Consent as a Legal Basis for Processing Personal Data

Type	Practical Guidance
Document type	Practice Note
Date	20 Oct 2023
Jurisdiction	Saudi Arabia
Copyright	LexisNexis

Table of contents

Overview

Saudi Arabia Royal Decree No. M19/1443 On the Approval of the Personal Data Protection Law (Saudi Arabia Cabinet Decision No. 98/1443 Personal Data Protection Law) introduces consent as a legal basis for the processing of personal data. Controllers may rely on consent as a legal basis for the processing of personal data of data subjects. Saudi Arabia Royal Decree No. M19 /1443 (Saudi Arabia Cabinet Decision No. 98/1443) identifies the circumstances which are subject to consent and those that are not. It also stipulates that data subjects may withdraw their consent when they no longer want their personal data to be processed. Moreover, Saudi Arabia Administrative Decision No. 1516/1445 Approving the Implementing Regulation of the Personal Data Protection Law elaborates on the procedures and conditions related to obtaining and withdrawing consent for the processing of personal data in the KSA and introduces the term "explicit consent".

Definitions

- *Collection:* The obtaining of personal data by the controller in accordance with the law's provisions whether directly from its owner or their representative, legal guardian or another party.
- *Competent Authority:* The authority determined by a Cabinet decision.
- *Controller:* Any public entity, and any private natural or legal person, that specify the purpose and manner of processing personal data, whether they process the data themselves or through a data processor.
- *Credit data:* Any personal data relating to the individual's request for, or obtaining of, financing from a financing entity, whether for a personal or a family purpose, including any data relating to their ability to obtain credit, their ability to repay it or their credit history.
- *Data subject:* An individual to whom personal data relates.
- *Processing:* Any process performed on personal data by any means, whether manual or automated, including the processes of collecting, recording, archiving, indexing, arranging, formatting, storing, modifying, updating, merging, retrieving, using, disclosing, transferring, publishing, data sharing or interconnecting, blocking, erasing and destroying.
- *Disclosure:* Enabling any person, other than the controller or the data processor, as the case may be, to obtain, use or view personal data by any means and for any purpose.
- *Public entity:* Any ministry, department, public institution or public authority, or any independent public entity in the KSA, or any of its affiliated entities.

Practical Guidance

Controllers should obtain the consent of data subjects before processing their personal data if they:

- Process personal data, which means any data, whatever its source or form, that leads to recognising the individual specifically or makes it possible to identify them directly or indirectly, including the name, personal identification number, addresses, contact numbers, licence numbers, records and personal property, bank account and credit card numbers, still or moving images of the individual and other data of a personal nature.
- Process sensitive data, which means any personal data related to the individual's ethnic or tribal origin, or religious, intellectual or political belief, as well as criminal and security data, identifying biometric data, genetic data, health data, location data and data that indicates that one or both parents of the individual are unknown.
- Use personal means of communication, including postal and electronic addresses, to share promotional or awareness material.

Under article 5(1) of Saudi Arabia Royal Decree No. M19/1443 (article 5(1) of Saudi Arabia Cabinet Decision No. 98/1443), controllers may not process personal data or change the purpose of its processing without the consent of data subjects. Therefore, the first legal basis for processing personal data is consent unless another basis for processing is being used. Data subjects should be informed of the processing of their personal data, and they should have given their consent before processing is carried out.

Exceptions to obtaining consent

Under article 6 of Saudi Arabia Royal Decree No. M19/1443 (article 6 of Saudi Arabia Cabinet Decision No. 98/1443), the exceptions are:

- when the processing serves the best interest for the data subject, and it is impossible or difficult to contact them;
- when the processing is mandated by another law or is an implementation of an earlier agreement to which the data subject is a party;
- when the controller is a public entity, and the processing is necessary for security purposes or judicial requirements; or
- when the processing is necessary to achieve the legitimate interests for controllers unless this poses a risk to the rights of data subjects or conflicts with their interests, and unless such data is sensitive.

