Migration Letters

Volume: 21, No: S8 (2024), pp. 432-450

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Received: 08-05-2000
Accepted: 22-07-2000

Individual Control over Personal Data in the Saudi Law Consent as a Case Study: A Comparative and an Analytical Study

Dr. Abdulaziz bin Ahmed Almezeini

1. Introduction

In accordance with Royal Decree No. M/19 dated 9/2/1443H corresponding to 16/09/2021G, the Saudi Arabian Personal Data Protection Law "PDPL" was promulgated in its first edition. This legislative ini[1]tiative was undertaken to position the Kingdom at the forefront of the substantial global advancements in the realm of data, widely recognized as the cornerstone of the twenty-first century. The impetus behind this regulatory development was to align with the digital transformation experienced by the Kingdom of Saudi Arabia, keeping pace with the global trends that had preceded many nations. The European Union took the lead in formulating this kind of regulations designed to safeguard personal data, particularly in the face of large technology corporations that could potentially encroach upon individual rights. Subsequently, the world benefited from the legislation enacted by the European Union, commonly known as the General Data Protection Regulations "GDPR". Among the nations that drew upon this legal framework is the Kingdom of Saudi Arabia.

However, the Kingdom of Saudi Arabia has exhibited a more stringent commitment to data protection than the European Union. This is evident in two crucial aspects: data localization and data processing. In the matter of data localization, the Kingdom stipulated that all data must be preserved and stored exclusively within the territory of Saudi Arabia. Additionally, concerning data processing, Saudi Arabia prohibited companies from engaging in such activities without obtaining explicit consent from the data subject.

Since the issuance of the PDPL, it has faced strong opposition from global technology companies operating within the Kingdom. The Kingdom's adoption of principles even more rigorous than those endorsed by the European Union was wholly unexpected. In response to a request from the Saudi Data and Artificial Intelligence Authority, Royal Decree No. 51627 was issued on 18/8/1443H corresponding to 21/03/2022G, deferring the enforcement of the PDPL for a period of 540 days from its publication in the official gazette. This delay aims to provide experts and stakeholders with the opportunity to review the law and assess its compatibility with the Kingdom's reality in this domain.

Nevertheless, despite this opposition and the passage of an extended timeframe, the second edition of the PDPL was promulgated by Royal Decree No. M/148 dated 5/9/1444H corresponding to 27/03/2023G. This version retained the majority of provisions that encountered resistance from major technology companies, without deletion or

Assistant Professor in the Department of Legal Policy, Higher Institute of Judiciary - Imam Muhammad bin Saud Islamic University.

modification. Among these provisions, the most noteworthy include data localization and data processing requirements.

Given the significance of both subjects, I conducted peer-reviewed paper on the first topic, which was subsequently published in the Journal of the Iraqi University in the month of Rajab 1444H[2]. As for the second topic, it constitutes the focus and subject of examination in this research, particularly with regard to the consent issued by the data subject, deemed the foremost and foundational legal basis permitting companies to process their data.

1.1 Significance of the Research:

The research holds considerable importance, as elucidated to some extent in the introduction, and further highlighted through the following points:

1. The PDPL represents an entirely new legal framework within the Kingdom of Saudi Arabia. Consequently, it necessitates a range of research studies to expound upon its provisions and concepts.
2. Data protection laws are relatively new on a global scale, resulting in a scarcity of references. Therefore, research in this area enriches the global legal library.
3. The subject of data processing is among the pivotal issues addressed by the Saudi Arabian PDPL, as it directly impacts the needs of both companies and individuals.
4. Consent from the data subject stands as one of the foremost legal bases permitting the processing of personal data. The research's significance stems from the critical nature of this sensitive subject.
5. The research serves as an educational tool for individuals, enlightening them about their rights in dealing with major technology companies. It informs them of when their consent is valid, and processing can occur based on it. Furthermore, it delineates the rights they are entitled to thereafter.
6. Other reasons, difficult to exhaustively list in this research, contribute to its significance.

1.2 Research Problem:

The research problem revolves around a fundamental legal basis that allows companies in possession of personal data related to individuals to process it through various types of processing, as will be elucidated in the depths of the research. This legal basis is the personal consent of the data subject to allow the company to process their personal data. This consent, issued by the individual, has conditions and requirements. If these conditions are met, the consent becomes valid, and the company is entitled to process the data based on that consent. However, if any of these conditions are not met or are disrupted, the consent becomes invalid, and the company is not entitled to process the data based on that consent. The research will focus on analyzing these conditions and regulations that must be met in the consent issued by the data subject to ensure its validity for processing in accordance with the Saudi PDPL and its executive regulations.

2. Methodology of the Research and Its Scope:

The research will adopt an analytical and comparative methodology by analyzing the texts of PDPL and its executive regulations and comparing them with the General Data Protection Regulation (GDPR) of the European Union. The rationale behind this approach is that European law serves as the origin in this field, as the European Union pioneered legislation protecting personal data globally. Many countries, including the Kingdom of Saudi Arabia, have subsequently adopted and incorporated significant portions of it into their own data protection laws. In contrast, the United States lacks federal legislation specifically addressing personal data protection, leaving this realm to contractual

[2] Almezeini, Abdulaziz bin Ahmed. (1444 H. – 2023G). Data Localization (A Comparative Legal Study). Journal of the University of Iraq. Issue 584. Volume 2, Page 58. (https://www.iasj.net/iasj/download/5e129bb8968f0e90).

relationships between technology companies and individuals without direct state intervention.

Therefore, the comparison is confined to European Union law, with some allusions in specific areas of the research to clarify the existing situation in the United States.

From the foregoing, the scope of the research is limited to the Saudi PDPL, issued by Royal Decree No. M/19 dated 9/2/1443H corresponding to 16/09/2023G, as amended by Royal Decree No. M/148 dated 5/9/1444H corresponding to 27/03/2023G, and its executive regulations published in Umm Al-Qura newspaper on 7/9/2023G[3]. Additionally, the research encompasses the General Data Protection Regulations of the European Union, as officially published on the European Union's official website[4].

2.1 Primary Obstacles:
The primary obstacles to accomplishing a thorough scientific study on this subject stem from the complete absence of local references. This scarcity is attributed to the recent emergence of Law related to the subject matter, observed at both the local and international levels. Consequently, in many aspects, the research has relied on analysis, comparison, and the utilization of certain articles and scientific papers previously published in this field in the English language.

Additionally, among the reasons for this scarcity is the absence of federal-level regulations governing the protection of personal data in the United States up to the present time. Hence, law reviews in this field is limited within American universities.

