AJSP
المجلة العربية للنشر العلمي
الإصدار السادس – العدد ستة وخمسون
تاريخ الإصدار: 2 – حزيران – 2023م
www.ajsp.net
ISSN: 2663-5798

"E-COMMERCE CONSUMER DATA PROTECTION IN SAUDI ARABIA: History, Challenges, and Suggested Improvements"

Researcher:

Sarah Waleed Alfayez

Prince Sultan University, Saudi Arabia

الإصدار السادس – العدد ستة وخمسون
تاريخ الإصدار: 2 – حزيران – 2023م
www.ajsp.net
ISSN: 2663-5798

SUMMARY:

ABSTRACT:

Background

Consumer protection is a hotly contested topic in e-commerce because of the practical challenges that consumers encounter when transacting online as opposed to offline. Because of the trust-based nature of this remote interaction, consumers dealing with online sellers are always at risk of illegal processing and using of personal data. Many nations have laws that handle privacy, The Kingdom of Saudi Arabia is no exception to this global trend. Saudi Arabia has a history of laws with data protection provisions that dates back to the early 2000s. In 2007, the country issued the Electronic Transactions Law, which included provisions on the protection and security of electronic data. However, these provisions were limited and did not provide comprehensive data protection. The E-Commerce Law, which had measures for data protection and privacy, was passed by Saudi Arabia in 2019. Except with the consumer to whom the personal data pertains, the service provider is not permitted to use the e-consumer's personal data or electronic communications for prohibited or authorized purposes or to disclose them to a third party[1]. The Data Protection Law, which provides a thorough legal framework for the protection of personal data in Saudi Arabia, was passed in 2021. Regardless of the nationality of the person in question or the location of the data processing, the law is applicable to all personal data processed in Saudi Arabia. The law mandates the use of suitable security measures to prevent unauthorized access to, disclosure of, alteration of, or destruction of personal data, as well as the legitimate, fair, and transparent processing of personal data[2]. As a result, this paper will follow the legislative texts pertaining to the protection of data applicable to online purchases made in Saudi Arabia. This will include an examination of those texts' legal challenges, it will also suggest recommendations to overcoming such challenges.

Methods

The analysis of the applicable personal data protection laws and regulations applicable in E-commerce in Saudi Arabia is conducted with the normative method to examine issues and weaknesses and investigate the possibilities of improvement. The conclusions on the existing problems and possible solutions shall be based on the analytical method.

Results and Conclusions

Data protection is crucial to ensure that personal information is kept secure and not misused by unauthorized individuals or entities. Saudi Arabia has implemented regulations to protect consumer data and privacy in e-commerce, However, despite the efforts, there are still many possible challenges which face the legal environment of data protection. Those challenges include ambiguity in some texts and definitions, and restrictive cross-border data transfer requirements. It is recommended to improve clarity in some critical concepts and definitions set out in the relative laws and regulations, as well as improving cross-border transfer of data requirements..

Keywords: Data protection laws, E-commerce, Saudi Arabia.

1. Introduction:

Due to good financial balances and a strong readiness to invest in the ICT sector, the Kingdom of Saudi Arabia ("Saudi Arabia" or "the Kingdom") has seen a surge in Information and Communications Technology (ICT) and Electronic

[1] Article 2 of E-Commerce Law

[2] Article 2 of the PDPL

Commerce (e-commerce) over the last decade[3]. Saudi Arabia has made significant investments in its ICT infrastructure as part of its economic development strategy[4]. With comparatively good living standards, the country also uses the most cutting-edge high-tech products. In turn, Saudi Arabia's economic success and expansion have resulted in a predicted increase in computer-related criminal activities[5]. Saudi Arabia had the opportunity to implement comprehensive political and regulatory reforms in this field, including telecommunications reforms with cyber security and balancing economic and social data security needs with political and national security goals[6]. this research will discuss the history of data privacy related laws and/or provisions in Saudi Arabia and provide an overview of such laws and provisions, it will explain the challenges related to those laws (especially (specific provisions in the E-Commerce Law and the Personal Data Protection Law, it will provide an example of successful implementation of data privacy laws and regulations in Saudi Arabia, and it will finally provide recommendations to overcoming such challenges and gaps.

