Managing Personal Data Transfers from Saudi Arabia

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

Overview

The Kingdom of Saudi Arabia (KSA) has enacted 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) to safeguard personal data and data subject rights. According to Saudi Arabia Royal Decree No. M19/1443 (Saudi Arabia Cabinet Decision No. 98/1443), controllers may transfer or disclose personal data to an entity outside the KSA.

Article 29 of Saudi Arabia Royal Decree No. M19/1443 (article 29 of Saudi Arabia Cabinet Decision No. 98/1443) outlines the regulations governing the transfer of personal data from the KSA to entities outside it. Personal data transfer outside the KSA is permissible to achieve specific purpose, i.e., meeting the KSA's international obligations, serving its interests, and complying with agreements involving the data subject. Such transfers must meet certain conditions like not compromising the national security or vital interests, transferring personal data with adequate level of protection, and minimising the amount of personal data to be transferred outside the KSA.

Moreover, Saudi Arabia Administrative Decision No. 1517/1445 on the Approval of the Regulation on Personal Data Transfer Outside the Geographical Boundaries of the Kingdom further elaborates on the regulations and guidelines of the transfer of personal data outside the KSA and allows for appropriate guarantees and exceptions to protect data privacy and security.

Definitions

- *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.
- *Data subject:* An individual to whom personal data relates.
- *Personal data:* Any data, whatever is its source or form, that leads to recognising an individual specifically or makes it possible to identify them directly or indirectly, including their name, personal identification number, address, contact number, licence number, records and personal property, bank account and credit card numbers, still or moving images of the individual and other data of a personal nature.
- *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.
- *Processor:* Any public entity, and any private natural or legal person, that processes personal data for the benefit and on behalf of the controller.
- *Public entity:* Any ministry, department, public institution or public authority, or any independent public entity in the KSA, or any of its affiliated entities.
- *Transfer:* Transferring personal data from one jurisdiction to another for processing.
- *Sensitive data:* 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.
- *Vital interest:* Any interest necessary to preserve the life of a data subject.

Practical Guidance

Adequate level of protection

Article 29(2)(b) of Saudi Arabia Royal Decree No. M19/1443 (article 29(2)(b) of Saudi Arabia Cabinet Decision No. 98/1443) states that there must be an appropriate level of protection of personal data in the recipient country. This level should not be less than the level of protection established by Saudi Arabia Royal Decree No. M19/1443 (Saudi Arabia Cabinet Decision No. 98 /1443), Saudi Arabia Administrative Decision No. 1516/1445 Approving the Implementing Regulation of the Personal Data Protection Law, and Saudi Arabia Administrative Decision No. 1517/1445.

To determine the appropriate level of protection in accordance with Saudi Arabia Administrative Decision No. 1517/1445, after carrying out the prescribed assessment, the Competent Authority decides whether to issue an adequacy decision. Where an adequacy decision has been issued it means that the country (in respect for which an adequacy decision has been issued) offers protection to personal data which is equivalent to the protection provided for under Saudi Arabia Royal Decree No. M19/1443 (Saudi Arabia Cabinet Decision No. 98/1443).

The assessment on the issuance of an adequacy decision is based on:

- whether there are personal data laws in that country which preserve a data subject's rights (these should not be less than the levels guaranteed by the KSA laws and regulations);
- whether the rule of law is followed and the rights of data subjects to preserve their privacy are guaranteed;

- how effective that country is at implementing data protection laws;
- the ability of data subjects to exercise their rights; and
- whether there are means for data subjects to file complaints or claims involving personal data processing.

The assessment also considers whether there is a supervisory authority monitoring the controller's compliance with personal data protection requirements, the willingness of that authority to cooperate with the authorities in the KSA, and the clarity of regulations on the disclosure of personal data by controllers to governmental or regulatory bodies. Moreover, the assessment will include whether these regulations conflicted with the KSA law. These assessments can be carried out for specific countries, specific sectors, and international organisations.

The Competent Authority, based on its assessment, either issues an adequacy decision about that jurisdiction, recommends that an international agreement should be followed, does not issue an adequacy decision for a jurisdiction, or does not recommend that an international agreement should be followed. These assessments are reviewed every four years by the Competent Authority.