2.2 Research Plan:
- Preliminary Section
- First Section: Legal Basis for Requiring the Consent of the Data Subject for Processing Their Personal Data
- Second Section: Consent Requirements
- Third Section: Legal Capacity of the Consent Issuer
- Fourth Section: Rights Arising from Granted Consent
- Conclusion

2.3 Preliminary Section
In this section, we will address the key terms outlined in the research, as follows:

- **Personal Data:**
  Definition of Personal Data as a Term:
  The PDPL provides a clear and unambiguous definition of personal data, which is unsurprising given its centrality to the Law. It defines personal data as follows:
  "Any data - regardless of its source or form - that can lead to the specific identification of an individual or make their identification possible directly or indirectly. This includes, but is not limited to name, national ID number, addresses, contact numbers, license numbers, records of personal possessions, banking account numbers, credit card information, and still or moving images of the individual. Personal data encompasses information of a personal nature."[5]
  According to this definition, personal data encompasses information that leads to the identification of an individual. This implies that data which does not lead to the

[3] The Executive Regulations of the Personal Data Protection System. (2023). Umm Al-Qura Newspaper. Effective Date: September 7, 2023. (https://uqn.gov.sa/details?p=23595).
[4] General Data Protection Regulation (GDPR). EU. Regulation 2016/679 of the European parliament and of the council of 27 April 2016. (https://gdpr-info.eu/).
[5] The first article of the Personal Data Protection Law issued by Royal Decree No. (M/19) on 2/9/1443 H corresponding to 03/04/2022G.

identification of the person is excluded from the definition and, consequently, is exempt from the provisions of the law. Examples of such excluded information include data related to society as a whole or a general category, such as students, teachers, merchants, and others. Such data is considered public information and does not allow for the specific identification of an individual, unlike, for instance, a mobile phone number or email address as outlined in the definition.

It is also noteworthy that, in the application of the law, personal data pertains to individuals, or in other words, natural persons. Legal entities, such as companies and government entities, are not covered by the law, as these data are governed by other regulations.

This approach in defining the scope of personal data aligns with the General Data Protection Regulations (GDPR) adopted by the European Union.[6] – As will become evident during this discussion -, the underlying principle of such laws is to protect individuals and their privacy in the face of the dominance of major technology companies and their control over individual data.

The law has also provided a clear definition of the data subject to avoid any ambiguity. The data subject is defined as "the individual to whom personal data relates, or the person representing them, or the one who has legal guardianship over them."[7]

The data subject is either the individual themselves or someone who validly represents them through a legal agency, or someone with legal guardianship over them. Further details on this matter will be elaborated in the third section.

- **Processing**

Definition of Processing in Legal Terms:

In the context of the PDPL, processing has a specific and precise meaning as clarified by the law. It is defined as follows:

"Any operation performed on personal data by any means, whether manual or automated, including but not limited to: collection, recording, storage, indexing, sorting, organization, coordination, storage, modification, updating, merging, retrieval, usage, disclosure, transfer, publication, data sharing or linkage, blocking, erasure, and destruction."[8]

The definition emphasizes generality and inclusiveness. Therefore, any operation carried out on an individual's personal data, starting from its collection to analysis, classification, publication, and beyond, falls within the scope of processing. This is significant, as processing is not limited to analytical and indexing operations but encompasses activities such as collection and publication under the provisions of the processing regulations.

2.4 Controller and Processor:

These terms will be reiterated in the context of the discussion, so it is necessary to clarify them before delving into the details. The law defines them as follows:

"**Controller:** Any public entity or natural or legal person that determines the purpose of processing personal data and how it is processed, whether processing the data directly or through a processor."

[6] Personal Data. General Data Protection Regulation (GDPR). EU.(https://gdpr-info.eu/issues/personal-data/#:~:text=GDPR%20Personal%20Data&text=Only%20if%20a%20processing%20of,identified%20or%20identifiable%20natural%20person).

[7] The first article of the Personal Data Protection Law issued by Royal Decree No. (M/19) on 2/9/1443 H corresponding to 03/04/2023G.

[8] The first article of the Personal Data Protection Law. Previous reference

"**Processor:** Any public entity or natural or legal person that processes personal data on behalf of and for the benefit of the controller."[9]

To illustrate the difference between these terms, consider a company whose primary activity is delivering orders through its electronic application. This company possesses a vast amount of personal data from users who have registered on its application. However, due to its focus on its core business of order delivery, it lacks the technical and practical capability to leverage the data it holds. Therefore, this company might engage another technology company with expertise in data processing. The technology company would be contracted to process the data on behalf of and for the benefit of the order delivery company. In this context, and according to the definitions provided in the law, the order delivery company is the controller because it "determines the purpose of processing personal data and how it is processed." On the other hand, the technology company is the processor because it "processes personal data on behalf of and for the benefit of the controller."

3. First Section

Legal Foundation

The PDPL explicitly stipulates the requirement for the data subject's consent for the processing of their data by the controller. In fact, the Law considers consent as the fundamental condition for the legitimacy of processing. Article 5 of the system states:

"-Except for the cases stated in this Law, neither Personal Data may be processed, nor the purpose of Personal Data Processing may be changed without the consent of the Data Subject. The Regulations Shall set out the conditions of the consent, the cases in which the consent must be explicit, and the terms and conditions related to obtaining the consent of the legal guardian if the Data Subject fully or partially lacks legal capacity.."
The executive regulations of the Law affirm this foundation, stating that the consent of the data subject is the primary legal justification for allowing the processing of such data. The regulations state:

"Article 3: The provisions and procedures stated in this Law shall not prejudice any provision that grants a right to the Data Subject or confers better protection to Personal Data pursuant to any other law or an international agreement to which the Kingdom is a party.