2. History:

Due to good financial balances and a strong readiness to invest in the ICT sector, Saudi Arabia has seen a surge in Information and Communications Technology (ICT) and Electronic Commerce (e-commerce) over the last decade[7]. With comparatively good living standards, the country also uses the most cutting-edge high-tech products, In turn, Saudi Arabia's economic success and expansion have resulted in a predicted increase in computer-related criminal activities[8]. Saudi Arabia had the opportunity to implement comprehensive regulatory reforms in this field[9], including the development of a number of laws and regulations protecting personal data. This section will discuss the history of data privacy related laws and provisions in Saudi Arabia.

2.1 The Basic Law of Governance

approved by the royal decree No. A/90, The Law makes no mention of data protection specifically. However Telegraphic, postal, telephone, and other means of communication must all be protected, With the exception of circumstances specified by law, they cannot be seized, delayed, read, or listened to.[10]

2.2 Credit Information Law

approved by the Royal Decree No M/37, intends to define the fundamental values and essential rules for the collecting, sharing, and safeguarding of consumer credit information.[11] The Credit Information Law stipulates several violations, the penalties of which can reach a fine of not more than (1,000,000 SAR) one million riyals, and it is doubled in the event of

[3] Abdullah, Ahmed (2020) "Consumers' Personal Data Protection in Saudi Arabia: A Comparative Analytical Study" [3] University of Kansas ProQuest Dissertations Publishing, 2020. Kansas, 27961274 P.18

Id.[4]

Id.[5]

Id.[6]

Id.[7]

Id.[8]

Id.[9]

Article 1407 The Basic Law of Governance No. A/90 dated 27/8/1412H.[10]

Article 2 of the Credit Information Law[11]

recurrence[12]

2.3 Anti-Cyber Crime Law

Approved by the Royal Decree No M/17, aims to safeguard information security, the rights of those who lawfully use computers and information networks, the public interest, morals, and the country's economy[13]. The law declares it unlawful to access another person's computer with the intent to delete, destroy, alter, or distribute that person's information, as well as to access another person's bank or credit information or to obstruct the transmission of data via an information network or computer[14].

2.4 The Deputy Ministry for Consumer Protection[15]

The Saudi Deputy Ministry of Consumer Protection is in charge of protecting consumers from fraud, deception, imitation, misleading advertising, and unfair practices, as well as having control over goods and services to ensure safety, raise consumer awareness, and boost the national economy by improving the quality of goods[16]. The Deputy is also tasked with the implementation of consumer-related regulations, which includes receiving consumer complaints, doing appropriate research and analysis, and cooperating with relevant authorities to handle such concerns and devise necessary remedies. The electronic stores control administration is one of the sub-departments.[17]

2.5 National Data Governance Interim Regulations

As the national data regulator in the Kingdom, the National Data Management Office (NDMO) published the framework for national data governance in 2020. It sets the rules and policies for data classification, data sharing, data privacy, freedom of information, open data, and other areas in advance of any required legislation. All organizations within the Kingdom that process personal data in whole or in part as well as all organizations outside the Kingdom that use any method to process personal data related to people residing in the Kingdom are subject to the Personal Data Protection in Chapter 5 of the Interim Regulations[18].

which states in Paragraph (1) of Article "Tenth" that NDMO is mandated to develop the policies, governance mechanisms, standards, and controls related to data and Artificial Intelligence and monitor compliance against them after issuance, NDMO has examined international norms and practices to develop these Interim Regulations centered on national data governance that aim to many objectives, including[19]:

---

[12] Article 13 of the Credit Information Law

[13] Article 2 of the Anti-Cyber Crime Law

[14] Article 4 and 5 of the Anti-Cyber Crime Law

[15] As per the Saudi Ministry of Commerce website https://mc.gov.sa/ar/About/Departments/cp/Pages/default.aspx (last visited April 2023)

[16] Abdullah, Ahmed (2020) "Consumers' Personal Data Protection in Saudi Arabia: A Comparative Analytical Study" University of Kansas ProQuest Dissertations Publishing, 2020, Kansas, 27961274

[17] Id.

