GDPR Compliance for Saudi Arabian Businesses

by Justin Whelan, HFW, with Practical Law Data Privacy & Cybersecurity

Status: **Law stated as of 01-Jul-2025** | Jurisdiction: **Middle East, Saudi Arabia**

This document is published by Practical Law and can be found at: **uk.practicallaw.thomsonreuters.com/w-046-6009**
Request a free trial and demonstration at: **uk.practicallaw.thomsonreuters.com/about/freetrial**

A Practice Note discussing the key differences between the KSA Personal Data Protection Law (PDPL) and the EU General Data Protection Regulation (GDPR). This Note discusses the GDPR's applicability to KSA organizations and additional measures that KSA organizations must take to comply with the GDPR.

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) explicitly requires non-EU-based organizations engaging in certain EU-related activities to comply with its requirements.

In the Kingdom of Saudi Arabia (KSA), the Personal Data Protection Law (PDPL) regulates personal data collection and processing. The PDPL is supplemented by the PDPL Implementing Regulation. This Note refers to both pieces of legislation, collectively as the KSA PDPL or the PDPL, except where otherwise stated.

The Saudi Data and Artificial Intelligence Authority (SDAIA) is responsible for enforcing the PDPL.

While the KSA PDPL is similar to the GDPR, for example, in data breach reporting timeframes and data processing principles, there are different requirements between the two regimes. For instance, the KSA PDPL predominantly imposes obligations on data controllers only, and provides for an Actual Interest basis for processing personal data (defined as any moral or material interest of the data subject that is directly linked to the purpose of processing personal data, and the processing is necessary to achieve that interest) (Article 6(1), PDPL; Article 1(5), PDPL Implementing Regulation). KSA organizations operating in the EU must review the GDPR's applicability provisions to determine whether it applies to their activities.

KSA organizations subject to the GDPR face greater data protection obligations than the KSA PDPL requires. Failing to comply with the GDPR also carries substantial penalties and may result in fines of up to EUR20 million or 4% of the organization's total worldwide annual revenue for the preceding financial year, whichever is higher (Article 83(5), GDPR).

This Note provides an overview of the KSA PDPL and the GDPR and highlights any key differences between the two laws. It also discusses the GDPR's applicability to non-EU organizations and steps that KSA organizations should take to comply with the GDPR. This Note specifically discusses:

- The GDPR's extra-territorial application.
- The requirement for non-EU-established organizations to appoint an EU representative.
- Obligations applicable to controllers and processors.
- The GDPR's accountability principle and the obligation to demonstrate compliance.
- Consent requirements.
- Data breach notification requirements.
- A comparison of data subject rights under the GDPR and the KSA PDPL.
- Cross-border data transfer restrictions.

EU General Data Protection Regulation (GDPR)

The GDPR applies to the processing of personal data by:

- Controllers and processors established in the EU (see Controllers and Processors Defined and EU Establishments).
- Certain non-EU-established controllers and processors (see Extra-Territorial Application).

The European Data Protection Board (EDPB) has also issued Guidelines on the territorial scope of the GDPR (Article 3) (EDPB 3/2018) (Nov. 12, 2019) (Territorial Scope Guidelines).

EU Establishments

A KSA controller or processor with an establishment in the EU must comply with the GDPR when processing personal data in the context of that establishment, regardless of the nationality of the data subjects or even if the organization processes the personal data outside the EU (Article 3(1), GDPR). For example, a KSA-based organization may be subject to the GDPR if it both:

- Has an EU-established subsidiary, affiliate, or branch.
- Processes personal data in the context of that establishment.

Lack of a branch or subsidiary in the EU does not preclude the non-EU entity from having an EU establishment. In some circumstances, the presence of a single employee or agent in the EU may subject the KSA controller or processor to the GDPR under Article 3(1). (Territorial Scope Guidelines, at 6.) The GDPR also applies to controllers and processors with an EU establishment that process personal data in the context of that establishment, even if data subjects are located outside the EU (Territorial Scope Guidelines, at 7 to 9).

To determine whether a non-EU organization processes personal data in the context of an EU establishment, the EDPB recommends identifying links between the non-EU organization's processing activities and the activities of the EU establishment. These links are key to determining whether the GDPR applies to the processing (Territorial Scope Guidelines, at 6 to 8).

For more on determining whether the GDPR applies based on an EU establishment, see Practice Note, Determining the Applicability of the GDPR: Applicability Based on an EU Establishment and the Territorial Scope Guidelines.

Extra-Territorial Application

The GDPR extends to controllers and processors not established in the EU when they engage in certain activities affecting EU data subjects. KSA organizations with an existing EU customer base must comply with the GDPR. Organizations without an existing customer base must comply if they target or intend to target individuals in the EU.

The GDPR applies to personal data processing conducted by a KSA controller or processor with no EU establishment that relates to:

- Offering goods or services to data subjects in the EU, regardless of whether the controller or processor requires payment.
- Monitoring EU data subjects' behavior that takes place in the EU.

(Article 3(2), GDPR.)

The Territorial Scope Guidelines recommend organizations first consider whether data subjects are located in the EU and then consider the processing relates to offering goods or services or monitoring behavior (Territorial Scope Guidelines, at 14).

However, mere accessibility of a non-EU-established controller's or processor's website by an EU data subject or access to the email address or other contact details of the non-EU-established controller or processor from the EU, does not by itself mean that the GDPR applies (Recital 23, GDPR).

Organizations may show intent to draw EU data subjects as customers by, for example:

- Referring to the EU or at least one EU member state by name when referencing the goods or services.
- Offering goods or services in an EU language or currency.
- Allowing EU data subjects to place orders in the local language.
- Offering delivery in EU member states.
- Directing marketing campaigns at an EU member state audience.
- Using country-specific top-level domains or the top-level domain ".eu."

(Territorial Scope Guidelines, at 17 to 18.)

KSA organizations that do not offer goods or services to EU data subjects may still fall within the GDPR's scope if they monitor EU data subjects' behavior that takes place in the EU. Monitoring under GDPR Article 3(2)(b) may encompass a broad range of activities, for example:

- Behavioral advertising.
- Geo-location tracking for marketing purposes.
- Data collection or tracking through wearables and other smart devices.
- Web analytics, cookies, and other online tracking.
- Online personalized diet and health analytics services.
- Closed circuit television camera use.
- Market surveys and other behavioral studies based on profiling.
- Data gathering or regular reporting on individuals' health status.

(Territorial Scope Guidelines, at 20.)

For more on determining whether the GDPR applies to organizations without an EU establishment, see Practice Note, Determining the Applicability of the GDPR: Applicability for Non-EU-Established Businesses and the Territorial Scope Guidelines.

EU Representative

KSA organizations subject to the GDPR but not established in the EU must designate an EU representative in writing, subject to limited exceptions (Article 27(1), GDPR). The EU representative is a natural or legal person established in the EU representing the controller or processor concerning their GDPR obligations (Article 4(17), GDPR). The EU representative must:

- Maintain an establishment in an EU member state where the organization's data subjects are located.
- Be empowered to address all issues relating to data processing raised by supervisory authorities and data subjects, in addition to or instead of the controller or processor.

(Article 27(3), (4), GDPR.)

The requirement to appoint an EU representative does not apply when:

- The processing:
  - is occasional;
  - excludes large-scale processing of special categories of personal data (see Personal Data and Sensitive Personal Data Defined) or criminal conviction or offense data; and
  - is unlikely to result in a risk to the rights and freedoms of data subjects, considering the nature, context, scope, and purposes of processing.
- The controller is a public authority or body.

