz6T4

Endnotes

[i] Kamminga, Menno. "Extraterritoriality." In *The Max Planck Encyclopaedia of Public International Law*. Oxford University Press, 2020.

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

[ii] Hustinx, Peter. "Data protection and international organizations: a dialogue between EU law and international law." *International data privacy law* 11, no. 2 (2021): 77-80.
[iii] Nuseirat, Wael Mohammed. "Legal Protection of Personal Data Privacy in the Kingdom of Saudi Arabia." *Manchester Journal of International Economic Law* 1 (2024).
[iv] (European Parliament, the Council of the European Union, 2016, Article 4).
[v] Alshamisi, Mohammad Khamis, Normalini Md Kassim, and Yashar Salamzadeh. "FACTORS INFLUENCING INTENT TO USE AN EDUCATIONAL MANAGEMENT INFORMATION SYSTEM (EMIS): INSIGHTS FROM PRIVATE UNIVERSITIES OF THE UNITED ARAB EMIRATES." *Community Practitioner* 20, no. 8 (2023): 115-133.
[vi] AlMarzooqi, Mezna A. "Physical activity and attitudes toward social media use of active individuals during the COVID-19 pandemic in Saudi Arabia: cross-sectional survey." *Frontiers in psychology* 12 (2021): 707921.
[vii] Wang, Lipeng, Zhi Guan, Zhong Chen, and Mingsheng Hu. "Enabling integrity and compliance auditing in blockchain-based gdpr-compliant data management." *IEEE Internet of Things Journal* 10, no. 23 (2023): 20955-20968.
[viii] Vardanyan, Lusine, Václav Stehlík, and Hovsep Kocharyan. "Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity." *TalTech Journal of European Studies* 12, no. 1 (2022): 159-185.
[ix] Kellerbauer, Manuel, Marcus Klamert, and Jonathan Tomkin. *The EU Treaties and Charter of Fundamental Rights: a Commentary*. Oxford University Press, 2024.
[x] Oladoyinbo, Tunboson Oyewale, Samuel Oladiipo Olabanji, Oluwaseun Oladeji Olaniyi, Olubukola Omolara Adebiyi, Olalekan J. Okunleye, and Adegbenga Ismaila Alao. "Exploring the challenges of artificial intelligence in data integrity and its influence on social dynamics." *Asian Journal of Advanced Research and Reports* 18, no. 2 (2024): 1-23.
[xi] Schellinger, Benjamin, Fabiane Völter, Nils Urbach, and Johannes Sedlmeir. "Yes, I do: Marrying blockchain applications with GDPR." *e-government* 19 (2022): 22.
[xii] Van den Bulck, Hilde, Steven Dewaele, and Karen Donders. "Signal integrity in EU Member States: Much ado about nothing?." In *European Audiovisual policy in transition*, pp. 221-238. Routledge, 2023.
[xiii] Fontanelli, Filippo. "The European Union's Charter of Fundamental Rights Two Years Later." *Perspectives on Federalism* 3, no. 3 (2011).
[xiv] Peers, Steve, Tamara Hervey, Jeff Kenner, and Angela Ward, eds. *The EU Charter of fundamental rights: a commentary*. Bloomsbury Publishing, 2021.
[xv] Bentzen, Heidi Beate. "Context as key: the protection of personal integrity by means of the purpose limitation principle." In *Research Handbook on EU Data Protection Law*, pp. 381-404. Edward Elgar Publishing, 2022.
[xvi] Kellerbauer, Manuel, Marcus Klamert, and Jonathan Tomkin. *The EU Treaties and Charter of Fundamental Rights: a Commentary*. Oxford University Press, 2024.
[xvii] Kuner, Christopher. "Data and extraterritoriality." In *Research Handbook on Extraterritoriality in International Law*, pp. 356-371. Edward Elgar Publishing, 2023.
[xviii] Henseler, Simon, and Aurelia Tamò-Larrieux. "Reaching beyond its territory- An analysis of the extraterritorial scope of European data protection law." In *Research Handbook on EU Data Protection Law*, pp. 290-313. Edward Elgar Publishing, 2022.
[xix] Czerniawski, Michal, and Dan Svantesson. "Challenges to the Extraterritorial Enforcement of Data Privacy Law–EU Case Study." (2024).
[xx] Alshaleel, Mohammed Khair. "The Extraterritoriality of the gdpr and Its Effect on gcc Businesses." *Global Journal of Comparative Law* 13, no. 2 (2024): 201-226.
[xxi] Voigt, Paul, and Axel von dem Bussche. "Scope of application of the GDPR." In *The EU General Data Protection Regulation (GDPR) A Practical Guide*, pp. 9-36. Cham: Springer Nature Switzerland, 2024.
[xxii] Pormeister, Kärt. "Genetic data and the research exemption: is the GDPR going too far?." *International Data Privacy Law* 7, no. 2 (2017): 137-146.
[xxiii] Torre, Damiano, Mauricio Alferez, Ghanem Soltana, Mehrdad Sabetzadeh, and Lionel Briand. "Modeling data protection and privacy: application and experience with GDPR." *Software and Systems Modeling* 20 (2021): 2071-2087.
[xxiv] Dove, Edward S., and Jiahong Chen. "What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9 (2)(e)." *International Data Privacy Law* 11, no. 2 (2021): 107-124.
[xxv] Voigt, Paul, and Axel von dem Bussche. "Enforcement and fines under the GDPR." In *The EU General Data Protection Regulation (GDPR) A Practical Guide*, pp. 275-299. Cham: Springer Nature Switzerland, 2024.
[xxvi] Zac, Amit, Pablo Wey, Stefan Bechtold, David Rodriguez, and Jose M. Del Alamo. "The Court Speaks, But Who Listens? Automated Compliance Review of the GDPR." *Center for Law & Economics Working Paper Series* 1 (2024).
[xxvii] Mulders, Stephan. "The relationship between the principle of effectiveness under Art. 47 CFR and the concept of damages under Art. 82 GDPR." *International Data Privacy Law* 13, no. 3 (2023): 169-181.
[xxviii] Janeček, Václav, and Cristiana Teixeira Santos. "The autonomous concept of "damage" according to the GDPR and its unfortunate implications: Österreichische Post." *Common Market Law Review* 61, no. 2 (2024).