[18] Article 5.1 of the National Data Management Office's Interim Regulations

[19] Article (3) of the National Data Governance Interim Regulations, *found at* https://sdaia.gov.sa/ndmo/Files/PoliciesEn.pdf (last visited April 2023)

1. Assist the Kingdom in pursuing its national plans and aspirations.

2. Create an environment where data sharing and cooperation are valued and encouraged to improve data, information, and knowledge assets.

3. Controlling how protected data and publicly available information are published, transferred, used, and reused.

4. Maintain the confidentiality of sensitive data and the privacy of individual data.

5. When dealing with personal data and open information maintained by governmental organizations, protect people's right to data privacy.

6. Specifically safeguard national sovereignty with regard to personal data.

2.6 E-Commerce Law

The E-Commerce Law, Royal Decree No. M/126, became effective in October 2019. When offering goods or services to customers based in KSA, e-commerce service providers, even those headquartered outside of KSA, are subject to the law.[20]

The protection of consumer data was outlined in three ways in Saudi Arabia's e-commerce law, namely as follows: Name, address, phone number, bank account information, and other personal information belonging to the customer must be protected first. Second, the service provider is not allowed to broadcast or use customer information and may only store it for specific purposes. Offer assistance. Third, the service provider is not permitted to save customer data until with permission if the consumer needs to form an electronic account owing to frequent usage of the electronic commercial website. [21]

2.7 The Personal Data Protection Law

The Personal Data Protection Law ("PDPL"), The Royal Decree No. (m/19), It applies to all data processing involving individuals in the Kingdom of Saudi Arabia by institutions residing in the Kingdom or outside the Kingdom, This includes processing personal information on Saudi citizens as well as information about the deceased.[22] The National Data Management Office ("NDMO") will be overseen by the Saudi Data & Artificial Intelligence Authority ("SDAIA") for the first two years, following which a transfer of supervision would be considered[23]. Both the Saudi Communications, Space, and Technology Commission ("CST") and the Saudi Central Bank will retain the authority to oversee data protection within their respective jurisdictions[24]. The PDPL provides for data subjects included in its provisions the following:

- The right to information, which includes the right to be informed of the legal or practical reasons considered for collecting his personal data and the purpose thereof, as well as the right to request that his data not be processed later in a manner inconsistent with the reason for collection or in circumstances other than those specified in The PDPL[25].
- The right to access their personal information possessed by the controlling authority, such as having access to it, acquiring a copy of it in an easily understood form that reflects the subject matter of the documents, and performing

[20] Article 2 of the E-Commerce Law

[21] Saudi E-Commerce Law

[22] Saudi Personal Data Protection Law, Article 2

[23] Article 2 of the Preamble of the Saudi Personal Data Protection Law

[24] Article 6 and 7 of the Preamble of the Saudi Personal Data Protection Law

[25] Saudi Personal Data Protection Law, Article 4 (1)

so with no material compensation - as determined by the regulations - without sacrificing what the credit information law requires in terms of monetary consideration, and without sacrificing what is outlined in The PDPL[26].

- The right to ask the controlling party to complete, alter, or update their personal information[27].
- The right to request that the governing authority remove any of his personal data that is no longer required, notwithstanding the constraints imposed by the PDPL[28].

3. Possible Challenges:

Saudi Arabia, as seen in the previous chapter, has taken big steps to improve its data protection legal environment. It was explained in Chapter three of this thesis the role of the government of Saudi Arabia in the protection of data in general and including e-commerce transactions, The country's data protection laws are designed to safeguard the privacy and security of personal information while ensuring that businesses comply with certain obligations when collecting, processing, and storing data. through the issuance of many regulations in various fields that prevent the use of private data in violating ways, However, despite the efforts, there are still many possible challenges which face the legal environment of data protection. This section will explore the possible challenges of data protection related laws and provisions in general, and on the E-Commerce industry in the Kingdom.