This principle and requirement in the Saudi Law closely align with the European General Data Protection Regulations (GDPR). It is worth noting that the executive regulations in their formulation are almost identical, with minor differences, to the European GDPR. Article 6 of the GDPR states:
"Article 6:
Processing shall be lawful only if and to the extent that at least one of the following applies:
)1(the data subject has given consent to the processing of his or her personal data for one or more specific purposes."[10]

This contrasts with the United States, where there is currently no unified federal law for the protection of personal data privacy. Therefore, there is no law requiring companies to obtain consent from the data subject before processing such data. Instead, there are only non-binding recommendations from the Federal Trade Commission (FTC) advising companies to " (i) provide clearer, shorter, and more standardised privacy notices that

[9] Previous Reference
[10] Article 6. General Data Protection Regulation (GDPR). EU. (https://gdpr-info.eu/art-6-gdpr/).

enable consumers to better comprehend privacy practices; (ii) provide reasonable access to the consumer data they maintain that is proportionate to the sensitivity of the data and the nature of its use; and (iii) expand efforts to educate consumers about commercial data privacy practices.."[11]

Even the California Consumer Privacy Act (CCPA), which was enacted in 2018 and is considered one of the most comprehensive state laws in the U.S. for protecting personal data privacy, does not require consent for processing personal data. It grants rights to data subjects, such as the right to know and the right to opt-out, without explicitly requiring consent for processing.[12]

This means that, in U.S. law, the default is that processing personal data is allowed, and companies are not obligated to demonstrate a "legal basis" for processing data as required by privacy laws in other countries.[13]

This contrasts with European law, which considers processing as initially prohibited to protect individual privacy. Companies are not allowed to process data unless they obtain consent from the data subject. European law prioritizes the protection of the citizen, the individual, and their privacy, particularly from the exploitation by companies and capital. Saudi Arabia has aligned itself with the European approach, considering the processing of personal data prohibited unless consent is obtained from the data subject. This is consistent with the principles of privacy enshrined in human rights covenants, which the Kingdom of Saudi Arabia has ratified. Article 12 of the Universal Declaration of Human Rights emphasizes:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.."[14]

Individuals shall not be exposed to arbitrary interference in their private life, family matters, residence, or correspondence, nor to campaigns that impinge upon their honor and reputation. Every person has the right to legal protection from such interference or campaigns.

The private life mentioned here (or privacy) encompasses a comprehensive concept. It is not merely the right of individuals to avoid eavesdropping on their telephone conversations, for example, or to inquire about their daily activities; rather, it extends far beyond that. Privacy transcends the physical space of individuals to include all aspects of cyber life. It has a direct connection to all information and personal data on an individual's mobile phone, personal computer, and all data on the internet. In this context, “privacy” is what lets you establish boundaries to protect your information and your life from unwanted interference”.[15]

The significance of privacy becomes apparent when identifying the violator of privacy. If the violator is an ordinary person, it is relatively easy to protect an individual's privacy using conventional and possible methods. However, if the violator is a major technology

[11] Data Protection Laws and Regulations. (2023). The International Comparative Legal Guides (ICLG) (https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa).
[12] California Consumer Privacy Act (CAPPA). (2018). (https://cppa.ca.gov/regulations/pdf/cppa_act.pdf)
[13] Legal Bases for Processing of Personal Data. (2022). Global Data Privacy & Security Handbook. Baker McKenzie. (https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/north-america/united-states/topics/legal-bases-for--processing-of-personal-data)
[14] The Universal Declaration of Human Rights. United Nations. (https://www.un.org/ar/universal-declaration-human-rights/).
[15] Soken-Huberty, Emmaline. Is Privacy a Human Right. Human Rights Careers. (https://www.humanrightscareers.com/issues/is-privacy-a-human-right/).

company, violating privacy becomes very easy, and the individual whose privacy has been violated may not even be aware of it. Such large companies may exploit people's data for their own interests, as exemplified by the Facebook scandal.

"Governments aren't the only entities that want your data. Corporations are constantly collecting info to study your shopping habits, what you like and dislike, and more. They often say it's to improve customer service, but this information can be weaponized, too. Cambridge Analytica is one of the most glaring examples. The organization took data from Facebook – without user consent – and used it to influence voters through political ads. This is a violation of privacy rights. After the story broke, Cambridge Analytica filed for Chapter 7 bankruptcy in 2018, while the FTC fined Facebook $5 billion in 2019."[16]

Governments play a crucial role in protecting individuals' data privacy from the violations of technology companies. Based on this foundation - the protection of privacy - the principle of obtaining consent for the processing of personal data for each individual is established.

Privacy has a legal basis in Islamic Sharia, as Allah, prohibited eavesdropping and listening to others explicitly in the Holy Quran, stating: "O you who have believed, avoid much [negative] assumption. Indeed, some assumption is sin. And do not spy or backbite each other. Would one of you like to eat the flesh of his brother when dead? You would detest it. And fear Allah; indeed, Allah is Accepting of Repentance and Merciful".[17]

The Prophet, peace be upon him, also emphasized this prohibition. Abu Huraira reported: "The Prophet, peace and blessings be upon him, said, "Beware of suspicion, for suspicion is the worst of false tales. Do not look for others' faults. Do not spy on one another, and do not practice Najsh, which is to offer a high price for something in order to allure another customer who is interested in the thing. Do not be jealous of one another, and do not nurse enmity against one another. Do not sever ties with one another. Become the servants of Allah as brothers."[18]

Furthermore, Allah, Almighty, prohibited entering people's homes without their permission "O you who have believed, do not enter houses other than your own houses until you ascertain welcome and greet their inhabitants. That is best for you; perhaps you will be reminded. And if you do not find anyone therein, do not enter them until permission has been given you. And if it is said to you, 'Go back,' then go back; it is purer for you. And Allah is Knowing of what you do."[19]
This privacy, as dictated by Islamic law, applies to everything in an individual's possession and related information and possessions. It is impermissible, according to Sharia, to benefit from or access such information without permission.

Based on this legal principle, requiring consent for the processing of personal data aligns with the principles of Islamic law and international human rights conventions.

4. Section Two

Consent Requirements

[16] Previous Reference.
[17] Surah Al-Hujraat, verse (12).
[18] Al-Nawawi, Muslim ibn al-Hajjaj al-Qushayri. Sahih Muslim. Edited by Muhammad Fuad Abdul-Baqi. Issa Al-Babi Al-Halabi Press and Co. Cairo. Vol. 4, Page 1985. Hadith Number: 5263. Chapter: "Prohibition of Suspicion, Spying, Competing, and Contending, and Similar Matters."
[19] Surah Al-Nour, verses (27,28)

First: Consent Must Be Given Willingly.
This principle, as outlined in the regulations, stands as one of the foremost regulations and holds significant importance. The consent given willingly implies that it is granted without coercion and is not provided under circumstances that force the data subject to give it. Coerced and compelled consent does not represent the genuine will of the individual but rather reflects compliance with external pressures and does not align with true consent.[20]

This principle addresses various issues, with a primary focus on the imbalance of power between the data subject and the controlling entity seeking consent. In cases where the controlling entity possesses substantial power and control, the data subject may feel compelled to give consent against their true desires, acknowledging the dominance of the controlling entity. Notably, this applies to contracts of submission where power dynamics vary.