ISSN 2583 7060
Volume 4 Issue 1 [January - March 2025]
This work is licensed under CC BY-SA 4.0.

[xxix] Marengo, Federico. "The challenges of the General Data Protection Regulation to protect data subjects against the adverse effects of artificial intelligence." (2023).
[xxx] Knetsch, Jonas. "The compensation of non-pecuniary loss in GDPR infringement cases." *Journal of European Tort Law* 13, no. 2 (2022): 132-153.
[xxxi] Bouderhem, Rabaï. "A review of Saudi e-commerce regulation under the scope of the GDPR." *Arab Law Quarterly* 1, no. aop (2024): 1-19.
[xxxii] Sarabdeen, Jawahitha, and Mohamed Mazahir Mohamed Ishak. "A comparative analysis: health data protection laws in Malaysia, Saudi Arabia and EU General Data Protection Regulation (GDPR)." *International Journal of Law and Management* 67, no. 1 (2024): 99-119.
[xxxiii] Alhazmi, Ahmed, and Anas Daghistani. "Privacy practices of popular websites in Saudi Arabia." *Journal of Umm Al-Qura University for Engineering and Architecture* 16, no. 1 (2025): 19-29.
[xxxiv] Abokhodair, Norah, and Sarah Vieweg. "Privacy & social media in the context of the Arab Gulf." In *Proceedings of the 2016 ACM conference on designing interactive systems*, pp. 672-683. 2016.
[xxxv] Abokhodair, Norah. "Transnational Saudi Arabian youth and Facebook: enacting privacy and identity." PhD diss., 2017.
[xxxvi] Alsajjan, Sultan Saud. "The Proposition of A Public Governance Framework for The Real Estate Sector in Saudi Arabia." PhD diss., SP Jain School of Global Management (India), 2022.
[xxxvii] Alotaibi, Hajed A. "The challenges of execution of Islamic criminal law in developing Muslim Countries: An analysis based on Islamic principles and existing legal system." *Cogent Social Sciences* 7, no. 1 (2021): 1925413.
[xxxviii] Aissani, Rahima. "Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait." *J. Legal Ethical & Regul. Isses* 25 (2022): 1.
[xxxix] Ahmed, Syed Zubair. "An Evaluation of the Anti-Fraud Regime in Saudi Arabia from the Islamic Shariah Perspective." *Universal Journal of Business and Management* 1, no. 2 (2021): 94-120.
[xl] Almebrad, A. (2018). The sufficiency of information privacy protection in Saudi Arabia [Doctoral dissertation, Indiana University Maurer School of Law]. Maurer School of Law Digital Repository. https://www.repository .law.indiana.edu/cgi/viewcontent.cgi?article=1055&context=etd
[xli] Rosadi, Aden. "Islamic Jurisdiction System In Saudi Arabic." *Al-Ahwal Al-Syakhsiyyah: Jurnal Hukum Keluarga dan Peradilan Islam* 2, no. 1 (2021): 1-14.
[xlii] Alzahrani, Reema Bakheet. "An overview of AI data protection in the context of Saudi Arabia." *International Journal for Scientific Research* 3, no. 3 (2024): 199-218.
[xliii] Elfakharani, Ashraf. "Evaluation and comparison of the electronic contract in the context of legislations in Egypt and Saudi Arabia: An explanatory study." *Law and Humanities Quarterly Reviews* 1, no. 2 (2022).