According to article 4(4) of Saudi Arabia Administrative Decision No. 1517/1445, it is possible for the Competent Authority to submit a proposal to the Prime Minister to cancel, amend, or suspend any of the decisions which has been taken on the level of protection of personal data outside the KSA if it has become clear through reviewing the level of protection of personal data that a particular country, sector, or international organisation no longer guarantees an adequate level of protection of personal data.

Saudi Arabia Royal Decree No. M19/1443 (Saudi Arabia Cabinet Decision No. 98/1443) or Saudi Arabia Administrative Decision No. 1517/1445 do not provide for any further control where transfer is based on an adequacy decision issued by the Competent Authority.

Control action

The law permits the transfer of personal data outside the KSA on the basis of appropriate level of protection, which means that the recipient jurisdiction offers protection to personal data which is, at minimum, equal to the protection provided for under KSA law and regulations. Assessment of that appropriate level of protection is not left to controllers. Instead, it is the Competent Authority, which based on an assessment, decides whether to issue an adequacy decision. Controllers may transfer personal data to those countries where the Competent Authority has issued an adequacy decision.

However, where a controller is transferring or disclosing personal data outside the KSA, the mere fact that there is an adequacy decision in place for that country does not free them from the obligations they have under Saudi Arabia Royal Decree No. M19 /1443 (Saudi Arabia Cabinet Decision No. 98/1443), Saudi Arabia Administrative Decision No. 1517/1445, and Saudi Arabia Administrative Decision No. 1516/1445. Therefore, controllers must continue to meet all of their obligations like protecting Data subject rights, guaranteeing personal data security, notifying data breaches, and carrying out impact assessments as required under the law.

Organisations should put in place policies and procedures that set the guidelines for personal data transfer or disclosure to entities outside the KSA. Controllers should also have a valid purpose for the transfer or disclosure, and the personal data transferred or sent should be kept to a minimum. They should specifically train their staff on transferring and disclosing personal data outside the KSA. They should also know and understand that there should be an adequate level of protection based on an adequacy decision, a valid purpose, and minimal personal data to be sent. These policies and procedures should be reviewed on a regular basis to make sure that they are up-to-date.

The Competent Authority in the KSA is expected to produce a list of countries deemed to offer adequate protection. Checks should be made on a regular basis to see whether there have been any changes to that list which would change a previous adequacy decision based on which transfers or disclosures have been made to a specific country. In addition, when a transfer or disclosure of personal data is planned to be made to a specific country for the first time, checks should be made to see if there is an adequacy decision in place.

Appropriate guarantees

Under article 5 of Saudi Arabia Administrative Decision No. 1517/1445, if an adequacy decision has not been issued by the Competent Authority on the country or international organisation, the data is to be transferred or disclosed provided that the regulatory requirements of that country or international organisation do not include anything that would negatively affect the data subject's privacy or the ability of the controller to adhere to the application of appropriate guarantees. Transfer or disclosure can still take place if one of the following safeguards are in place:

- Binding Common Rules – These are meant to work for intra-group transfers of personal data and to be applied amongst the group entities which are established or operating in different countries. They must be approved by the Competent Entity on the basis of application received by them in each case. Binding Common Rules apply to every relevant party in a group of entities which work in a joint economic activity, including the employees. These are to be complied by transferor, transferee, and their respective employees in relation to taking measures to protect the personal data.
- Standard Contractual Clauses – These are a set of clauses which follow a standard form issued by the Competent Authority which guarantee an adequate level of protection when transferring data outside the country.
- A Compliance Certificate has been issued – These are issued by an entity licensed by the Competent Authority. The controller or processor must also commit to applying the appropriate guarantees.

- Binding Code of Conduct – These are rules which have been approved by the Competent Authority following a request made in each case. The controller or processor must also commit to applying the appropriate guarantees.