(Article 27(2)(a), GDPR.)

For more on the EU representative's obligations under the GDPR, see Territorial Scope Guidelines, at 23 to 28. For more on the key requirements and considerations when appointing a data protection representative, see Practice Notes, Appointing a data protection representative (UK and EU) and Appointing a representative in the EEA and the UK: FAQs.

Controllers and Processors Defined

The GDPR defines and imposes obligations on:

- A controller, which means the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of processing personal data (Article 4(7), GDPR).
- A processor, which means the natural or legal person, public authority, agency, or other body that processes personal data on a controller's behalf (Article 4(8), GDPR).

The EDPB has issued Guidelines on the concepts of controller and processor in the GDPR (EDPB 07/2021) (July 7, 2021).

The KSA PDPL defines a controller as any public entity, natural person or private legal person that specifies the purpose and manner of processing personal data, whether the data is processed by that controller or by the processor (Article 1(18), PDPL).

The KSA PDPL defines a processor as any public entity, natural person or private legal person that processes personal data for the benefit and on behalf of the controller (Article 1(19), PDPL).

KSA organizations subject to the GDPR must determine whether they act as a controller or processor to understand which GDPR obligations apply (see Processor Obligations).

KSA organizations acting solely as processors must review the GDPR's applicability provisions and requirements.

Personal Data and Sensitive Personal Data Defined

The GDPR broadly defines personal data to include any information relating to an identified or identifiable natural person (data subject). Personal data includes location data and online identifiers. (Article 4(1), GDPR.) The KSA PDPL similarly broadly defines personal data as any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, addresses, contact numbers, license numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of personal nature (Article 1(4), PDPL).

The GDPR considers certain categories of personal data more sensitive and defines special categories of personal data as:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.

- Health data and data about sex life or sexual orientation.
- Genetic and biometric data.

(Article 9(1), GDPR.)

Special categories of personal data includes personal data that may indirectly reveal sensitive information concerning an individual (Case C-184/20: OT v Vyriausioji tarnybinės etikos komisija (Chief Official Ethics Commission, Lithuania); see Legal Update, Information indirectly disclosing sexual orientation is special category personal data (ECJ)).

The GDPR prohibits processing special categories of personal data unless an exception applies. The GDPR also restricts processing criminal conviction and offense data (Article 10, GDPR). For more on processing special categories of personal data, see Practice Note, Overview of EU General Data Protection Regulation: Special Categories of Personal Data and Justifications for Processing Special Categories of Personal Data.

The KSA PDPL also defines certain special categories of data, including:

- **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 (Article 1(11), PDPL).
- **Genetic Data:** Any personal data related to the hereditary or acquired characteristics of a natural person that uniquely identifies the physiological or health characteristics of that person, and derived from biological sample analysis of that person, such as DNA or any other testing that leads to generating Genetic Data (Article 1(12), PDPL).
- **Health Data:** Any personal data related to an individual's health condition, whether their physical, mental or psychological conditions, or related to health services received by that individual (Article 1(13), PDPL).
- **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 (Article 1(15), PDPL).

KSA organizations that process special categories of personal data or criminal conviction and offense data about EU data subjects must ensure that they meet the GDPR's requirements for processing this data.

Principles Governing Personal Data Processing

Similar principles govern personal data processing under the GDPR and the KSA PDPL including:

- **Lawfulness, fairness, and transparency.**
- **Purpose limitation,** which means that an organization should:
  - only collect personal data for specified, explicit, and legitimate purposes; and
  - not process the personal data in a manner that is incompatible with those purposes, except under limited circumstances.
- **Data minimization,** which means personal data should be:
  - adequate;
  - relevant; and
  - limited to what is necessary for processing.
- **Accuracy,** which means personal data must be:
  - accurate and kept up-to-date; and
  - corrected or deleted without delay when inaccurate.
- **Storage limitation,** which requires that the organization keep personal data in identifiable form only for as long as necessary to fulfill the purposes the organization collected it for, subject to limited exceptions.
- **Integrity and confidentiality,** which requires that the organization secure personal data by appropriate technical and organizational measures against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

(Article 5(1), GDPR.)

Although the KSA PDPL does not explicitly list the above data protection principles, they are embedded throughout the PDPL's provisions.

For more on processing personal data under the GDPR, see Practice Note, Overview of EU General Data Protection Regulation. For more on processing personal data under the KSA PDPL, see Country Q&A, Data Protection in Saudi Arabia: Overview.

Applicability of EU Member State Laws

The GDPR introduced a single legal framework across EU member states. However, several GDPR provisions allow EU member states to enact

national legislation specifying, restricting, or expanding the scope of certain GDPR requirements. As a result, organizations may still face inconsistent requirements from one EU member state to the next. For information on the permitted EU member state variations under the GDPR, see Practice Note, GDPR Derogations and Exemptions: Overview.

KSA organizations handling EU personal data may be subject to multiple national laws if they:

- Have multiple EU establishments.
- Are a non-EU-established organization that offers goods or services to or monitors EU data subjects' behavior that takes place in multiple EU member states.

Organizations subject to the GDPR must review the territorial scope provisions in the relevant EU member state laws to determine which laws apply. For more on how member state laws implement the GDPR, see GDPR National Implementation Legislation Toolkit.

The requirements of the national laws implementing the GDPR are outside the scope of this Note. However, KSA organizations should review and comply with the relevant laws' requirements in addition to the GDPR.

Data Privacy Governance

Organizations subject to the GDPR must assess how the requirements affect their organization and what steps the organization must take to comply, which may include auditing existing data protection practices and updating procedures and policies. Organizations should also consider ways to leverage existing practices already in place to comply with the KSA PDPL.

Some organizations that comply with the KSA PDPL for their personal data processing activities, including when processing personal data about EU data subjects, may need to adjust their practices to comply with the GDPR's standard for processing EU personal data. Some organizations may choose to adopt the GDPR's standard and apply its requirements to all its data collection and processing activities. Other organizations may adopt a regional approach and only apply the GDPR's requirements to their processing activities relating to EU personal data.

Accountability and Demonstrating Compliance

The GDPR incorporates the principle of accountability and requires a controller to both:

- Comply with the six principles when processing personal data (Article 5(1), GDPR; see Principles Governing Personal Data Processing).
- Demonstrate compliance with all six of the principles (Article 5(2), GDPR).

The GDPR also requires a controller to implement appropriate technical and organizational measures to ensure and be able to demonstrate that the processing complies with the GDPR's requirements (Article 24(1), GDPR). Meeting the GDPR's accountability requirement means doing more than just establishing data protection policies and procedures. The accountability principle effectively requires a controller to implement a formal data protection compliance program (see Practice Note, Demonstrating Compliance with the GDPR: Accountability and Demonstrating Compliance).

Although the KSA PDPL does not explicitly list data protection principles, the above principles are embedded in the PDPL's provisions.

The KSA PDPL also requires controllers to implement all the necessary organizational, administrative and technical measures to protect personal data, including during personal data transfers, consistent with the provisions and controls set out in the Implementing Regulations (Article 19, PDPL).

Organizations should audit existing compliance programs for compatibility with the GDPR and assess compliance gaps (see Implementing the General Data Protection Regulation (GDPR) Checklist: Align the Business's Personal Data Processing Practices with GDPR's Requirements).

Accountability for Processors

The accountability principle under GDPR Articles 5 and 24 expressly applies to controllers. However, in practice, the GDPR obligations imposed directly on processors or indirectly passed on by controllers also subject processors to certain accountability requirements.

The KSA PDPL also primarily imposes obligations on controllers.