3.1 Ambiguity in critical wordings within the laws and regulations

While most data protection related laws and/or provisions provide definitions of most ambiguous words stipulated within that law or provision, there is still some ambiguity which lies with undefined words within that law or provision. What happens in the legal field is not just the legal determination of a term's meaning; rather, it is the coercive determination of the exclusive manner by which a term must be understood and used in a set of certain factual circumstances [29]. The fundamental tenets of a legal system, such as the rule of law and the concept of separation of powers, are directly related to and connected to definitions[30]. While the PDPL provides broad definitions of some data protection concepts, such as personal data and sensitive data; there still remains a lack of clarity on some key issues, such as the definition of consent. The PDPL does not define the word "consent" which was mentioned -with relation of the individual who is the subject of the law- six times throughout the PDPL. Laws and regulations' defining clauses serve basic objectives, by attempting to eliminate ambiguity by developing a lexicon that is not (or at least should not be) ambiguous, definitions help to minimize vagueness and uncertainty in statutes[31]. However, in the Saudi NDMO's ("National Data Management office") National Data Governance Interim Regulations, the Interim Regulations provide a definition of consent as A knowing, voluntary, explicit, and documented statement of consent by the data subject indicating their agreement to the processing of their personal information[32].

We encounter a similar conundrum in Article 24 (1) of the PDPL, which states that The Regulations define additional controls and procedures regarding the processing of credit data in a way that guarantees the preservation of its owners' privacy and

[26] Saudi Personal Data Protection Law, Article 4 (2)

[27] Saudi Personal Data Protection Law, Article 4 (3)

[28] Saudi Personal Data Protection Law, Article 4 (4)

[29] Yaniv Roznai (2014) 'A Bird is Known by its Feathers'—On the Importance and Complexities of Definitions in Legislation, The Theory and Practice of Legislation, 2:2, 145-167, DOI: 10.5235/2050-8840.2.2.145 P.147

[30] Id. P. 148

[31] A. Aarnio, *On Legal Reasoning* (1977) 75. On the distinction between ambiguity and vagueness see M. Azar, 'Transforming Ambiguity into Vagueness in Legal Interpretation' in A. Wagner et al. *(eds.), Interpretation,Law and the* Construction *of* Meaning (Springer, Dordrecht 2007) P. 121-137.

[32] Article 2 of the NDMO's National Data Governance Interim Regulations

protects their rights outlined in the system and the credit information system, provided that they include the following: 1- Take the required steps to ensure that the owner of the personal data has given their explicit consent before the data is collected, its purpose is changed, or it is disclosed or published in compliance with the Credit Information Law.[33] There lies a shadow on the meaning of "explicit consent", it is worth mentioning -though- that this text was recently amended in 07-03-2023 by the Royal Decree No.(M/148) dated 07-03-2023, before the amendment it was read as "written consent" rather than "explicit consent", it is worth mentioning as well that the draft Implementing Regulation of the PDPL define "explicit consent" as " A verbal or written consent that is express, specific, and issued free and absolute by the owner of the data indicating his acceptance of the processing of his personal data"[34], however, even if the said draft of the Implementing Regulation was approved, it still does not apply to the Law (PDPL) as the Implementing Regulation will be enacted by NDMO, while the PDPL was enacted by a Royal Degree, and thus, the definition of the "explicit consent" mentioned in the draft of the PDPL Implementing Regulation can not be strictly applied in the PDPL, but rather, it can be a used a mere guidance for judges and and arbitrators to draw on their opinions from for interpretation.

3.2 Restrictive Cross-Border Data Transfer Conditions

The development of international data-sharing regulations paralleled the expansion of the field of personal data protection, a well-defined component of which it is.[35] and while the saudi E-Commerce Law and Credit Information Law do not provide provisions regulating cross-border data transfer, the Article 96 PDPL is dedicated to cross-border transfer of data, when reading the article, it is noticed that Saudi Arabia allows transfer of personal data with certain conditions, one of the most important of which is conditioning an adequate level of personal data protection is available outside the Kingdom -to the country said data is meant to be transferred to- Not less than the level of protection established in the law and regulations, which provide protection of data for the Saudi Residents similar or better than the data protection regulations provided in the Kingdom, however the regulator has limited this provision with the condition of the results of an evaluation conducted by the competent authority in this regard in coordination with whomever it deems appropriate from the concerned authorities[36], this ultimately means that when a company (a controller), for instance, plans to transfer personal data of E-Commerce users outside the borders of the Kingdom, assuming it has fulfilled all conditions set out in Article 29 of the PDPL, such company is limited by the results of the evaluation of the competent authorities, which raises multiple unclear points, will such evaluation be provided as a guideline from the competent authority explaining the legality of data transfer to each country and each type of personal data or will it be a case-by-case evaluation? Looking at the draft of the implementing regulation of the PDPL, Article 28 (1) it states that The Kingdom's borders are where the Controlling Authority must retain and process personal data. It cannot be kept or processed outside the Kingdom unless the competent authority has first reviewed the implications and given written consent, after which the regulatory authority has individually coordinated with the competent authority in a case by case way[37], and unlike the European Union's General Data Protection Regulation's ("GDPR")