For instance, if the controlling entity is a powerful government agency, the data subject may be coerced into giving consent due to fear. In such instances, it is not advisable for a government entity, processing personal data, to solely rely on consent as the legal basis for processing. Instead, an alternative legal basis defined in Article 6 of the regulations should be considered. Specifically:

"In the following cases, Processing of Personal Data shall not be subject to the consent referred to in Paragraph (1) of Article (5) herein:

(a) If the Processing serves actual interests of the Data Subject, but communicating with the Data Subject is impossible or difficult.;
(b) If the Processing is pursuant to another law or in implementation of a previous agreement to which the Data Subject is a party;
(c) If the Controller is a Public Entity and the Processing is required for security purposes or to satisfy judicial requirements."[21]

This exclusion is based on the understanding that consent, in situations of power imbalance and data subject fear, is not an acceptable form of consent, as it is not freely given.[22]

Furthermore, if the controlling party seeking data processing is also the employer, and the data subject is an employee within the same company, the company's interest in processing personal data for its benefit, such as monitoring employee behavior, may create a situation where the employee is compelled to give consent. In such cases, the consent is deemed unacceptable as it is not given freely.[23]

The regulations, in Article 7, emphasize this point:

"The consent referred to in paragraph (1) of Article (5) of this Law may not form a condition of providing a service or a benefit, unless such service or benefit is directly related to the Processing of Personal Data for which the consent is given.."[24]

An example illustrating this scenario is when an individual applies for a personal loan from a bank, and the bank stipulates the requirement for the data subject's consent to process their personal data for the bank's purposes and interests. If the data subject refuses, the bank

[20] Meskenaite, Gabbi. (2022). An examination of the criteria for valid consent under the GDPR in the light of the rationale and technological neutrality. Graduate Thesis. Faculty of Law. Lund University. Page 26. (https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9096679&fileOId=9099573).
[21] Article 5. Personal Data Protection Law..
[22] Meskenaite, Gabbi. (2022), page 27.
[23] Same Reference.
[24] Article 7. Personal Data ProtectionLaw.

might withhold the loan. Even if the data subject agrees, the consent is deemed unacceptable because it has become “a condition for providing a service or offering a benefit.” This condition is crucial, and both companies and individuals need to be mindful of its implications.

The application of the principle of free will in granting consent is extensive, and it cannot be exhaustively covered in this discussion. However, the overarching framework revolves around two fundamental elements: the absence of coercion and the consideration of power imbalances between the controlling entity seeking to process data for its purposes and the individual data subject.

Second: The Purpose of Processing Must Be Clear and Specific

This principle serves as a preventive measure against the misuse of personal data consent by the controlling entity for purposes other than those intended by the data subject. It requires that the request for consent from the controlling entity to the individual explicitly outlines the purposes for which the data will be processed. The regulations stipulate that the consent request must encompass the specific purposes for which the data will be processed, and these purposes must be clear and well-defined in the request. This implies that " consent is requested as part of a paper contract that covers other matters, the consent request must be identifiable; Information on the processing purpose must be distinctly and clearly provided and preferably presented in a separate document so that the consent information and request is specific rather than bundled with other matters ."[25]
Several implications derive from this condition:

Firstly, if consent is sought for vague purposes, such as stating that the processing aims for "marketing objectives," "future research," or "enhancing user experience in the future,"[26] such consent is deemed unacceptable. The lack of clarity and ambiguity in these purposes contradicts the requirement for explicit and well-defined purposes. It is preferable for consent to be broad and general for data processing in general than to accept such unclear purposes.

Secondly, requiring clarity and specificity of purposes necessitates obtaining separate consent for each purpose of processing. The regulations explicitly state in paragraph (1-h) of Article 11: " A separate consent shall be obtained for each Processing purpose.."[27] For instance, if a data subject owns multiple devices, and a manufacturing company seeks to process personal data to enhance both devices, the company cannot obtain a single consent covering both purposes. Instead, independent consent must be obtained for processing data for the enhancement of each device separately. Any attempt to obtain a single consent for multiple purposes renders the consent unacceptable according to the regulations.

Thirdly, the principle emphasizes the concept of limited consent, meaning that the consent granted by the data subject is restricted and confined to the specific purpose agreed upon. The controlling entity is prohibited from expanding the processing beyond the agreed-upon purpose. For instance, if consent is obtained for developing a specific device, the company cannot utilize that consent to develop another device. As mentioned earlier, it is the responsibility of the controlling entity to obtain consent for each evolving purpose.

Fourthly, the regulations state that "those purposes shall be clear, specific, and shall be explained and clarified to the Data Subject before or at the time of requesting consent." [28] This crucial requirement pertains to the timing of elucidating and disclosing the purposes.

---

[25] Meskenaite, Gabbi. (2022). P.31. Previous Reference.
[26] Same Reference.
[27] Executive Regulations of the Personal Data Protection Law. (2023). Previous reference.
[28] Same Reference.

The controlling entity is not allowed to first obtain consent and then clarify the purposes later. The purposes must be transparent and fully disclosed before or at the time of seeking consent, failing which the consent is considered unacceptable.

Fifthly, concerning the issue of clarity of purposes, the data subject must be provided with sufficient information about the purposes to enable them to make an informed decision on whether to grant consent. If the information provided is inadequate, the purposes will not be considered clear enough. If consent is obtained under such circumstances, it is deemed unacceptable. This principle is particularly significant for companies addressing ordinary users who may lack the expertise of specialists. The information provided must be sufficient for the user's level of understanding and should be presented with the appropriate level of clarity.[29]

Third: Consent Must Be Explicit.
The second paragraph of Article 11 of the regulations stipulates that "Data Subject's consent shall be explicit in the following cases:

1. When the Processing involves Sensitive Data;
2. When the Processing involves Credit Data;
3. When decisions are made solely based on automated Processing of Personal Data".[30]

The term "explicit consent" refers to the requirement that consent serves as the sole legal justification. In other words, no other legal justification allows the controlling entity to process personal data. These justifications are explicitly stated in Article 6 of the PDPL and are as follows:

" In the following cases, Processing of Personal Data shall not be subject to the consent referred to in Paragraph (1) of Article (5) herein:

1. If the Processing serves actual interests of the Data Subject, but communicating with the Data Subject is impossible or difficult.
2. -If the Processing is pursuant to another law or in implementation of a previous agreement to which the Data Subject is a party.
3. If the Controller is a Public Entity and the Processing is required for security purposes or to satisfy judicial requirements..
4. -If the Processing is necessary for the purpose of legitimate interest of the Controller, without prejudice to the rights and interests of the Data Subject, and provided that no Sensitive Data is to be processed. Related provisions and controls are set out in the Regulations.."[31]

Furthermore, the regulations specify that consent must be explicit, especially when dealing with sensitive or credit-related personal data. The system defines sensitive and credit-related data in its first article as follows:

"Sensitive Data: Personal Data revealing racial or ethnic origin, or religious, intellectual or political belief, data relating to security criminal convictions and offenses, biometric or Genetic Data for the purpose of identifying the person, Health Data, and data that indicates that one or both of the individual's parents are unknown."[32]

[29] Meskenaite, Gabbi. (2022). P.32. Previous reference.
[30] The executive regulations of the Personal Data Protection Law. (2023). Previous reference.
[31] The Personal Data Protection Law issued by Royal Decree No. (M/19) dated 2/9/1443 H corresponding to 03/04/2023G. Each of these justifications warrants separate consideration. However, our focus in this research is on one justification, namely, consent.
[32] The Personal Data Protection Law issued by Royal Decree No. (M/19) dated 2/9/1443 H corresponding to 03/04/2023G.

"Credit Data: Any Personal Data related to an individual's request for, or obtaining of, financing from a financing entity, whether for a personal or family purpose, including any data relating to that individual's ability to obtain and repay debts, and the credit history of that person."[33]

There is no room to delve into the details of this type of data and other legal justifications, as each requires separate consideration. Our focus here is on the requirement of consent itself.

Therefore, if consent is the sole legal justification or is related to sensitive or credit-related data, it must be explicit and not implicit. This means that the data subject must clearly and expressly state their agreement to the processing of their personal data. Conversely, silence or failure to object, even if deemed implicit consent, is not acceptable in this context. To avoid legal risks, the consent checkbox, for example, in an online form, must be left empty, and the data subject must deliberately choose to consent for the explicit condition to be met. The same applies if a website displays a message upon entry, stating that "browsing this site constitutes your consent to the processing of your data." proceeding with a service does not constitute consent, as such action would neither be specific nor informed and thus not possible to attribute to consen.[34]

Fourth: Consent Documentation for Future Verification.
This principle mandates that the controlling entity must store the consents obtained from data subjects and preserve them for future verification. In the event of a data breach or unauthorized disclosure, or if a data subject raises objections to the processing of their personal data by the controlling entity, the controlling entity must have stored these consents. This ensures that authorities can investigate the consent and confirm that it complied with regulatory conditions. The controlling entity cannot claim to have destroyed or failed to retain the original consents. In such a case, the controlling entity would bear full responsibility, even if it obtained the consent legally and soundly.[35]

In general, this means that the burden of proof regarding consent, in the event of any dispute, falls on the controlling entity. The controlling entity must demonstrate that the consent relied upon as a legal justification for processing personal data was valid and met the regulatory conditions outlined in the law and regulations.
On the other hand, the regulations do not specify the information that must be stored. However, the standard in this context can be inferred, indicating that the required **stored data includes:**[36]

1. **Identity of the Consenting Party:** Name of the individual who provided consent: If no name is available, the identifier (username), mobile number, or email address.
2. **Timestamp of Consent:** A copy of a dated written document if consent was obtained in writing. Online records indicating the time of consent if obtained electronically. In the case of verbal consent, a record must be kept with notes on the time and date of the conversation.
3. **Purpose of Consent Request:** A copy or screenshot of the consent request document or webpage, including information about the purposes for which data

[33] Same Reference.
[34] Meskenaite, Gabbi. (2022). P.32. Previous reference.
[35] Breen, S et al. (2020). GDPR: Is your consent valid?. Business Information Review (BIR). (DOI: 10.1177/0266382120903254).
[36] How should we obtain, record, and manage consent?. Information Commissioner's Office (ICO). (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/how-should-we-obtain-record-and-manage-consent/#how4).

processing is intended. This is crucial for investigations to verify compliance with regulations, especially regarding the clarity and specificity of stated purposes.

4. **Method of Consent:** For written consent, the actual document should be retained. For online consent, electronic records should be stored digitally. Verbal consent should be recorded, capturing the words spoken by the individual providing consent.

These are the key pieces of information that must be preserved to verify consent in the future, meeting the standard for alleviating responsibility on the part of the controlling entity in case of a dispute over consent.

5. Section Three

Legal Capacity of the Consent Issuer

Paragraph (1-c) of Article Eleven of the Executive Regulations stipulates that the consent of the data subject must emanate from full legal capacity; otherwise, it becomes null and void. However, the regulations neither define nor elaborate on the concept of "full legal capacity." To elucidate this, reference is made to other relevant statutes, notably the Civil Transactions Law issued by Royal Decree No. M/191 dated 29/11/1444 H corresponding to 18/06/2023. According to Article Twelve of said system:

" 1. A fully competent person is a person who has reached the age of majority, has full mental capacity, and has not been interdicted. 2. The age of majority shall be 18 years according to the Hijri calendar.."[37]

Thus, the criteria for full legal capacity are threefold:

1. Reached the age of majority.
2. Full mental capacity.
3. Has not been interdicted.

Consequently, those lacking legal capacity include those deemed “fully incompetent person” who expressly mentioned in Article Thirteen of the Law:

“(1. An incompetent person is a person who is non-discerning due to young age or idiocy. 2. A person under the age of seven shall be deemed a non-discerning person)."[38]

Similarly, “partially incompetent persons”, as outlined in Article Fourteen of the Law, have the some provisions, and they include:

“a) A minor who has reached the age of discernment but has not reached the age of majority. b) A lunatic: A person who is deficient in reason but has not reached the point of idiocy. c) A person interdicted for being a spendthrift or for being imprudent..”[39]

In summary, the essence of the statement is that the regulations stipulate obtaining consent from individuals with full legal capacity. In cases where the data subject lacks full legal capacity, consent must be obtained from their legal guardian or legal representative, as explicitly stated in Article 5 of the PDPL.

It is noteworthy that there was initially an exception to this general age requirement for individuals aged between 13 and 18, as outlined in the draft executive regulations published for the public.[40] According to Article 12, Paragraph 4 of the draft:

[37] The Civil Transactions Law issued by Royal Decree No. (M/191) dated 29/11/1444 H corresponding to 18/06/2023. (https://www.uqn.gov.sa/details?p=23125).
[38] Previous Reference.
[39] Same Reference.
[40] Draft Executive Regulations of the Personal Data Protection Law. Survey Platform. National Competitiveness Center.