Content of Binding Common Rules

Article 5(2) of Saudi Arabia Administrative Decision No. 1517/1445 requires any Binding Common Rules to include at least the following:

- commercial registers and contact details for the group of entities operating in the joint economic activity;
- a description of the personal data which is to be transferred, the transfer, purpose, type of processing, and recipient countries;
- a commitment by all the group entities to comply with these rules;
- a requirement to apply all the personal data protection provisions, including purpose limitation, data minimisation, retention periods, lawful basis of processing, processing controls and, requirements on subsequent transfer to parties who are not covered under the Binding Common Rules;
- data subject rights, including the right to complain, along with the means to exercise them;
- responsibility of the controller for any infringement of the Binding Common Rules;
- a method for providing information on the Binding Common Rules along with other information to data subjects;
- identification of the role of a data protection officer, if any, or any other person or entity responsible for monitoring compliance with the Binding Common Rules;
- a mechanism for handling complaints and managing data breaches;
- a mechanism for ensuring and following up on continuous and effective compliance with these rules by group members including data protection audits, methods for taking remedial action, and making the results of these audits available to the Competent Authority;
- a mechanism for approval request from the Competent Authority for any amendment to these Binding Common Rules;
- a mechanism to enable cooperation and communication with the Competent Entity by group entities;
- regulatory requirements on disclosure of personal data to group entities in other countries which may have a negative impact on the provisions in the Binding Common Rules, along with a mechanism which should be followed when there is a conflict between regulatory requirements outside the KSA and KSA law and regulations; and
- a mechanism for training group entity employees who have regular access to personal data and sensitive data, and ensuring they have the necessary qualifications.

Risk assessment

Under article 8 of Saudi Arabia Administrative Decision No. 1517/1445, where data is transferred outside the KSA, under the terms found in article 5 of Saudi Arabia Administrative Decision No. 1517/1445, controllers must conduct a risk assessment which at least covers:

- the purpose of transfer or disclosure;
- the nature of transfer or disclosure and its geographic scope;
- the appropriate means and guarantees taken and their adequacy in providing the required levels of protection to the data;
- the measures adopted to ensure the minimum amount of data needed to achieve the purpose is transferred or disclosed;
- the material and moral effect the transfer or disclosure will have, and the possibility of any potential harm to the data subject; and
- the measures which will be taken to prevent and mitigate any identified risks to personal data protection.

Exemption removal

Under article 7 of Saudi Arabia Administrative Decision No. 1517/1445, these exemptions will not apply if it is found that the transfer or disclosure process affects the KSA's national security or its vital interests, or if a risk assessment indicates the transfer or disclosure has a high risk to the data subject's privacy. They will also cease to apply if the guarantees applied by the controller no longer apply or are no longer applicable. In these cases, the transfer or disclosure of the personal data outside the KSA should cease immediately, and risks should be reassessed.

Control action

Controllers who transfer or disclose personal data outside the KSA should have a clear understanding if the relevant countries, specific sectors, or particular international organisations are subject to an adequacy decision or a relevant international treaty which provides adequate safeguards. If they are not, and the required conditions apply, the transfer or disclosure can be made as long as one of the appropriate safeguards is in place.

Where a controller is part of a group of entities operating in a joint economic activity, it may be possible for Binding Common Rules to be put in place to allow overseas transfers or disclosure. However, these must include all the necessary elements and

have been approved by the Competent Entity. They should also check where the Competent Entity has drawn up standard contractual clauses which can be included in relevant contracts or if it is possible to obtain a Compliance Certificate or comply with a Binding Code of Conduct.

Policies and procedures should be put in place to ensure all relevant employees understand and follow the relevant requirements of the option used. Ongoing compliance with the relevant guarantees and requirements should be checked. This will include compliance by processors or group employees outside the KSA. There should also be a periodical review of these policies and procedures to make sure that they are up-to-date.

Staff transferring or disclosing personal data outside the KSA should also be aware of the specific circumstances such as risks to national security or a high risk to the data subject's privacy where overseas transfers would never be allowed and must be stopped immediately if identified by risk assessments.

Exemptions

Article 6 of Saudi Arabia Administrative Decision No. 1517/1445 allows the transfer of personal data outside the KSA even when there is:

- no appropriate level of protection of personal data outside the KSA; and/or
- the controller is not able to use any of the guarantees which include the use of binding rules, standard contractual clauses, certificates of compliance or binding rules of conduct.