However, if a processor violates a controller's instructions or the data processing agreement provisions, then the processor will be considered as a controller and held directly accountable for any PDPL violations (Article 17(4), PDPL Implementing Regulation).

For more information on accountability, see Processors and Practice Note, Demonstrating Compliance with the GDPR: Accountability for Processors.

Other Compliance Measures Required by the GDPR

The GDPR and the KSA PDPL similarly contain requirements to:

- **Appoint data protection officers (DPOs).** (Article 37, GDPR; Article 32, PDPL Implementing Regulation.) The SDAIA has issued guidance on when controllers must appoint a DPO. For more on when the GDPR requires controllers and processors to appoint a DPO and the DPO's obligations, see:
  - Practice Note, Data Protection Officers Under the GDPR;
  - Standard Document, Data protection officer: role specification (EU);
  - Implementing the General Data Protection Regulation (GDPR) Checklist: Appoint Data Protection Officer (DPO) or Other Data Protection Leader;
  - Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: EU; and
  - Article 29 Working Party: Guidelines on Data Protection Officers (DPOs) (WP243) April 5, 2018).
- **Conduct a data protection impact assessment (DPIA) for certain types of high-risk processing.** (Article 35, GDPR; Article 25, PDPL Implementing Regulation.) For more on when the GDPR requires a DPIA, see Practice Note, Data Protection Impact Assessments Under the GDPR.

For more on developing a privacy compliance program, see Practice Note, Developing a Privacy Compliance Program. For more on the GDPR's obligation to demonstrate compliance and how to comply with this obligation, see Practice Note, Demonstrating Compliance with the GDPR.

Data Protection by Design and Default

The GDPR requires controllers to implement data protection measures "by design and default" when processing personal data (Article 25(1), GDPR). This means that controllers must implement appropriate technical and organizational measures, like pseudonymization, to ensure compliance with data protection principles.

For more on this requirement under the GDPR, see Practice Note, Overview of EU General Data Protection Regulation: Data Protection by Design and by Default and Implementing the General Data Protection Regulation (GDPR) Checklist: Data Protection by Design and Default.

Although privacy by design and default is not strictly required under the KSA PDPL, it is encouraged to be embedded into all stages of the personal data processing lifecycle.

Certifications and Codes of Conduct

The GDPR explicitly recognizes codes of conduct (Article 40) and certifications (Article 42) as mechanisms to demonstrate compliance with the GDPR's requirements. Participation in a code of conduct or certification scheme is voluntary.

In KSA, the SDAIA is permitted to grant licenses to entities that:

- Issue accreditation certificates to controllers and processors.
- Conduct audits or checks of personal data processing activities related to the controller's activity.

The SDAIA is also empowered to specify the appropriate tools and mechanisms to monitor compliance of controllers and processors outside of KSA when processing personal data related to individuals residing in KSA. (Article 33, PDPL; Articles 35 and 36, PDPL Implementing Regulation.)

Before codes of conduct and certifications can provide reliable evidence of GDPR compliance, clear rules and requirements for certification must be in place. The GDPR provides for the development of these rules.

For more on codes of conduct and certification mechanisms, see Practice Note, Overview of EU General Data Protection Regulation: Codes of Conduct and Certification Mechanisms and GDPR European Data Protection Board Guidance Tracker.

Records of Processing Activities

The GDPR requires controllers and processors to maintain a record of processing activities under its responsibility (Article 30, GDPR). This requirement does not apply when the organization employs fewer than 250 people unless the processing:

- Is likely to result in a risk to the data subjects' rights and freedoms.
- Is not occasional.
- Includes special categories of personal data or criminal conviction or offense data.

The KSA PDPL similarly requires controllers to maintain records of personal data processing operations and must provide the SDAIA with access to the records upon request (Article 31,

PDPL; Article 33(4), PDPL Implementing Regulation). Controllers must retain these records for five years after any personal data processing activity ends (Article 33(1), PDPL Implementing Regulation).

Information Controllers Must Record Under the PDPL	Information Controllers and Processors Must Record Under the GDPR
The record of personal data processing activities must include, at a minimum: • The controller's name and relevant contact details. • Information about the DPO, where required in accordance with PDPL Implementing Regulation Article 32. • The data processing purposes. • A description of personal data categories being processed and data subject categories. • Where possible, the retention periods for each personal data category. • The categories of recipients to whom the personal data is disclosed. • A description of the data transfer operations outside of KSA, including the legal basis for the transfer and recipient parties. • Where possible, a description of the procedures and organizational, administrative, and technical measures in place that ensure the data's security. (Article 33(5), PDPL Implementing Regulation).	Controllers must maintain records of: • The controller's name and contact details and, where applicable, the joint controller, the controller's representative, and the data protection officer (Article 30(1)(a), GDPR). • The purpose for the personal data processing (Article 30(1)(b), GDPR). • A description of the personal data processing, including categories (Article 30(1)(c), GDPR). • The data subjects or class of data subjects whose personal data is being processed (Article 30(1)(d), GDPR). • All non-EU countries or international organizations that receive personal data and in certain instances the documentation of appropriate safeguards (Article 30(1)(e), GDPR). • The time limits for erasure of the different categories of data (Article 30(1)(f), GDPR). • A general description of the technical and organizational security measures referred to in GDPR Article 32(1) (Article 30(1)(g), GDPR). Processors must maintain a record of processing activities carried out by the controller including: • The processor's name and contact details and, where applicable, the processor's representative, each controller for which the processor acts, and the data protection officer (Article 30(2)(a), GDPR). • The categories of processing carried out on behalf of the controller (Article 30(2)(b), GDPR). • All non-EU countries or international organizations that receive personal data and in certain instances the documentation of appropriate safeguards (Article 30(2)(c), GDPR). • A general description of the technical and organizational security measures referred to in GDPR Article 32(1) (Article 30(2)(d), GDPR).

For more on what to include in the record of processing activities, see:

- Practice Note, Demonstrating Compliance with the GDPR: Record of Processing Activities.
- Practice Note, Data Mapping and GDPR Recordkeeping Obligations.
- Standard Document, Record of Processing Activities Under Article 30 (GDPR).

Conditions for Processing

The KSA PDPL and the GDPR require controllers to have a legal basis for processing and recognizes consent as one legal basis permitting processing (Article 6(1)(a), GDPR; Article 5, PDPL and see Practice Note, Consent under the GDPR). Some EU supervisory authorities have questioned the

validity of processing based on consent in certain circumstances, such as in an employer/employee relationship. Organizations should rely on another legal basis to process personal data whenever possible unless applicable law requires consent. Other legal bases under the GDPR that permit personal data processing include when processing is necessary for:

- Performing a contract with the data subject.
- Complying with a legal obligation.
- Protecting the data subject's vital interests.
- Performing a task carried out in the public interest.
- Pursuing the controller's or a third party's legitimate interests, except where the data subject's interests or fundamental rights and freedoms override the controller's interests.

(Article 6(1), GDPR; see Practice Note, Overview of EU General Data Protection Regulation: Lawful Processing.)

The KSA PDPL similarly recognizes processing without consent when processing is:

- In the data subject's actual interest, but communicating with the data subject is impossible or difficult.
- Pursuant to another law or in implementation of a previous agreement to which the data subject is a party.
- Necessary for the controller's legitimate interests, without prejudice to the data subject's rights and interests, and if no sensitive data is processed.
- Required for security purposes or to satisfy judicial requirements and the controller is a public entity.

(Article 6, PDPL.)

For more on lawful processing under the KSA PDPL, see Country Q&A, Data Protection in Saudi Arabia: Overview: Question 10.