[33] Article 24 (1) of the Personal Data Protection Law

[34] The draft of which can be found on Istla'a Platform, which is a unified governmental electronic platform to seek the opinions of the public, government entities and the private sector regarding economic and development environment laws, regulations issued by government entities prior to its approval, draft of mentioned implementing regulation link https://istitlaa.ncc.gov.sa/ar/transportation/ndmo/pdpl/Documents/مشروع%20اللائحة%20التنفيذية%20لنظام%20حماية%20البيانات%20الشخصية.pdf (last visited May 2023)

[35] Phillips, M. International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Hum Genet* 137, 575–582 (2018) DOI: 10.1007/s00439-018-1919-7

[36] Article 29 of the Saudi Personal Data Protection Law

[37] Article 28 (1) of the Implementing Regulations of the PDPL, posted at Istla'a Platform at: https://istitlaa.ncc.gov.sa/ar/transportation/ndmo/pdpl/Documents/%D9%85%D8%B4%D8%B1%D9%88%D8%B9%20%D8%A7%D9%84%D9%84%D8%A7%D9%8A%D9%94%D8%AD%D8%A9%20%D8%A7%D9%84%D8%AA%D9%86%D9%81%D9%8A%D8%B0%D9%8A%D8%A9%20%D9%84%D9%86%D8%B8%D8%A7%D9%85%20%D8%AD%D9%85%D8%A7%D9%8A%D8%A9%20%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA%20%D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D8%A9.pdf

adequacy condition, or where if the controller or processor has put in place the essential security measures and there are available adequate legal remedies for data subjects with enforceable rights, personal data may be transferred to a third country or an international organization without an adequacy determination[38], A legally binding and enforceable agreement between public authorities or entities, standard data protection terms published by the European Commission, or binding company policies may all include such adequate measures[39] Such measures do not require a supervisory authority's approval[40]. However, in some circumstances, the supervisory authority's approval is required[41], in the case of Saudi Arabia where it is mandatory for controllers to obtain the competent authority's approval of personal data transfer in each case, and given the length of time it may take to obtain case-by-case approval of cross-border data transfer, this can be challenging and cause some business and company inconveniences, particularly given that numerous international businesses with branches in the Kingdom share a database, and businesses operate in a globalized economy.

4. Findings and Recommendations:

4.1 Findings: In summary of this paper, findings can be summarized in the following points:

1. The Kingdom of Saudi Arabia has made significant progress in terms of data protection since the introduction of the Personal Data Protection Law (PDPL) in 2019 and the NDMO's Interim Regulations in 2020, which brought the country in line with international standards on data protection. Historical examples of related laws or provisions include: E-Commerce Law, Credit Information Data Law.
2. Saudi Arabia has taken big steps to improve its data protection legal environment, however, there are still many challenges which face the legal environment of data protection in the Kingdom, those challenges include ambiguity in some wordings such as "consent", challenges also include provisions in relation with the requirements for cross-border data transfer, specifically the case-by-case approval requirement.