Under article 27 of Saudi Arabia Royal Decree No. M19/1443 (article 27 of Saudi Arabia Cabinet Decision No. 98/1443), controllers may also collect or process personal data for scientific, research, or statistical purposes without the consent of data subjects if:

- the personal data does not include any specific indication of the identity of the data subject;
- if any specific indication of the data subject's identity will be destroyed during processing and prior to disclosure to any other entity and the data is not sensitive data; or
- if the collection or processing of personal data for these purposes is requested by another law or an implementation of an agreement to which the data subject is a party.

According to article 7 of Saudi Arabia Royal Decree No. M19/1443 (article 7 of Saudi Arabia Cabinet Decision No. 98/1443), giving consent cannot be a condition for providing a service or benefit unless the service or benefit relates to the processing for which consent has been given. For example, it would not be possible to require individuals to consent to the use of their personal data for marketing purposes in order to use a free Wi-Fi service. However, if there were personalisation options available as part of that service which required personal data to be provided and used in order to use those services, it would be possible to request personal data and seek consent for using it.

Explicit consent

Saudi Arabia Administrative Decision No. 1516/1445 identifies a type of consent to be used as a legal bases for processing. Explicit consent is direct and given by a data subject in any form that clearly indicates the data subject's acceptance of the processing of their personal data in a manner that cannot be interpreted otherwise.

Explicit consent is also needed:

- if the processing includes sensitive data which includes any personal data related to an individual's ethnic or tribal origin, or religious, intellectual or political beliefs, criminal and security data, identifying biometric data, genetic data, health data, and data that indicates that one or both parents of the individual are unknown;
- if the processing includes credit data; or
- if decisions will be made based entirely on the automated processing of personal data.

Process for obtaining consent

According to article 11 of Saudi Arabia Administrative Decision No. 1516/1445, controllers can obtain data subjects' consent in any appropriate form. This can be written or oral consent or by using electronic means provided that:

- consent is given freely and not obtained in a misleading way;
- it is not a condition for providing a service or benefit unless the service or benefit relates to the processing, as per article 7 of Saudi Arabia Royal Decree No. M19/1443 (article 7 of Saudi Arabia Cabinet Decision No. 98/1443);
- the processing purpose has been set out in a clear and specific way, and those purposes have been explained and clarified to data subjects before or at the time consent is requested;
- consent has been obtained from a person who has full legal capacity or, where appropriate, their legal guardian;
- details of the consent have been documented in a way which will allow it to be verified in the future, the method used to obtain consent, and time consent was obtained;
- consent has been separately obtained for each processing activity if there are different processing purposes; and
- if the purpose of processing or the processing itself changes, consent must be obtained again, so if there is a new purpose for processing, controllers should not rely on the previously obtained consent and must request and obtain consent from data subjects again before that processing can be done.

Obtaining explicit consent will also have to be documented so that it can be proven in the future where it was required.

Consent of legal guardians

Under article 13 of Saudi Arabia Administrative Decision No. 1516/1445, the legal guardian of a data subject who fully or partially lacks legal capacity has the option to give consent to the processing of that data subject's personal data and, in doing so, are required to act in the best interests of the data subject and not to harm their interests. In this case, the controller is expected to first verify the validity of that person's legal guardianship. When a controller obtains consent from a legal guardian, they are also required to make sure the legal guardian's consent to the processing does not result in any harm to the interests of the personal data subject.

It should also be noted that if the data subject later becomes legally competent, for example, they are now an adult, going forward, they (instead of their legal guardian) would then have the right to consent.

Withdrawal of consent

Article 5(2) of Saudi Arabia Royal Decree No. M19/1443 (article 5(2) of Saudi Arabia Cabinet Decision No. 98/1443) states that data subjects have the right to withdraw their consent at any time.

Article 12 of Saudi Arabia Administrative Decision No. 1516/1445 states that when data subjects withdraw their consent they should inform the controller of the same through any available means which were detailed to them when they gave their consent.