KSA organizations subject to the GDPR should identify and document their legal basis for processing EU personal data (see Practice Note, Demonstrating Compliance with the GDPR: Record of Processing Activities).

Justifications for Processing Special Categories of Personal Data

The GDPR generally prohibits organizations from processing special categories of personal data unless an exception applies. The GDPR prohibits organizations from processing special categories of personal data unless an exception applies, including when:

- The data subject explicitly consents to the processing.
- The processing relates to personal data made public by the data subject.
- The processing relates to the legitimate interests of certain non-profit organizations.
- The processing is necessary for:
  - carrying out the controller's rights and obligations in the context of employment law, social security, and social protection;
  - protecting the vital interests of the data subject or another person and the data subject is physically or legally incapable of giving consent;
  - establishing, exercising, or defending legal claims or whenever courts are acting in their judicial capacity;
  - reasons of substantial public interest;
  - preventive or occupational medicine to assess the working capacity of an individual, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services;
  - reasons of public interest in the area of public health;
  - archiving in the public interest; or
  - scientific, historical research, or statistical purposes.

(Article 9, GDPR.)

The GDPR also limits personal data processing relating to criminal convictions and offenses to certain circumstances, including when applicable law authorizes the processing and provides for appropriate safeguards for the rights and freedoms of data subjects (Article 10, GDPR).

The KSA PDPL requires explicit data subject consent before controllers may process sensitive data and legitimate interest is not permitted as a legal basis for processing (Articles 6(4) and 10(7), PDPL; Article 16(1)(c), PDPL Implementing Regulation). Although the KSA PDPL is somewhat unclear, a controller may be able to process sensitive data without data subject consent, if it can show that it relied on one of the legal bases provided for in PDPL Article 6(1), (2), or (3).

KSA organizations must ensure they have a legal basis under the GDPR to process EU data subjects'

special categories of personal data. For more information on processing special categories of personal data see, Practice Note, Overview of EU General Data Protection Regulation: Special Categories of Personal Data.

GDPR Consent Requirements

The GDPR imposes stringent requirements on obtaining valid consent and requires consent to be:

- Freely given.
- Specific.
- Informed.
- Unambiguous.

(Article 4(11), GDPR.)

Implied consent and opt-out consent are not valid under the GDPR (Article 4(11), GDPR). A data subject's silence, inactivity, or failure to uncheck a pre-checked box does not indicate consent. The GDPR also requires that written requests for consent be:

- Clearly distinguishable from other matters. Bundled consents are not valid.
- Intelligible.
- Easily accessible.
- Written using clear and plain language.

(Article 7(2), GDPR.)

To obtain freely given consent, the controller must not condition the performance of a contract, including providing a service, on the data subject's consent for processing unrelated to or unnecessary for the contract's performance or service's provision (Article 7(4), GDPR).

Certain types of personal data processing under the GDPR require explicit consent, including when relying on consent to:

- Process special categories of personal data.
- Transfer personal data cross-border.
- Make decisions based on automated personal data processing.

(Articles 9, 22, and 49, GDPR.)

The GDPR does not define explicit consent. However, the Article 29 Working Party's Guidelines on Consent under Regulation 2016/679 (WP259) (Apr. 10, 2018) (GDPR Consent Guidelines), describe explicit consent as confirming consent in an oral or written statement.

The GDPR permits data subjects to withdraw consent at any time (Article 7(3), GDPR). For more on the GDPR's consent requirements and obtaining valid consent, see the GDPR Consent Guidelines and Practice Note, Consent under the GDPR: Using Consent to Process Personal Data in the EEA and Best Practices When Using Consent to Process Personal Data.

Satisfying the GDPR's requirements for valid consent is difficult and may often be impractical. Due to the heightened requirements for obtaining valid consent and the data subject's right to withdraw consent at any time, organizations are encouraged to rely on one of the other legal bases in GDPR Article 6 to process personal data (see Conditions for Processing).

KSA Consent Requirements

The KSA PDPL prohibits personal data processing without the data subject's consent, subject to certain exceptions. Consent is valid only if it is freely given by an individual with full legal capacity. (Article 5, PDPL.) Explicit consent is required when:

- Processing sensitive data or credit data.
- Decisions are made solely by automated processing.

(Article 11(2), PDPL Implementing Regulation.)

Where the data subject's consent is required, it must be:

- Given by a person who has full legal capacity.
- Given freely and not obtained through misleading methods and obtained in compliance with PDPL Article 7 (prohibiting controllers from requiring consent as a condition of providing a service or a benefit, unless the service or benefit is directly related to the data processing for which the consent is given).
- Documented through means allowing future verification, such as specifying time and the mean of consent.
- Separately obtained for each processing purpose.

Controllers must ensure the processing purposes are communicated in a clear and specific manner, and explained and clarified to the data subject before or at the time of requesting consent. (Article 11(1), PDPL Implementing Regulation.)

The KSA PDPL permits the data subject to withdraw their consent at any time (Article 12(1), PDPL Implementing Regulation).

Consent from Minors

The GDPR requires parental consent to process personal data about children under 16 years old for online services offered directly to children (called information society services in the GDPR. The GDPR allows the EU member states to lower the age of consent to a minimum age of 13. Controllers must use reasonable efforts to verify parental consent considering available technology. (Article 8, GDPR.)

Under the KSA PDPL, the legal guardian of a data subject who lacks full or partial legal capacity must act in their best interests by either:

- Exercising the rights granted to the data subject.
- Consenting to the processing of the data subject's personal data.

(Article 13(1), PDPL Implementing Regulation).

Obtaining the consent of the legal guardian is conditional upon taking appropriate measures to verify guardianship validity over the data subject (Article 13(2), PDPL Implementing Regulation). When obtaining consent from a data subject's legal guardian, the controller must ensure that:

- The legal guardian's consent will not cause any harm to the data subject's interests.
- The data subject is allowed to exercise their rights when they reach legal capacity.

(Article 13(3), PDPL Implementing Regulation).

KSA organizations that collect personal data from children are governed by the age of consent set by the EU member state the child resides in and must comply with the GDPR's consent requirements for minors. For more on the requirements for obtaining consent from minors, see Practice Note, Consent Under the GDPR: Child Consent and GDPR Age of Child Consent Chart (EEA): Overview.

Processors

Processor Obligations

The KSA PDPL does not address processors other than providing that a processor:

- Will be considered a controller if it violates the controller's instructions or the data processing agreement and will be held directly accountable for any PDPL violations (Article 17(4), PDPL Implementing Regulation).
- Who contracts with a sub-processor, must:
  - take sufficient guarantees to ensure that the contract does not impact the level of protection provided to the personal data being processed;
  - choose only those sub-processors that provide sufficient guarantees to comply with the KSA PDPL; and
  - obtain prior consent from the controller, and give the controller an opportunity to object.

  (Article 17(5), PDPL Implementing Regulation.)

The GDPR imposes more direct obligations and liability on processors, including requirements to:

- Process personal data only according to the controller's instructions (Article 29, GDPR).
- Maintain a record of data processing activities (Article 30(2), GDPR).
- Appoint a DPO under certain circumstances (Article 37, GDPR).
- Implement appropriate technical and organizational measures (Article 32, GDPR).
- Have written controller authorization before engaging subcontractors under GDPR Article 28(2) and pass obligations down to any processors it engages via contract (Article 28(4), GDPR).
- Notify the controller of any security breach without undue delay (Article 33(2), GDPR; see Data Breach Notification).
- Appoint an EU representative when the processor is not located in the EU, subject to certain limited exceptions (Article 27, GDPR; see EU Representative).
- Only transfer personal data internationally under GDPR Article 44, which requires the processor to have a compliant data transfer mechanism (see Cross-Border Data Transfers).
- Make all information available to the controller so that it may demonstrate compliance with its obligations under GDPR Article 28 (Article 28(3)(h), GDPR).