[xliv] Alyousof, Shahd Hosam. "The Impact of the Medical–Legal Partnership (MLP) Model on Public Health Students Regarding Screening of Social Determinants of Health: Qualitative Study." Master's thesis, Alfaisal University (Saudi Arabia), 2023.
[xlv] Saqf Al Hait, Adel. "Cyber hacking: building a harmonised criminal legal framework for addressing cyber hacking in the Arab convention on combating information technology offences: a comparative study between Jordanian & Saudi cyber laws." PhD diss., Anglia Ruskin Research Online (ARRO), 2023.
[xlvi] Aloufi, Abdulrahman. "THE NEED TO ENHANCE ONLINE CONSUMER PROTECTION UNDER EXISTING SAUDI ARABAIN E-COMMERCE LAWS." PhD diss., Curtin University, 2023.
[xlvii] Al-Qahtani, Kholod Saaed, and MM Hafizur Rahman. "Data Governance and Digital Transformation in Saudi Arabia." In *Proceedings of International Conference on Information and Communication Technology for Development: ICICTD 2022*, pp. 95-106. Singapore: Springer Nature Singapore, 2023.
[xlviii] Kanojia, Siddharth. "Ensuring privacy of personal data: a panoramic view of legal developments in personal data protection law in Saudi Arabia." *J. Int'l L. Islamic L.* 19 (2023): 270.
[xlix] Nusairat, Wael Mohammed. "Legal Protection of Personal Data Privacy in the Kingdom of Saudi Arabia." *Manchester Journal of Transnational Islamic Law & Practice* 20, no. 1 (2024).
[l] Nusairat, Wael Mohammed. "Legal Protection of Personal Data Privacy in the Kingdom of Saudi Arabia." *Manchester Journal of Transnational Islamic Law & Practice* 20, no. 1 (2024).
[li] Alkhamsi, Norah Nasser, and Sultan Saud Alqahtani. "Compliance Framework for Personal Data Protection Law Standards." *International Journal of Advanced Computer Science & Applications* 15, no. 7 (2024).
[lii] Sunan Abi Dawud 3207, Book 21, Hadith 119.https://sunnah.com/abudawud/21/119
[liii] Al-Marani, Abdul-Jabbar Hadi Abdullah, and Isyaku Hassan. "AN INVESTIGATION INTO THE MEANING AND USAGE OF "PERFECT HADITH" TERMINOLOGY FROM IBN HAJAR'S VIEWPOINT." *Synesis (ISSN 1984-6754)* 14, no. 1 (2022): 280-290.
[liv] Alhababi, Hamad Hamed. "Cross-Border Data Transfer between the gcc Data Protection Laws and the gdpr." *Global Journal of Comparative Law* 13, no. 2 (2024): 178-200.

This work is licensed under CC BY-SA 4.0.

[lv] Sarabdeen, Jawahitha, and Mohamed Mazahir Mohamed Ishak. "A comparative analysis: health data protection laws in Malaysia, Saudi Arabia and EU General Data Protection Regulation (GDPR)." *International Journal of Law and Management* 67, no. 1 (2025): 99-119.
[lvi] Al-Khalifa, Hend, Malak Mashaabi, Ghadi Al-Yahya, and Raghad Alnashwan. "The Saudi privacy policy dataset." *arXiv preprint arXiv:2304.02757* (2023).

This work is licensed under CC BY-SA 4.0.