Before requesting consent from the data subject, the controller must establish procedures which will allow the data subject to withdraw that consent and take the necessary steps to ensure these measures are put in place. The procedures for withdrawing consent must be similar to, or easier than those for obtaining it, so the way in which it is possible to withdraw consent cannot be more difficult than the way in which that consent was given.

When consent is withdrawn, the controller must cease processing without any undue delay after receiving the withdrawal request. It should be noted that the withdrawal of consent does not affect the lawfulness of processing which was carried out before consent was withdrawn.

When consent is withdrawn, the controller also has to take appropriate steps to notify those to whom the personal data was disclosed and request they destroy it.

In cases where there are multiple legal bases for the processing of personal data, withdrawal of consent will not affect its processing.

Control action

Controllers should design policies and procedures that determine when and how they will obtain consent from data subjects to process personal data. The initial step should be to identify the basis of processing and the type of personal data being obtained. Explicit consent will be needed when decisions are completely made on the basis of automated processing of personal data. For example, where artificial intelligence (AI) is being used for selections as part of a recruitment process. In addition, if the data being processed is sensitive data or credit data, explicit consent will also be needed.

Where consent is the legal basis for processing, it should be sought and obtained before the processing takes place. It must be obtained freely, for example, it is not possible to pressurise the data subject into giving consent by making it a condition for obtaining a service or benefit.

The data which will be used, and the processing purpose must be clearly and specifically explained in an accurate manner. It is not permitted to provide misleading information about why the data is being collected and how it is being processed.

Regardless of the way consent is obtained, even if it is obtained orally, the process and the consent itself should be documented to prove in the future that consent has been given, when necessary. Where explicit consent is required, this must be documented too. The key point here is that the consent which has been given could not be interpreted otherwise.

It is also necessary to establish if the person required to give the consent has the capacity to do so, and if consent needs to be given instead by their legal guardian. If consent is sought from a legal guardian, their status must also be confirmed before the consent is given.

Where ongoing processing of data is taking place, controllers must ensure they have procedures in place to check each time data is processed that consent has not subsequently been withdrawn or that where consent is withdrawn, the recent data has been removed from material due to be processed.

Controllers should also ensure that if there is any change to the purpose or procedures used to process personal data that consent is sought again, and this new type of processing does not take place until consent is given.

Employees should be adequately trained to identify the circumstances when consent is required, how it should be obtained and recorded, and what checks need to be put in place to ensure there is still valid consent for the specific processing currently being undertaken.

Consequences

Failure to obtain consent of data subjects would result in a breach of Saudi Arabia Royal Decree No. M19/1443 (Saudi Arabia Cabinet Decision No. 98/1443) and Saudi Arabia Administrative Decision No. 1516/1445.

According to article 35(1) of Saudi Arabia Royal Decree No. M19/1443 (article 35(1) of Saudi Arabia Cabinet Decision No. 98 /1443), whoever discloses or publishes sensitive data with the intent to harm the data subject or to achieve a personal benefit shall be punished by:

- imprisonment for no more than two years;
- a fine not exceeding three million Riyals; or
- both.

The fine may be doubled in case of recidivism even if this results in exceeding its maximum limit, provided that it does not exceed double this limit.

According to article 36(1) of Saudi Arabia Royal Decree No. M19/1443 (article 36(1) of Saudi Arabia Cabinet Decision No. 98 /1443), any natural or legal person covered by this law who violates any of the law's provisions or supporting regulations will be punished with either:

- a warning; or
- a fine not exceeding five million Riyals.

The fine may be doubled in case of a repeat offence even if this results in exceeding the normal maximum fine, provided that the fine is not more than double the maximum limit.

According to Saudi Arabia Royal Decree No. M19/1443 (Saudi Arabia Cabinet Decision No. 98/1443), data subjects may also file a complaint with the Competent Authority where there has been a violation of Saudi Arabia Royal Decree No. M19/1443 (Saudi Arabia Cabinet Decision No. 98/1443) and its regulations.