For more on processors' GDPR obligations and demonstrating compliance, see Practice Notes, Processor Obligations Under the GDPR and Demonstrating Compliance with the GDPR: Accountability for Processors.

Controller Obligations

Under the PDPL, a controller must:

- Select processors that provide the necessary guarantees to implement the PDPL's provisions.

- Monitor the processor's compliance with the PDPL.
- Continue to fulfill their own responsibilities towards the data subject or the SDAIA.

(Article 8, PDPL.)

The PDPL Implementing Regulation also requires the controller to ensure that any processor it selects provides sufficient guarantees to protect personal data and enters into a processor agreement that includes certain obligations (Article 17(1), PDPL Implementing Regulation). For more on controller's obligations when engaging third-party processors, see Country Q&A, Data Protection in Saudi Arabia: Overview: Question 15.

Controllers have similar obligations under the GDPR when engaging processors (Article 28, GDPR). The GDPR only permits transfers to processors when the processor provides sufficient guarantees that it has implemented appropriate technical and organizational measures to protect personal data under the GDPR (Article 28(1), GDPR).

Processor relationships under the GDPR must be governed by a contract or other legal act under applicable law that binds the processor and that specifies:

- The subject matter and duration of the processing.
- The nature and purpose of the processing.
- The type of personal data processed and the categories of data subjects.
- The obligations and rights of the controller.

(Article 28(3), GDPR.)

Contracts with processors should also include certain terms specified in GDPR Article 28(3).

KSA controllers subject to the GDPR must comply with the GDPR's obligations applicable to engaging processors. KSA organizations should audit their existing contracts to determine whether they contain the required contract terms and, if not, they should update existing contracts. For more on updating existing contracts, see Implementing the General Data Protection Regulation (GDPR) Checklist: Address Processor Requirements and Review and Update Vendor and Service Contracts.

Data Security

The KSA PDPL requires controllers to implement all the necessary organizational, administrative, and technical measures to protect personal data, including while carrying out personal data transfers, in accordance with the PDPL and controls set out in the Implementing Regulation (Article 19, PDPL).

The controller must take the necessary organizational, administrative, and technical measures to ensure personal data security and data subject privacy, and:

- Implement necessary security and technical measures to limit security risks related to personal data breach.
- Adopt all relevant controls, standards, and rules issued by the National Cybersecurity Authority, or adopt recognized best practices and cybersecurity standards if the controller is not obligated to follow the National Cybersecurity Authority's controls, standards, and rules.

(Article 23, PDPL Implementing Regulation.)

The GDPR includes a similar requirement to protect personal data and requires controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk (Article 32, GDPR). The GDPR also requires controllers to implement appropriate measures to ensure and be able to demonstrate that the processing complies with the GDPR's requirements (Article 24(1), GDPR; see Accountability and Demonstrating Compliance). This includes implementing data protection by design and default (Article 25, GDPR).

The GDPR highlights several appropriate security measures, including:

- Pseudonymization and encryption (see Practice Note, Anonymization and Pseudonymization Under the GDPR).
- Ensuring the ongoing confidentiality, integrity, availability, and resilience of data processing systems and services.
- Restoring availability and access to personal data in a timely manner if a physical or technical incident occurs.
- A process for regularly testing, assessing, and evaluating the effectiveness of the organization's technical and organizational security measures.

(Article 32(1), GDPR.)

When assessing the appropriate level of security, controllers and processors must take account of the risks presented by processing, including from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data (Article 32(2), GDPR). A controller or processor may demonstrate compliance with GDPR Article 32 using an approved:

- Code of conduct.
- Certification mechanism.

(Articles 40 and 42, GDPR; see Certifications and Codes of Conduct.)

KSA organizations must audit their security practices to ensure compliance with the GDPR. For more on complying with the GDPR's security requirements, see:

- Practice Note, Data Security Under the GDPR.
- Implementing Data Security Measures Under the GDPR Checklist.
- Implementing the General Data Protection Regulation (GDPR) Checklist: Review Personal Data Protection and Security Measures and Data Protection by Design and Default.

Data Breach Notification

If the controller becomes aware of a breach, it must notify the SDAIA within 72 hours, if the breach potentially causes harm to the personal data, the data subject, or conflicts with their rights or interests. The Implementing Regulation also sets out the information that must be included in the notification. (Article 24(1), PDPL Implementing Regulation.)

If the controller is not able to provide any of the required information within 72 hours from the time it became aware of the personal data breach, it must provide it as soon as possible, along with justifications for the delay (Article 24(2), PDPL Implementing Regulation).

The controller must notify the data subject of a personal data breach without undue delay, if the breach may cause damage to their data or conflict with their rights or interests. The PDPL Implementing Regulation sets out the information that must be included in the notification. (Article 24(5), PDPL Implementing Regulation.)

The GDPR establishes similar personal data breach notification requirements. A data breach under the GDPR means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to personal data (Article 4(12), GDPR). Controllers must notify:

- The relevant supervisory authority without undue delay and no later than 72 hours after any breach of personal data, unless the data breach is unlikely to pose a risk of harm (Article 33, GDPR).
- The data subject without undue delay if the personal data breach poses a high risk of harm, subject to certain limited exceptions (Article 34 and Recital 86, GDPR).

The GDPR requires processors to notify the controller without undue delay when it becomes aware of a data breach (Article 33(2), GDPR).

The EDPB has issued Guidelines on Personal data breach notification under the GDPR (EDPB 9/2022) (March 28, 2023) (GDPR Breach Guidelines I) and Guidelines on Examples regarding Personal Data Breach Notification (EDPB 01/2021) (December 14, 2021) (GDPR Breach Guidelines II), which each provide guidance on identifying data breaches, assessing risk of harm to data subjects, and providing notification to supervisory authorities and data subjects. GDPR Breach Guidelines II supplement GDPR Breach Guidelines I.

The GDPR only requires data subject notification when the security breach poses a high risk of harm to data subjects (Article 34(2), GDPR). The GDPR requires controllers to assess the risk of harm to data subjects. Risks to data subjects may include:

- Loss of control over personal data.
- Limitation of data subject rights.
- Discrimination.
- Identity theft or fraud.
- Financial loss.
- Damage to reputation.
- Significant economic or social disadvantage.

(GDPR Breach Guidelines I, at 9 and GDPR Breach Guidelines II, at 6 to 7.)

In certain situations, the controller is exempt from notifying data subjects (Article 34(3), GDPR; see GDPR Breach Guidelines I, at 22 and example cases in GDPR Breach Guidelines II).

The GDPR requires processors to notify the controller without undue delay when they become aware of a data breach (Article 33(2), GDPR).

KSA organizations subject to the GDPR must comply with the data breach notification requirements for EU personal data. Organizations should conduct a gap analysis to compare the organization's current incident response plan to the GDPR's requirements and develop a plan to update relevant policies and procedures applicable to EU personal data. For more on complying with the GDPR's breach notification requirements, see:

- Practice Note, Data breach notification (UK).
- Implementing the General Data Protection Regulation (GDPR) Checklist: Follow Data Breach Notification Requirements.

- GDPR Breach Guidelines I.
- GDPR Breach Guidelines II.

Data Subject Rights

The GDPR provides more rights to data subjects than the KSA PDPL. The GDPR also requires controllers to facilitate the exercise of data subject rights and imposes several obligations on controllers for responding to data subject requests (Article 12(2), GDPR).