"Taking into consideration Article 26 of the regulations, for control purposes—unless the data subject's information is sensitive—obtaining consent from individuals aged between 13 and 18 can be done without the need for approval from the legal guardian, provided that the consent request and informative materials are prepared in a language and formulation suitable for the understanding of the age group."

This implies that individuals in the age group of 13 to 18 years can provide consent directly without requiring approval from the legal guardian or legal representative, subject to two conditions:

1. The data being processed should not be sensitive. The system has defined sensitive data as "any personal data that includes an indication of the individual's racial or tribal origin, religious, intellectual, or political beliefs, or evidence of their membership in associations or non-profit institutions. This also includes criminal and security data, as well as biometric data that identifies identity, genetic data, credit data, health data, location data, and data indicating that the individual is of unknown parentage or parentage."
2. The language used to obtain consent from this age group should be understandable and suitable for their intellectual capacity and age, allowing them to have the ability to make an informed decision.

However, in the final version of the executive regulation published in the official gazette (Umm Al-Qura newspaper), this paragraph was entirely deleted.[41] Thus, the Saudi regulator has taken a more stringent stance even compared to the European Union regarding the age of full legal capacity. The general data protection law in the EU stipulated that the minimum age for valid consent is 16 years,[42] and if an individual is below this age, the consent of the legal guardian is required. In contrast, the Saudi regulator specified the minimum age as 18 years.

The European law did not stop at this limit; it allowed member states to lower the minimum age, provided it does not fall below 13 years. Some laws, including the British law, adopted this direction, considering consent acceptable if given by an individual aged 13 or older.[43] In cases where the data subject is not legally competent, consent for processing their data must be obtained from their legal guardian, according to Article 5 of the PDPL and as outlined in Article 13 of the executive regulation. As the regulation did not clarify the meaning of "legal guardian", the definition can be derived from other related laws, specifically, the latest law, the Family Law issued by Royal Decree No. M/73 dated 6/8/1443H corresponding to 26/02/2023G, where Article 137 states:

" 1. A guardian is the father, or any person designated by the court. 2. A trustee is the person designated by the father to assume trusteeship upon the father's incapacitation or death. The guardian or trustee, as the case may be, shall represent and manage the affairs of the incompetent person.."[44]

If these conditions are not met, the court appoints a custodian, as stated in Article 125:

---

[41] The executive regulations of the Personal Data Protection Law. (2023). Previous reference.
[42] Article 8. General Data Protection Regulation (GDPR). EU. (https://gdpr-info.eu/art-8-gdpr/).
[43] What are the rules about an ISS and consent?. Information Commissioner's Office (ICO). (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-are-the-rules-about-an-iss-and-consent/#a2).
[44] The Family Law issued by Royal Decree No. M/73 on 6/8/1443 Hijri corresponding to 09/03/2022G (https://www.uqn.gov.sa/?p=11442)

" Subject to Article 10 of this Law, a custodian shall satisfy the following requirements: 1. Competency. 2. Ability to raise and provide protection and care for the person subject of custody. 3. Being free from dangerous infectious diseases.."[45]

The legal guardian or custodian, when consenting on behalf of an individual lacking or with diminished legal capacity, is subject to several provisions outlined by the regulations:[46]

Firstly: The guardian or custodian shall implement all the rights accorded to the data subject under the law and regulations, and any consent provided by them shall be deemed as if it were given by the personal data subject themselves.

Secondly: The legal guardian or custodian must consider the best interests of the data subject lacking legal capacity, rather than prioritizing their own personal interests. If it is established that the legal guardian or custodian granted consent for personal gain, causing harm to the data subject, they bear full responsibility.

Thirdly: The regulations stipulate that the controller " in case of Processing Personal Data of a Data Subject that lack full or partial legal capacity, obtaining the consent of the legal guardian shall be conditioned upon taking appropriate measures to verify guardianship validity over the Data Subject "[47]

Verification of the legal guardian's identity and confirmation of their guardianship is required, utilizing the same procedures employed to verify the identity of the data subject, whether through the "Absher"[48] system or official documents. If the entity is not involved in identity verification processes, relying on user-provided information, it typically queries the user about their age during account creation. If the user claims to be under 13 years old, these companies generally either prevent them from completing registration or inquire about the email of their legal guardian or trustee to obtain their consent for account creation.

It is conceivable that individuals may provide false information about their age, especially when below the legal age. However, companies commonly absolve themselves of responsibility during the registration process, holding users entirely accountable for the consequences of any inaccuracies in the provided information.
The question remains: What is the Saudi regulator's stance on such challenges? The resolution of these issues remains unclear as the law is till new, and how relevant authorities will address these challenges is yet to be fully determined.

Fourthly: In the event that the personal data subject reaches full legal capacity, either by reaching the statutory age (18 years) or by the removal of any impediments to their legal capacity (such as guardianship), the data controller must transfer all powers related to their personal data from their former guardian or custodian to the personal data subject themselves..[49]

6. Section Four

Rights Arising from Granted Consent

There are two types of rights for individuals who have given their consent for the processing of their personal data, and these rights persist throughout the duration of the

[45] Previous Reference.
[46] The Executive Regulations of the Personal Data Protection Law. (2023). Previous Reference.
[47] Previous Reference.
[48] Absher is a comprehensive online platform developed by the Saudi Arabian government to provide a wide range of electronic services to citizens and residents. (https://www.absher.sa/wps/portal/individuals/Home/homepublic)
[49] Previous Reference

data controller's processing. The first type: rights limited to consent, and the second type: rights related to consent and other legal grounds for processing personal data.

As for **the rights limited to consent,** there is one right, namely the right to withdraw consent at any time by the data subject. The following points discuss some issues related to this right:

- The fifth article of the regulations, in its second paragraph, stipulates that the data subject may withdraw consent for the processing of their data at any time. It is also understood from this provision that if the data subject does not have the right to withdraw or is not enabled to exercise such a right, their consent is not considered valid. Therefore, the right to withdraw and revoke is deemed an essential condition for the validity of consent.[50]
- The same article is explicit in stating that the right to withdraw consent is a constant right at all times. This affirmation is further reiterated by the regulations in the first paragraph of Article Twelve. This implies that the right to withdraw is not subject to expiration, even after the passage of a certain number of years. Consequently, it necessitates the ongoing commitment of the data controller to fulfill the other requirements associated with this right, as elucidated below.
- The regulations, in the second paragraph of Article Twelve, stipulates that " Before requesting consent from the Data Subject, the Controller shall establish procedures that allow for the withdrawal of such consent and take the necessary measures to ensure their implementation, ensuring that consent withdrawal is as or easier than obtaining.."[51]

In this text, there are two important provisions. The **first** is that the data controller must establish procedures for withdraw, reconsideration of the consent before requesting the consent from the data subject. This implies that if the procedures for withdrawing consent are not prepared and in place before seeking consent, the consent is not considered acceptable.