Under article 36(2) of Saudi Arabia Royal Decree No. M19/1443 (article 36(2) of Saudi Arabia Cabinet Decision No. 98/1443), relevant committees can be established to examine violations of the law and impose warnings or fines detailed in article 36(1) of Saudi Arabia Royal Decree No. M19/1443 (article 36(1) of Saudi Arabia Cabinet Decision No. 98/1443), depending on the type, seriousness, and impact of the violation. Although where such a decision is issued, there is a right to appeal it before the competent court.

Moreover, employees and workers appointed by the Head of the Competent Authority can make arrests and investigate violations of the data protection law or seek the assistance of other competent authorities in making arrests and carrying out searches under article 37 of Saudi Arabia Royal Decree No. M19/1443 (article 37 of Saudi Arabia Cabinet Decision No. 98/1443). They also have the right to seize the means or tools used to commit these violations.

In addition, the competent court is also able, by virtue of article 38(1) of Saudi Arabia Royal Decree No. M19/1443 (article 38(1) of Saudi Arabia Cabinet Decision No. 98/1443), to order the confiscation of funds obtained as a result of committing the violations of Saudi Arabia Royal Decree No. M19/1443 (Saudi Arabia Cabinet Decision No. 98/1443) and the relevant regulations, without prejudice to bona fide third-party rights.

It is also possible, under article 38(2) of Saudi Arabia Royal Decree No. M19/1443 (article 38(2) of Saudi Arabia Cabinet Decision No. 98/1443), for the competent court or committee to order the violator to publish a summary of the decision at their own expense in one or more local newspapers in their place of residence or via another appropriate means after the judgment becomes final depending on the type of the violation, its seriousness, and the extent of its consequences.

In addition, under article 40 of Saudi Arabia Royal Decree No. M19/1443 (article 40 of Saudi Arabia Cabinet Decision No. 98 /1443) those who sustain damage due to a breach of this law have the right to claim compensation before a competent court for material or moral damage based on the extent of the damage.

Related Content

Legislation

- Saudi Arabia Cabinet Decision No. 98/1443 Personal Data Protection Law
- Saudi Arabia Administrative Decision No. 1516/1445 Approving the Implementing Regulation of the Personal Data Protection Law

Authors

Saeed Hasan Khan
Director, Bizilance Legal Consultants
saeed.hasan@bizilancelegal.ae
+971 52 914 1118

Biography

Saeed Hasan Khan is taxation, privacy and corporate lawyer having more than 20 years' experience advising clients on taxation, corporate, data privacy, regulatory compliance and contractual obligations, and in representing clients before the authorities. He has developed a keen professional interest in emerging laws on personal data protection, and has gained an understanding of the underlying concepts and principles governing global data protection laws, including the EU's General Data Protection Regulation. He has carried out a great deal of research on personal data protection laws in various jurisdictions in order to compare their core legal principles. He advises clients on compliance framework regarding personal data protection. He is an advocate of the High Court, a member of the Chartered Institute of Arbitrators (UK) and a member of the International Association of Privacy Professionals. He has completed a course from the London School of Economics and Political Science on "Data: Law, Policy and Regulation".

Saifullah Khan
Director, Bizilance Legal Consultants
saifullah.khan@bizilancelegal.ae
+971 58 184 8960

Biography

Saifullah Khan is an international trade, privacy and policy lawyer with more than 20 years of diversified and multi-jurisdictional professional experience serving a large client base in the domestic and international markets. His areas of interest include trade remedy laws of the World Trade Organization, customs law, competition law and data privacy. With respect to emerging discipline of data privacy, he advises clients from different jurisdictions on data privacy compliance and cross-border transfer of data. Additionally, he assists clients in the preparation and review of privacy policies and intra-group agreements concerning cross-border transfer of personal data, etc. He is an advocate of the High Court, a member of the Chartered Institute of Arbitrators (UK) and a member of the International Association of Privacy Professionals. He has completed a course at the London School of Economics and Political Science on "Data: Law, Policy and Regulation".