KSA controllers subject to the GDPR must understand their obligations when handling data subject requests and take steps to implement procedures for responding to different types of requests. For more on handling data subject requests, see Handling Data Subject Requests Under the GDPR Toolkit.

This table compares data subject rights under the GDPR and the PDPL. The sections below provide additional information on each data subject right.

PDPL Data Subject Rights	GDPR Data Subject Rights
Information (Article 4(1), PDPL; Article 4, PDPL Implementing Regulation).	Similar information right but with broader content requirements (Articles 12 to 14 and Recitals 58 to 62, GDPR). To compare content requirements, see Notice.
Access (Article 4(2), PDPL; Article 5, PDPL Implementing Regulation).	Access their own personal data (Articles 12 and 15 and Recital 63, GDPR). To compare requirements, see Access and Correction.
Correct personal data (Article 4(4), PDPL; Article 7, PDPL Implementing Regulation).	Correct personal data (Article 16, GDPR). To compare requirements, see Access and Correction.
Erase personal data (Article 4(5), PDPL; Article 8, PDPL Implementing Regulation).	Erase personal data, also known as the right to be forgotten (Article 17 and Recitals 65 and 66, GDPR). To compare requirements, see Erasure (Right to Be Forgotten).
Restrict personal data processing when the data subject contests the data's accuracy (Article 7(1), PDPL Implementing Regulation).	Restriction right (Article 18, GDPR). To compare requirements, see Processing Restriction.
Right to data portability (Article 4(3), PDPL; Articles 6 and 10, PDPL Implementing Regulation).	Data portability right (Articles 20(1), (2) and Recital 68, GDPR). To compare requirements, see Data Portability.
	Additional GDPR data subject rights not found in the PDPL: • Right to object to data processing (Article 21 and Recitals 69 and 70, GDPR; see Processing Objection). • Right to object to automated decision-making (Article 22(1) and Recital 71, GDPR; see Automated Decision-Making Objection). For more on these rights, see Practice Note, Data Subject Rights Under the GDPR.

The GDPR requires controllers to notify third-party recipients of personal data about correction, erasure, and processing restriction requests and must inform the data subject about the recipients if the data subject requests this information (Article 19, GDPR). Similarly, under the PDPL, when correcting personal data, the controller must notify parties to whom the personal data has been disclosed previously without delay (Articles 7(3) and 22(2)(b), PDPL Implementing Regulation). When destroying personal data, the controller must notify:

- Other parties to whom the controller has disclosed such personal data and request destruction (Article 8(2)(a), PDPL Implementing Regulation).
- Individuals to whom the personal data has been disclosed and request destruction (Article 8(2)(b), PDPL Implementing Regulation).

Notice

The GDPR and PDPL both require organizations to provide data subjects with a privacy notice that includes specific information about an organization's data collection and processing activities (Articles 13 and 14, GDPR; Article 12, PDPL).

KSA PDPL Notice Requirements	GDPR Notice Requirements
Before a controller collects personal data from a data subject, it must make a privacy policy available to data subjects that specifies: • The purpose of collection • The personal data to be collected. • The means used for collection, processing, storage, and destruction. • Information about the data subject's rights and how to exercise such rights. (Article 12, PDPL.)	When a controller collects personal data directly from a data subject, it must first inform the data subject about: • The controller's identity and contact details and, if applicable, its EU representative's identity and contact details. • Contact details for the controller's data protection officer, if applicable. • The purposes for which the controller processes any personal data collected. • The legal basis for the processing. • Identification of the controller's legitimate interests when they serve as the legal basis for data processing. • The recipients or categories of recipients of the personal data, if any. • Whether the controller intends to transfer personal data outside of the European Economic Area (EEA) and the data transfer mechanism it uses to legalize the transfer. • How long the controller stores the personal data or the criteria it uses to determine retention periods. • Whether the data subject must provide the personal data by law, by contract, or for another reason and the consequences of not providing the personal data. • Whether the controller uses automated decision-making, including profiling, the auto-decision logic used, and the consequences of this processing for the data subject.

KSA PDPL Notice Requirements	GDPR Notice Requirements
	• The data subject's rights, including: – rights of access, rectification, erasure, restriction, objection, and data portability; – the right to withdraw consent and how to exercise that right; and – the right to make a complaint with a local supervisory authority and how to exercise that right, if applicable. (Article 13, GDPR.) When the controller obtains personal data about a data subject from a third party, the controller must also provide notice to the data subject. This notice must include the same information as the notice required when the controller collects personal data directly from a data subject. However, the controller: • Must add the following information to the notice: – the categories of personal data the controller collects; and – the source of the personal data, including whether it came from publicly accessible sources. (Article 14, GDPR.) • Does not need to notify the data subject about whether the data subject must provide the personal data by law, by contract, or for another reason or the consequences of not providing the personal data. For more on the data subject's information rights, see Practice Note, Data Subject Rights Under the GDPR: Information Right.

For a KSA PDPL privacy policy to comply with GDPR requirements, controllers should:

- Audit existing PDPL privacy policies and conduct a gap analysis to ascertain what additional information the controller must provide (see Practice Note, Complying with the GDPR's Transparency Obligation to Data Subjects).
- Revise and issue new privacy notices to EU data subjects.

For more compliance steps, see Implementing the General Data Protection Regulation (GDPR) Checklist: Review and Update Privacy Notices and Updating Privacy Notices to Comply with the GDPR Checklist.

Access and Correction

Data subjects have similar access and correction rights under both the PDPL and the GDPR.

PDPL Access and Correction Rights	GDPR Access and Correction Rights
Data subjects have the right to: • Obtain confirmation from the controller that it is processing their personal data. • Access their personal data, including requesting a copy in a readable and clear format, as long as it does not adversely affect the rights of others, such as intellectual property rights or trade secrets. • Obtain certain information about the processing. • Correct inaccurate personal data. • Complete incomplete personal data. (Articles 4, 5, 6, 7, PDPL Implementing Regulation.)	Data subjects have the right to: • Obtain confirmation from the controller that it is processing their personal data. • Access their personal data, including receiving a copy on request unless providing a copy adversely affects the rights and freedoms of others. • Obtain certain information about the processing. • Correct inaccurate personal data. • Complete incomplete personal data. (Articles 15 and 16 and Recital 63, GDPR.) For more on the access and correction rights, see Practice Note, Data Subject Rights Under the GDPR: Personal Data Access Right and Personal Data Rectification Right.

Because the PDPL and the GDPR impose similar procedural requirements for organizations when responding to data subject requests, it is likely that organizations that implement a PDPL-compliant procedure will also broadly comply with the GDPR.

For GDPR compliance steps, see Responding to Data Subject Requests Under the GDPR Checklist: Establish Steps for Responding to All Data Subject Requests, Provide Information, and Correct or Complete Personal Data.

Erasure (Right to Be Forgotten)

Under the GDPR, data subjects have the right to request the erasure of the personal data that a controller holds about them, also known as the "right to be forgotten" (Article 17 and Recital 65, GDPR). After a data subject requests erasure for one of the statutory reasons, the controller must erase it without delay unless an exception applies permitting retention.

The PDPL grants data subjects a similar right to request destruction of their personal data if the data subject:

- Requests the destruction.
- Withdraws consent, and consent is the sole legal basis for processing.

(Article 4(5), PDPL; Article 8(1)(a), (c), PDPL Implementing Regulation.)

The PDPL also requires a controller to destroy personal data under the following circumstances, even if the data subject does not proactively exercise their right:

- The personal data is no longer necessary to achieve the purpose for which it was collected.
- d) If the controller becomes aware that the personal data has been unlawfully processed.