The **second** provision is that the data controller must make the procedures for withdrawing consent equivalent to or easier than the procedures for obtaining consent, not more difficult. Otherwise, the consent is deemed unacceptable. For example, if consent is obtained through a specific application, the withdrawal should be possible through the same application without additional cost or effort. Similarly, if consent is granted by simply clicking "yes" on an organization's website, the withdrawal should follow the same straightforward process. If the data controller provides the option to withdraw consent by contacting a call center during business hours, despite obtaining consent through an application, this would be considered a violation of the regulation. This is because it involves a greater effort, rendering the consent unacceptable.[52]

- The third paragraph of the same article in the regulation also stipulates that " In the event of consent withdrawal, the Controller shall cease Processing without undue delay from consent withdrawal request. Consent withdrawal of shall not affect the lawfulness of Processing based on consent before its withdrawal."

This consists of two provisions. The **first** is that the data controller is obligated to promptly cease processing upon receiving the withdrawal of consent, specifically concerning data processing after the withdrawal. As for data that was processed both before and after obtaining consent, there is no issue. In other words, withdrawing consent does not

[50] Meskenaite, Gabbi. (2022). P.28. Previous Reference.
[51] The Executive Regulations of the Personal Data Protection Law. (2023). Previous Reference.
[52] Meskenaite, Gabbi. (2022). P.28. Previous Reference.

invalidate the consent granted earlier (this is the **second** provision), but it cancels it for subsequent processing.

As for the other type of rights, they are the **rights shared with other legal justifications for processing personal data.** These rights, as stipulated by Article 4 of the PDPL, are as follows:

"Data Subject shall have the following rights pursuant to this Law and as set out in the Regulations: 1-The right to be informed about the legal basis and the purpose of the Collection of their Personal Data. 2-The right to access their Personal Data held by the Controller, in accordance with the rules and procedures set out in the Regulations, and without prejudice to the provisions of Article (9) of this Law. 3-The right to request obtaining their Personal Data held by the Controller in a readable and clear format, in accordance with the controls and procedures specified by the Regulations. 4-The right to request correcting, completing, or updating their Personal Data held by the Controller. 5-The right to request a Destruction of their Personal Data held by the Controller when such Personal Data is no longer needed by Data Subject, without prejudice to the provisions of Article (18) of this Law.."

In truth, each of these rights deserves independent consideration. However, we will examine those related to consent as follows:

Firstly, the right to be informed: In general, individuals have the right to be fully informed about any data collection or processing activities involving their data. This falls within the requirements of transparency and disclosure, which are considered fundamental principles of the European General Data Protection Regulations.[53] This approach is also adopted by the Saudi Arabian PDPL. The executive regulations specify several matters that the data controller must clarify and disclose before obtaining consent and must continue to do so as long as the data controller processes personal data in accordance with that consent. These pieces of information include:

1. "a) Controller's identity, its contact details, and any other details related to the channels established by the Controller for the purpose of communicating in relation with Personal Data protection. b) Contact details of the data protection officer appointed by the Controller, where applicable. c) The legal basis and a specific, clear, and explicit purpose for collecting and Processing Personal Data. d) The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period. f) Explanation on how to withdraw consent given to process of any Personal Data. g) Explaining whether collecting or Processing Personal Data is mandatory or optional. ."[54]

The regulations also identify two cases in which the right to be informed is waived for the data subject who has given consent, and the data controller is not obligated to provide the aforementioned information:

" Paragraph (1) of this article shall not apply if the information specified in subparagraphs (a) to (g) is already available to the Data Subject, or if providing such information conflicts with any of the existing laws in the Kingdom.."[55]

Secondly, the right to access and obtain personal data: This right grants individuals whose consent has been obtained for the processing of their personal data the right to access

[53] What is the "right to be informed" under EU data protection law?. (2019). Golden Data Law. Medium. (https://medium.com/golden-data/what-is-the-right-to-be-informed-under-eu-data-protection-law-9e943e28af7b).
[54] The Executive Regulations of the Personal Data Protection Law. (2023). Previous Reference.
[55] Previous Reference.

their personal data and obtain a readable and clear copy of it, along with any other relevant information. It helps individuals understand how and why their data is being used, ensuring that it is done legally and in accordance with prior disclosures.[56]

Access to this data can be obtained in two ways: either through a documented request from the data subject to the data controller, requesting a copy of their personal data (this request may be written or oral), or by the data controller providing a clear method on its website or application that enables the data subject to directly access their personal data. Both methods are considered valid. In such cases, the data controller must provide a copy of the data " Personal Data shall be provided to the Data Subject in a commonly used electronic format and the Data Subject may request a printed hard copy if feasible."[57]
The regulations imposes a limitation on this right, stating that " Exercising the right to access Personal Data shall not adversely affect the rights of others, such as intellectual property rights or trade secrets."[58] If accessing personal data would lead to a violation of intellectual property rights of another party, this right is waived according to the regulation.

Furthermore, the regulations requires the data controller, "when enabling the data subject to access their personal data, to ensure that this does not involve the disclosure of personal data identifying another individual."[59] This provision obliges the data controller to do its utmost to protect the personal data of third parties when the data subject exercises their right to access their data. If the data subject gains access to data belonging to others, the responsibility lies with the data controller, as it is obligated to safeguard the personal data in its possession.