4.2 Recommendations:

In the hope of contributing to ongoing efforts to strengthen data protection measures in Saudi Arabia, the following points are recommendations suggested to the improvement of the personal data protection rules:

1. Improving clarity in some concepts and definitions set out in the relative laws and provisions, especially on the most important one in similar laws which are terms such as "consent", "implied consent", "explicit consent". A term may fall under the broad meaning even if the court decides one interpretation is preferable to the other, provided both readings are rational, clearly, there are less misunderstandings when ambiguity is defined narrowly.[42] The narrow definition only detects ambiguities when the best two interpretations are tied; by contrast, the wide definition detects ambiguities whenever the weaker interpretation is conceivable. Depending on how plausible an interpretation must be in order for it to be considered reasonable, there may be extra difficulties under the broad definition.[43]
2. improving of cross-border transfer of data requirements, although the draft of the implementing regulations of the PDPL in its Articles 29 and 30 mentions an "approved list" of countries, it is still unclear what it means, specially that article 28 states clearly that in any case of transferring of personal data outside the Kingdom has to be done

[38] Article 46 (1) of the GDPR

[39] Article 46 (2) of the GDPR

[40] Article 46 (1) of the GDPR

[41] Article 46 (3) of the GDPR

[42] Michael B. Rappaport "The Ambiguity Rule and Insurance Law: Why Insurance Contracts Should Not Be Construed against the Drafter" Heinonline 30 Ga. L. Rev. 171 (1995-1996)

[43] Id.

after obtaining necessary approvals for every case, it seems from reading the mentioned articles that transferring of personal data outside the Kingdom for countries not enlisted in the approved list that it requires doing studies for risk analysis to be given to the competent authority to be granted approval of data transfer, a similar mechanism as the GDPR's adequacy list could be considered in Saudi Arabia, for a similar mechanism to be between Saudi and other countries with which Saudi has the most commercial exchange if their related regulations give no less than the standards of protection as the regulations in Saudi, rather than a case-by-case approval.

5. Conclusion:

E-commerce has become an essential part of our daily lives, providing us with the convenience of purchasing products and services online. However, with the rise of e-commerce, concerns about data protection have also emerged. Data protection is crucial to ensure that personal information is kept secure and not misused by unauthorized individuals or entities. Saudi Arabia has implemented regulations to protect consumer data and privacy in e-commerce, including the development of a number of laws and regulations protecting personal data, those laws and regulations include: the Credit Information Law, the Anti-Cyber Crime Law, E-Commerce Law, Personal Data Protection Law, National Management Data Office Interim Regulations. The country's data protection laws and regulations are designed to safeguard the privacy and security of personal information while ensuring that businesses comply with certain obligations when collecting, processing, and storing data. through the issuance of many regulations in various fields that prevent the use of private data in violating ways, However, despite the efforts, there are still many possible challenges which face the legal environment of data protection. Those challenges include ambiguity in some texts and definitions, and restrictive cross-border data transfer requirements. It is recommended to improve clarity in some concepts and definitions set out in the relative laws and provisions, especially on the most important one in similar laws which are terms such as "consent", "implied consent", "explicit consent", and improvement of cross-border transfer of data requirements, as when transferring of personal data outside the Kingdom it is mandatory for controllers to obtain the competent authority's approval of personal data transfer in each case, a similar mechanism as the GDPR's adequacy list could be considered in Saudi Arabia.

REFERENCES:

Abdullah, Ahmed (2020) "Consumers' Personal Data Protection in Saudi Arabia: A Comparative Analytical Study"University of Kansas ProQuest Dissertations Publishing, 2020. 27961274.

A. Aarnio, On Legal Reasoning (1977) 75. On the distinction between ambiguity and vagueness see M. Azar, 'Transforming Ambiguity into Vagueness in Legal Interpretation' in A. Wagner et al. (eds.), Interpretation,Law and the Construction of Meaning (Springer, Dordrecht 2007) P. 121-137.

Roznai, Yaniv, "A Bird Is Known by Its Feathers - On the Importance and Complexities of Definitions in Legislation Special Issue on Legislative Drafting and Linguistics" PB - Routledge, P.147

Phillips, M. International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). Hum Genet 137, 575–582 (2018).

Michael B. Rappaport "The Ambiguity Rule and Insurance Law: Why Insurance Contracts Should Not Be Construed against the Drafter" 30 Ga. L. Rev. 171 (1995-1996)

Saudi Basic law of Governance (A/90)

Saudi E-Commerce Law (M/126)

Saudi Credit Information Law (M/37)

Saudi Anti-Cyber Crime Law (M/17)

Saudi Personal Data Protection Law (M/19)