(Article 8(1)(b), (d), PDPL Implementing Regulation.)

For more on the erasure right under the GDPR, see Practice Note, Data Subject Rights Under the GDPR: Personal Data Erasure Right ("Right to Be Forgotten").

For guidance on complying with the GDPR's erasure right, see Responding to Data Subject Requests Under the GDPR Checklist: Establish Steps for Responding to All Data Subject Requests and Erase Personal Data Unless Continued Retention is Necessary for Certain Purposes.

Processing Objection

The PDPL does not explicitly provide data subjects with a right to object to data processing, however they may withdraw consent for processing personal data at any time (Article 12(1), PDPL Implementing Regulation). The controller must also provide a mechanism that enables the data subject to stop

receiving direct marketing material whenever desired (Articles 28(3)(b) and 29(1)(b), PDPL Implementing Regulation).

The GDPR also provides data subjects with the right to object to data processing under certain circumstances, including:

- For direct marketing purposes, including profiling related to direct marketing. A controller must stop processing a data subject's personal data for direct marketing purposes when the data subject objects (Article 21(2) and (3) and Recital 70, GDPR).
- For scientific or historical research purposes or statistical purposes under GDPR Article 89(1), unless the processing is necessary for the performance of a task carried out in the public interest (Article 21(6) and Recital 69, GDPR).
- For processing, including any profiling, based on the following legal grounds:
  - necessary to perform a task in the public interest under GDPR Article 6(1)(e); or
  - necessary for the controller's or a third party's legitimate interests under GDPR Article 6(1)(f).

(Article 21(1) and Recital 69, GDPR.)

If the data subject objects to processing performed under GDPR Article 6(1)(e) or 6(1)((f), the controller must stop processing the personal data unless the controller either:

- Demonstrates a compelling legitimate ground for processing the personal data that overrides the data subject's interests.
- Needs to process the personal data to establish, exercise, or defend legal claims.

(Article 21(1), GDPR).

For more on when this right applies, see Practice Note, Data Subject Rights Under the GDPR: Data Processing Objection Right.

For guidance on handling processing objections under the GDPR, see Responding to Data Subject Requests under the GDPR Checklist: Establish Steps for Responding to All Data Subject Requests and Stop Processing Personal Data.

Processing Restriction

The PDPL permits a data subject to temporarily restrict the controller from processing their personal data when the accuracy of the data is contested, allowing the controller time to verify accuracy (Article 7(1), PDPL Implementing Regulation).

The GDPR grants data subjects the right to restrict the processing of their personal data under certain circumstances (Article 18, GDPR). For more on when this right applies, see Practice Note, Data Subject Rights under the GDPR: Data Processing Restriction Right.

For guidance on handling processing restriction requests, see Responding to Data Subject Requests Under the GDPR Checklist: Establish Steps for Responding to All Data Subject Requests and Review and Honor Processing Restriction Requests.

Data Portability

The PDPL provides data subjects with a right to obtain their personal data in a clear and readable format, provided exercising this right does not adversely affect the rights of others (Article 4(3), PDPL; Article 6(1), PDPL Implementing Regulation). The personal data must be provided in a commonly used electronic format and the data subject may request a printed hard copy if feasible (Article 6(2), PDPL Implementing Regulation).

When seeking to fulfill a data subject's request to obtain their personal data, controllers must ensure they comply with PDPL Article 15, which prohibits a controller from disclosing personal data except in the following situations:

- The data subject consents to the disclosure in accordance with the PDPL's provisions.
- Personal data has been collected from a publicly available source.
- The entity requesting disclosure is a public entity, and the collection or processing is required for public interest or security purposes, or to implement another law, or to fulfill judicial requirements.
- The disclosure is necessary to protect public health, public safety, or to protect the lives or health of specific individuals.
- The disclosure will only involve subsequent processing in a form that makes it impossible to directly or indirectly identify the data subject.
- The disclosure is necessary to achieve the legitimate interests of the controller, without prejudice to the rights and interests of the data subject, and provided that no sensitive data is to be processed.

The GDPR also provides data subjects with a right to data portability. The data portability right grants individuals the right to:

Receive a copy of certain personal data from the controller in a commonly used and machine-readable format and store it for further personal use on a private device.

Transmit certain personal data to another controller.

Have certain personal data transmitted directly from one controller to another where technically possible.

(Article 20(1), (2) and Recital 68, GDPR.)

For more on when this right applies, see Practice Note, Data Subject Rights Under the GDPR: Data Portability Right.

For steps on handling data portability requests, see Responding to Data Subject Requests Under the GDPR Checklist: Establish Steps for Responding to All Data Subject Requests and Determine Whether the Data Portability Right Applies.

Automated Decision-Making Objection

Under the GDPR, data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which has legal or other significant effects on the data subject (Article 22(1) and Recital 71, GDPR).

This right does not apply when the automated decision is:

Necessary for entering into or performing a contract with the data subject.

Authorized by EU or member state law applicable to the controller if the law requires suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests.

Based on explicit data subject consent.

(Article 22(2), GDPR.)

When using automated decision-making that is necessary for entering into or performing a contract with the data subject or based on data subject consent, the controller must:

Implement suitable measures to protect the data subject's rights.

Allow the data subject to obtain human intervention for any automated decisions.

Allow the data subject to express an opinion and contest any automated decisions.

(Article 22(3), GDPR.)

The controller must not use special categories of personal data in automated decision-making except under certain limited circumstances (Article 22(4), GDPR).

The PDPL does not provide data subjects with an express right not to be subject to decisions based solely on automated processing, however the data subject's explicit consent is required before those decisions can be made (Article 11(2)(c), PDPL Implementing Regulation).

For more on using automated data processing under the GDPR and compliance steps for handling data subject objections, see:

- Practice Note, Data Subject Rights Under the GDPR: Automated Decision-Making Obligations.
- Practice Note, Profiling and Automated Decision-Making Under the GDPR.
- Responding to Data Subject Requests Under the GDPR Checklist: Establish Steps for Responding to All Data Subject Requests and Limit the Use of Solely Automated Decision-Making.

Cross-Border Data Transfers

The PDPL and the GDPR both prohibit the cross-border transfer of personal data unless an exception applies or the organization satisfies certain conditions. Some PDPL exceptions permitting cross-border transfers are similar to exceptions found under the GDPR.

GDPR Requirements

Controllers and processors transferring personal data outside of the EU must comply with certain requirements for data transfers established in GDPR Chapter V (Transfer of Personal Data to Third Countries or International Organisations). The GDPR provides several data transfer mechanisms for legally transferring personal data outside of the EU, including:

- An adequacy determination by the European Commission (Article 45, GDPR). As of the date of this Note, the EU Commission has not granted KSA an adequacy decision.
- Certifications and codes of conduct (see Certifications and Codes of Conduct).
- Where the controller or processor provides appropriate safeguards, if data subjects can enforce their legal rights and have effective legal remedies (Article 46, GDPR). Controllers and processors can provide appropriate safeguards without supervisory authority approval by using:

  - a legally binding and enforceable instrument between public authorities or bodies;
  - binding corporate rules (BCRs) (Article 47, GDPR; see Practice Note, BCR under the UK GDPR (UK));
  - standard data protection clauses adopted by the European Commission; or
  - standard data protection clauses adopted by a supervisory authority and approved by the European Commission.

  (Article 46(2), GDPR.)