These limited exemptions include:

- where the transfer or disclosure is necessary to conclude or implement an agreement to which the personal data subject is a party;
- the controller is a public entity and the transfer or disclosure is necessary for the national security or in order to achieve a public interest;
- the controller is a public entity, and the transfer or disclosure is necessary to investigate or detect a crime, prosecute perpetrators of a crime, or implement a criminal penalty; or
- the transfer or disclosure is needed to protect the data subject's vital interest, and they cannot be contacted.

Vital interests are defined quite restrictively in Saudi Arabia Administrative Decision No. 1516/1445 as any interest necessary to preserve the data subject's life.

Risk assessment

Under article 8 of Saudi Arabia Administrative Decision No. 1517/1445, where data is transferred outside the KSA, under the terms found in article 6 of Saudi Arabia Administrative Decision No. 1517/1445, controllers must conduct a risk assessment which at least covers:

- the purpose of transfer or disclosure;
- the nature of transfer or disclosure and its geographic scope;
- the appropriate means and guarantees taken and their adequacy in providing the required levels of protection to the data;
- the measures adopted to ensure the minimum amount of data needed to achieve the purpose is transferred or disclosed;
- the material and moral effect the transfer or disclosure will have, and the possibility of any potential harm to the data subject; and
- the measures which will be taken to prevent and mitigate any identified risks to personal data protection.

Cessation of the exemption

Article 7 of Saudi Arabia Administrative Decision No. 1517/1445 states that the exemptions provided for in article 6 of Saudi Arabia Administrative Decision No. 1517/1445 will cease immediately if:

- it is found that the transfer or disclosure affects national security or the KSA's vital interests;
- the results of a risk assessment show this transfer or disclosure will result in a high risk to the data subject's privacy;
- the appropriate guarantees applied by the controller no longer apply; or
- the controller is no longer able to adhere to the appropriate guarantees they apply.

In any of these situations, the transfer or disclosure of the personal data outside the KSA should cease immediately, and risks should be reassessed. The competent entities are required to continuously assess and review conditions and procedures for revoking these assessments.

Control action

Controllers should identify the purpose of the transfer or disclosure of personal data outside the KSA to determine whether there is an exemption they can rely on to still transfer or disclose personal data outside the KSA even where an adequate level of protection or alternative guarantees are not available. They should put in place policies and procedures which provide

guidelines on transfer or disclosure of personal data to entities outside the KSA according to the applicable laws and regulations. Staff should be trained on how to identify a potential risk to national security, the KSA's vital interests, and situations where a data subject could be harmed by transfer or disclosure of their personal data outside the KSA. They should also be clear on the circumstances where a data subject's vital interests would be protected, and a transfer or disclosure exemption might be available. The specific risk assessment required in these circumstances should be documented and procedures put in place to ensure it takes place.

Staff should also understand that transfer and disclosure must stop immediately if high risks to data subject privacy, the KSA's national security, or vital interests are discovered, or if the controller is no longer able to adhere to the guarantees they have put in place or those guarantees no longer apply. It should also be clear to them when a data subject's vital interests might be negatively impacted and when a transfer relates to the performance of a contract with the data subject. Policies and procedures in this area should be periodically reviewed and updated where necessary.

Consequences

Failure to transfer personal data outside the KSA in accordance with the applicable laws and regulations would result in a breach of Saudi Arabia Royal Decree No. M19/1443 (Saudi Arabia Cabinet Decision No. 98/1443) and its regulations.

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 will 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 article 34 of Saudi Arabia Royal Decree No. M19/1443 (article 34 of 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 will 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 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
- Saudi Arabia Administrative Decision No. 1516/1445 Approving the Implementing Regulation of the Personal Data Protection Law
- Saudi Arabia Administrative Decision No. 1517/1445 on the Approval of the Regulation on Personal Data Transfer Outside the Geographical Boundaries of the Kingdom

Authors

Saeed Hasan Khan
Lawyer, 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
Lawyer, 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".