الغزاوي ومشاركوه

AlGhazzawi & Partners

PERSONAL DATA PROTECTION LAW

In the era of digital transformation, Saudi Arabia leads with internet coverage over 73% and smartphone penetration exceeding 80%. With concerns arising, the Personal Data Protection Law aims to safeguard privacy rights among technological advancements

Introduction

Did you know that Saudi Arabia is at the forefront of digital transformation, a trend now essential across various sectors globally?.....With internet coverage exceeding 73% and smartphone penetration surpassing 80%. The Kingdom's heavy reliance on digital technologies prompts individuals to frequently provide personal data for identity verification. However, concerns about the legality of data collection and retention have spurred the enactment of the Personal Data Protection Law. This legislation, tailored to address such concerns, aims to safeguard individuals' privacy rights, especially concerning the accumulation of CVs and resumes by companies for future recruitment endeavors. Despite its widespread adoption, the legality of this practice under the Personal Data Protection Law remains an important area for examination in Saudi Arabia.

The Law was established under Royal Decree No. (M/19) dated 09/01/1443H (16/09/2021G), and subsequently amended by Royal Decree No. (M/148) dated 05/09/2023G. It officially came into effect on 21/09/2023, mandating all companies involved in processing personal data to adhere to its provisions. This article aims to clarify the Law's applicability, its scope, and the obligations it imposes on entities.

Boundaries of the Law

The applicability of the Personal Data Protection Law is precisely defined in Paragraph 1 of Article 2, which states:

"The Law applies to any Processing of Personal Data related to individuals that takes place in the Kingdom by any means, including the Processing of Personal Data related to individuals residing in the Kingdom by any means from any party outside the Kingdom."

While this law aligns with global trends in personal information protection, its focus on Saudi Arabia ensures compliance with the jurisdictional requirements of the country's laws. Consequently, the law exclusively pertains to individuals residing in Saudi Arabia, encompassing data processing activities conducted both within and outside the Kingdom, provided the data processed pertains to individuals residing in Saudi Arabia.

Defining Terms

• The Law defines **Personal Data** as any data, regardless of its source or form, that may lead to identifying an individual specifically or indirectly. This includes but is not limited to, names, personal identification numbers, addresses, contact numbers, license numbers, records, personal assets, bank and credit card numbers, photos, videos, and any other data of a personal nature.

• It is crucial to differentiate between **Personal Data** and **Sensitive Data**, with the latter holding greater significance due to its sensitive nature. The law explicitly prohibits the processing of Sensitive Data for advertising purposes. Examples of Sensitive Data, as defined by the law, include information such as racial or ethnic origin, religious, intellectual, or political beliefs, criminal convictions, biometric or genetic data for identification purposes, health data, and information indicating unknown parental lineage. Any individual who discloses or publishes Sensitive Data with the intent to harm or gain personal benefit is subject to punishment under the law. Such actions may result in imprisonment for a maximum period of two years, a fine not exceeding three million Riyals, or both.

• Additionally, the term "**Processing**" requires clarification within this context. It encompasses any operation performed on Personal Data, whether manual or automated. This includes activities such as collecting, recording, saving, indexing, organizing, formatting, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing, and destroying data. Understanding the scope of Processing is essential for ensuring compliance with data protection regulations.

Individuals' Rights

The Law grants individuals' certain rights to protect their Personal Data. These rights include:

1 - Being informed of the collection and processing of their data.
2 - Accessing their collected data.
3 - Obtaining their data in a readable format.
4 - Correcting or updating their data.
5 - Requesting the deletion of their data when no longer necessary for its initial purpose.

Prohibited Acts

Data Controllers must adhere to several restrictions outlined in the Law to avoid violating its provisions inadvertently. These restrictions include:

1 - limitations on collecting data only directly from individuals.
2 - Not disclosing Personal Data.
3 - Refraining from using personal communication means for advertising purposes.
4 - Refraining from copying identifiable official documents.

Exceptions

The Law provides exceptions to its general provisions, outlined in both the law itself and its implementing regulations. These exceptions include personal or family use, instances where communication with the individual is impossible or difficult, processing in implementation of a previous agreement, and disclosing data collected from publicly available sources.

Case Study: Legality of Collecting CVs

To assess the legality of collecting CVs from candidates, specific criteria must be evaluated, including:

1 - The candidate's residency.
2 - The nature of the data.
3 - Its acquisition method.
4 - Intended use.
5 - The candidate's rights regarding their data.

This evaluation process ensures compliance with legal standards and safeguards individuals' rights.

legal Complaint

Finally, as an individual whose personal information may be compromised, you have the right to recourse by filing a complaint with the Saudi Authority for Data and Artificial Intelligence within ninety days from the date of the incident or upon becoming aware of the violation.

The competent authority maintains a register specifically designated for recording such complaints. Your complaint should include the following details:

1 - The location and time of the data breach.
2 - Your name, identification details, address, and contact number.
3 - Information regarding the party against whom the complaint is lodged.
4 - A clear and detailed description of the violation along with supporting evidence and relevant information.
5 - Any additional requirements specified by the Saudi Authority for Data and Artificial Intelligence.

By adhering to these guidelines, you can effectively assert your rights and contribute to the protection of personal data within the Kingdom.

This article provides an overview of the Personal Data Protection Law in Saudi Arabia, emphasizing the importance of compliance with its provisions to protect individuals' privacy rights and ensure responsible data processing practices by entities operating within the country.

AlGhazzawi & Partners

Written by
Othman Al Tuwajri
Associate
AlGhazzawi & Partners

Reviewed by
Haval Kittani
Senior Associate
AlGhazzawi & Partners