- Appropriate safeguards with approval from the supervisory authority, by using:
  - Standard contractual clauses (SCCs) between the controller or processor and the controller, processor, or recipient in the non-EU country; or
  - provisions inserted into administrative arrangements between public authorities or bodies that include enforceable data subject rights.

  (Article 46(3), GDPR.)

- Absent an adequacy decision or appropriate safeguards, when:
  - the data subject explicitly consents. Valid consent under the GDPR is difficult to obtain, and organizations should generally rely on another data transfer mechanism (see GDPR Consent Requirements);
  - the transfer is necessary for performing a contract;
  - the transfer is necessary for important reasons of public interest;
  - the transfer is necessary to establish, exercise, or defend legal claims;
  - the transfer is necessary to protecting the data subject's vital interests and the data subject is incapable of giving consent; or
  - the transfer is necessary, under limited circumstances, to pursue the legitimate interests of the controller and the data subject's interests or rights and freedoms do not override those legitimate interests.

  (Article 49(1), GDPR.)

For more information on cross-border data transfer mechanisms under the GDPR, see:

- Practice Note, Overview of EU General Data Protection Regulation: Cross-border data transfers
- Practice Note, Controller Binding Corporate Rules (BCR) Under the GDPR (EU).
- GDPR Cross-Border Transfers Checklist.

PDPL and the Transfer Regulation Requirements

Controllers may transfer personal data outside of KSA or disclose it to a party outside KSA if the transfer:

- Relates to performing an obligation under an agreement to which KSA is a party.
- Serves the interests of KSA.
- Is carried out:
  - for the performance of an obligation to which the data subject is a party; or
  - to fulfill other purposes as set out in the KSA Transfer Regulations.

(Article 29(1), PDPL.)

Additionally, for a transfer or disclosure to be valid, the following conditions must be met:

- The transfer or disclosure must not cause any prejudice to national security or the vital interests of KSA.
- The recipient country provides an adequate level of protection for the personal data, as determined by the SDAIA.
- The transfer or disclosure is limited to the minimum amount of personal data needed.

(Article 29(2), PDPL.)

These conditions do not apply to cases of extreme necessity to preserve the life or vital interests of the data subject or to prevent, examine or treat disease (Article 29(3), PDPL).

The KSA Transfer Regulation adds additional circumstances where, subject to the controller's prior risk assessment, cross-border transfers are permitted, including when the transfer is carried out to:

- Perform necessary operations for central processing to enable the controller to conduct its activities.
- Provide a service or benefit to the data subject.
- Conduct scientific research and studies.

(Article 29(1)(D), Transfer Regulation.)

In these circumstances, the controller is exempt from compliance with the adequate level of protection and minimum limitations but must:

- Ensure appropriate contractual safeguards if the transfer or disclosure is:
  - between public bodies to implement an agreement to which KSA is a party, or serves KSA interests (Article 4(2)(A), Transfer Regulation);
  - to provide a service or benefit directly to the data subject in a manner that does not violate their expectations or conflict with their interests, and if the transfer or disclosure is to a party that has received an approval certificate from a body licensed by the SDIAI, provided no sensitive data is transferred (Article 4(2)(D), Transfer Regulation); and
  - necessary for conducting scientific research and studies and limited to the minimum amount of data required. The controller must either comply with SCCS or ensure that the transfer or disclosure is made to a body that has received an approval certificate from an entity licensed by the SDAIA, provided no sensitive data is transferred (Article 4(2)(E), Transfer Regulation).
- Comply with SCCs if the transfer or disclosure is non-recurring or for a limited period and involves a limited number of data subjects, unless it is made to a body that has received an approval certificate from an entity licensed by the SDAIA and the data is not Sensitive Data (Article 4(2)(B), Transfer Regulation).
- Comply with BCRs or SCCs if the transfer or disclosure is necessary to perform central operations and the controller is part of a group of multinational entities, unless the personal data recipient obtains a certificate of approval issued by a body licensed by the SDAIA (Article 4(2)(C), Transfer Regulation).

Organizations complying with the PDPL still need to take additional steps when transferring personal data outside of the EU to comply with the GDPR. For compliance steps, see Implementing the General Data Protection Regulation (GDPR) Checklist: Review Cross-Border Transfer Mechanisms.

GDPR and PDPL Statutory References

Subject Matter	GDPR Article	PDPL Article
Extra-territorial application of the GDPR (see Extra-Territorial Application)	Article 3	Article 2
EU representative (see EU Representative).	Article 27	N/A
Controller defined (see Controllers and Processors Defined)	Article 4(7)	Article 1(18)
Processor defined (see Controllers and Processors Defined)	Article 4(8)	Article 1(19)
Personal data defined (see Personal Data and Sensitive Personal Data Defined)	Article 4(1)	Article 1(4)
Special categories of personal data (sensitive data) defined (see Personal Data and Sensitive Personal Data Defined)	Article 9	Article 1(11), 1(12), 1(13), and 1(15)
Data processing principles (see Principles Governing Personal Data Processing)	Article 5	N/A but embedded throughout
Data protection officers (see Other Compliance Measures Required by the GDPR)	Article 37	Implementing Regulation Article 32
Data protection by design and by default (see Data Protection by Design and Default)	Article 25	N/A but strongly encouraged

Subject Matter	GDPR Article	PDPL Article
Data protection impact assessments (see Other Compliance Measures Required by the GDPR)	Article 35	Article 22 and Implementing Regulation Article 25
Certification and codes of conduct (see Certifications and Codes of Conduct)	Articles 40 and 42	Implementing Regulation Articles 34 and 35
Record of processing activities (see Records of Processing Activities)	Article 30	Implementing Regulation Article 33
Consent (see Conditions for Processing)	Articles 4(11) and 7(2)	Articles 5, 6, 7, and 10 PDPL and Implementing Regulation Articles 11 and 12
Consent from minors (see Consent from Minors)	Article 8	Article 5 and Implementing Regulation Article 13
Processor obligations (see Processor Obligations)	Articles 27, 28, 29, 30, 32, 33, 37, and 44	Implementing Regulation Article 17
Controller obligations when engaging processors (see Controller Obligations)	Article 28	Implementing Regulation Article 17
Data security (see Data Security)	Articles 25 and 32	Article 19 and Implementing Regulation Article 23
Data breach notification (see Data Breach Notification)	Articles 33 and 34	Implementing Regulation Article 24
Data subject rights (see Data Subject Rights)	Articles 12 to 22 and 34	Article 4 and Implementing Regulation Articles 3, 4, 5, 6, 7, and 8
Data subject information right (see Notice)	Articles 12 to 14	Article 4(1) and Implementing Regulation Article 4
Data subject access right (see Access and Correction)	Articles 12 and 15	Article 4(2) and 4(3) and Implementing Regulation Articles 5 and 6
Data subject correction right (see Access and Correction)	Article 16	Article 4(4) and Implementing Regulation Article 7
Data subject erasure right (see Erasure (Right to Be Forgotten))	Article 17	Article 4(5) and Implementing Regulation Article 8

Subject Matter	GDPR Article	PDPL Article
Data subject processing objection right (see Processing Objection)	Article 21	N/A but right to withdraw consent at Implementing Regulation Article 12
Data subject processing restriction right (see Processing Restriction)	Article 18	Implementing Regulation Article 7(1)
Data subject data portability right (see Data Portability)	Article 20	Article 15 and Implementing Regulation Articles 6(2) and 10
Data subject automated decision-making and automated data processing rights (see Automated Decision-Making Objection)	Article 22	Implementing Regulation Article 11(2)(c)
Cross-border data transfers (see Cross-Border Data Transfers)	Articles 44 to 50	Article 29 and Transfer Regulation