Thirdly, the right to rectify personal data: If the data subject, who has given consent for the processing of their data, becomes aware of any inaccuracies, they have the right to request the data controller to rectify the data. This request entails the following:

- The data subject has the right to request the data controller to cease processing their data during the correction period until the correction is completed.[60] This means that if the data controller continues processing during the correction period after the data subject has requested cessation, it constitutes a violation of the regulation, and the consent becomes unacceptable.
- The data controller is obligated to request copies of the documents and records that substantiate the data subject's claim of inaccuracy, such as national identification cards, certificates, and other relevant documents. Subsequently, the data controller must correct the data based on these documents. However, the data controller must immediately destroy these images and documents upon completion of the correction process and refrain from retaining them.[61]
- Once the data controller completes the correction, it must promptly and without delay notify all parties that have benefited from the data about the correction process to avoid the repercussions of erroneous information.[62]

Fourthly: The Right to Request the Destruction of Personal Data: This right is closely tied to the right to withdraw consent, as elucidated above. In the event that the data subject, who had previously given consent, revokes their consent, the data controller must immediately destroy the personal data of this individual if the consent is the sole legal basis

---

[56] Right of access. Information Commissioner's Office (ICO). (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-of-access/).
[57] The Executive Regulations of the Personal Data Protection Law. (2023). Previous Reference.
[58] Previous Reference.
[59] Same Reference.
[60] Same Reference.
[61] Same Reference.
[62] Same Reference.

for processing their personal data.[63] Following the destruction, the data controller must take the following steps:

a) "Take appropriate measures to notify other parties to whom the Controller has disclosed such Personal Data and request their Destruction;
b) Take the appropriate measures to notify the individuals to whom the Personal Data have been disclosed by any means and request their Destruction.
c) Destroy all copies of the Personal Data stored in the Controller's systems, including backups, in accordance with relevant regulatory requirements."[64]

7. Conclusions

Among the most significant findings that can be drawn from the research are the following:

1. Personal data held by companies holds immense value, and its utilization is maximized through various processing methods. Consequently, companies are motivated to process such data through diverse means. To regulate these processing operations, laws and regulations have been established.
2. One of the primary legal bases allowing companies to process personal data is the consent of the data subject. Laws and regulations have been enacted to govern this consent, aligning with the protection of individuals in the face of major corporations.
3. The consent issued by the data subject is subject to specific requirements for it to be valid and acceptable. Therefore, companies must have precise awareness of these requirements to avoid legal accountability.
4. Individuals need to be informed about the controls associated with consent to be aware of them and avoid falling under the exploitation of technology companies.
5. Individuals retain ongoing rights after granting their consent. Therefore, individuals must be educated about these rights to exercise them whenever desired.

The Personal Data Protection Law is still in its early stages, and technological advancements are occurring rapidly. Researchers and stakeholders must rapidly conduct research and development suitable for this field. The system and its implementing regulations still require extensive research, analysis, and discussion due to its ongoing evolution.

References

Al-Bukhari, Abu Abdullah Muhammad bin Ismail. Sahih Al-Bukhari. Edited by a group of scholars. The Sultanate Press.

Al-Nawawi, Muslim bin Al-Hajjaj Al-Qushayri. Sahih Muslim. Edited by Mohammed Fuad Abdul-Baqi. Issa Al-Babi Al-Halabi and Partners Press. Cairo.

Al-Muzaini, Abdulaziz bin Ahmed. (1444 AH). Data Localization (A Comparative Legal Study). Al-Iraqiyya University Journal. 584. Number (58/2). (https://www.iasj.net/iasj/download/5e129bb8968f0e90).

Breen, S. (2020). GDPR: Is your consent valid?. Business Information Review (BIR). (DOI: 10.1177/0266382120903254).

California Consumer Privacy Act (CAPPA). (2018). (https://cppa.ca.gov/regulations/pdf/cppa_act.pdf)

Civil Transactions System issued by Royal Decree No. M/191, dated 29/11/1444 H corresponding to 18/06/2023G. (https://www.uqn.gov.sa/details?p=23125).

Draft Executive Regulations of the PDPL. Survey Platform. National Competitiveness Center. (https://istitlaa.ncc.gov.sa/ar/Transportation/NDMO/IMPLEMENTINGPDPL/Pages/default.aspx)

Data Protection Laws and Regulations. (2023). The International Comparative Legal Guides (ICLG). (https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa).

[63] Same Reference.
[64] Previous Reference.

Executive Regulations of the PDPL. (2023). Umm Al-Qura Newspaper. Effective Date: September 7, 2023. (https://uqn.gov.sa/details?p=23595).

General Data Protection Regulation (GDPR). EU. Regulation 2016/679 of the European parliament and of the council of 27 April 2016. (https://gdpr-info.eu/).

How should we obtain, record, and manage consent?. Information Commissioner's Office (ICO). (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/how-should-we-obtain-record-and-manage-consent/#how4).

Legal Bases for Processing of Personal Data. (2022). Global Data Privacy & Security Handbook. Baker McKenzie. (https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/north-america/united-states/topics/legal-bases-for--processing-of-personal-data)

Meskenaite, G. (2022). An examination of the criteria for valid consent under the GDPR in the light of the rationale and technological neutrality. Graduate Thesis. Faculty of Law. Lund University. Page 26. (https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9096679&fileOId=9099573).

Personal Data. General Data Protection Regulation (GDPR). EU. (https://gdpr-info.eu/issues/personal-data/#:~:text=GDPR%20Personal%20Data&text=Only%20if%20a%20processing%20of,identified%20or%20identifiable%20natural%20person).

Personal Status System issued by Royal Decree No. M/73, dated 6/8/1443 H corresponding to 09/03/2022G. (https://www.uqn.gov.sa/?p=11442).

PDPL issued by Royal Decree No. (M/19), dated 1443/2/9 H corresponding to 16/09/2021G. Umm Al-Qura Newspaper. (https://uqn.gov.sa/?p=7759).

Right of access. Information Commissioner's Office (ICO). (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-of-access/).

Riyadh Dictionary of Contemporary Arabic Language. King Salman International Complex for the Arabic Language. Analysis of the term "بيانات" (Data). (https://dictionary.ksaa.gov.sa/result/%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA).

Riyadh Dictionary of Contemporary Arabic Language. King Salman International Complex for the Arabic Language. Analysis of the terms "معالجة" (Processing) and "معالجة البيانات" (Data Processing). (https://dictionary.ksaa.gov.sa/result/%D9%85%D8%B9%D8%A7%D9%84%D8%AC%D8%A9%20%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA).

Soken-Huberty, Emmaline. Is Privacy a Human Right. Human Rights Careers. (https://www.humanrightscareers.com/issues/is-privacy-a-human-right/).

Universal Declaration of Human Rights. United Nations. (https://www.un.org/ar/universal-declaration-human-rights/).

What are the rules about an ISS and consent?. Information Commissioner's Office (ICO). (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-are-the-rules-about-an-iss-and-consent/#a2).

What is the “right to be informed” under EU data protection law?. (2019). Golden Data Law. Medium.(https://medium.com/golden-data/what-is-the-right-to-be-informed-under-eu-data-protection-law-9e943e28af7b).