Data Protection Policy

Last updated: February 2022

Galadari Advocates & Legal Consultants, along with its subsidiaries, branches and associates (hereinafter, "**Galadari**", "**the Firm**", "**we**", "**us**", "**our**"), recognize the immense value of protection of personal data. In accordance with such recognition, Galadari's Data Protection Policy (hereinafter, '**the Policy'**) represents our commitment to treat personal information of employees, customers, stakeholders and other interested parties with utmost care and confidentiality.

This Policy is implemented in compliance with the DIFC Law No. 05 of 2020 for Data Protection and Regulation and the UAE Federal Decree Law No. 45 of 2021 regarding the Protection of Personal Data (PDPD Law) and the UAE Federal Decree Law Lo. 44 of 2021 Creation of the UAE Data Office established the Data Protection Office. For the purposes of applicable data protection law, Galadari Advocates & Legal Consultants will be designated as a "data controller" since data submitted to us will be controlled by the Firm. We may, however, at times, assume the role of "processor" depending on the need of the case.

The primary objective of the Policy is to increase user awareness and avoid accidental data loss scenarios, and to ensure that the Firm is compliant with the local and DIFC laws. In keeping with that, it outlines our plan of action for prevention of a data breach. Via this Policy, we intend to encompass the role of the Firm and the responsibilities of lawyers, general staff, and the Firm with respect to access and use of that Personal Information. We endeavor to collect, gather, store, and handle personal data fairly, transparently being respectful of an individual's privacy rights.

While we do not anticipate that the institution of such Policy will be able to eliminate all malicious/negligent data handling, nonetheless, we expect this Policy would serve to be a strong deterrent towards any mal handling of data.

1. **Definitions**:

   For the purposes of this Policy, the following terms shall be construed as provided herein:

a. *Personal Data* – Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected can lead to the identification of a particular person, also constitute personal data. i.e., a username or surname, a home address, email ID, educational details, digital footprints, photographs, social security numbers, financial data etc.

All rights reserved

b. *Processing Data* – Processing data includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available**,** alignment or combination, restriction, erasure, or destruction of personal data.

c.

Sensitive Data – Sensitive data can be described as high-risk information that must be protected against unauthorized disclosure such as PII (Personally identifiable information), PHI (Protected health information), Biometric Data, Social Security Number, Bank Details, trade secrets, employee information and customer information, intellectual property data, Industry-specific data, education records, confidential information etc.

d. *Data Breach* – If any data that has been recorded for processing, has been unauthorizedly used by any third party or transferred to any third party

e. *Medical Data* - Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about that person's health status. It is also classified under “High Risk Data”.

f. *Personal Data Breach*- a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

g. *Data Retention Policy*- A data retention policy, or records retention policy, is an organization's established protocol for retaining information for operational or regulatory compliance needs.

h. *Third Party*- Any person authorised to Process Personal Data, other than the: (a) the Data Subject; (b) the Controller; (c) Joint Controller; (d) the Processor; or (e) Sub-processor.

i. *Data Controller*

j. *Data processor*

2. Scope of the Policy:

This data security Policy applies to all parties including but not limited to employees, job candidates, customers, clients, suppliers, vendors etc. who provide personal data to the Galadari Advocates & Legal Consultants, irrespective of the nature or amount of data disclosed to the Firm.

This Policy applies to all data including corporate data or personal data. It would, hence, apply to every server, database and IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks including any handsets from the Firm. Every user who interacts with company’s IT services is also subject to this Policy. Information that is classified as ‘Public’ is not subject to this Policy. Other data can be excluded from the Policy by company management based on specific business needs.

All rights reserved

The ambit of this Policy extends the employees of the Firm. It will also apply to all lawyers, contractors, consultants, partners, and any other external entity who are not directly under the direct employment contract with the Firm but have been responsible for collecting personal data on behalf of the Firm form individuals. Generally, our Policy will be applicable to anyone we collaborate with or acts on our behalf and may need access to personal or sensitive data.

3. Purpose of collection of data:

The purpose of the Policy extends to the purpose for collection of data and the methods adopted to ensure an ethical and legal processing of the same. In keeping with this, the Firm will ask for data for provision of legal services, communication of relevant material and headway in issues, management of business relationships with clients, compliance with legal obligations like audits, keeping your employment information up to date and for any ancillary to any of the above or any other purposes for which your personal data was provided to us.

4. **Policy Elements:**

As part of our day-to-day operations, we need to obtain and process information. As a mandate of this Policy, our company aims to collect this information in a transparent way and only with the full cooperation and knowledge and consent of interested parties. Once this information is available to us, the following rules apply.

This section outlines the appropriate technical and organizational security measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, unauthorized access, and other unlawful or unauthorized forms of Processing, in accordance with applicable law.

1.1 Collection of Personal Data

Any personal data collected shall be done after the approval and consent of the stakeholders and the individual will be informed of the employees/ individuals who may access the surrendered information. The Firm will undertake reasonable steps to ensure that the individual whose information is deduced has consented to such processing. The individual will also be informed of the consequences of the failure to disclose such information to the Firm to ensure an informed consent has been made.

Forms of Collecting such Personal Data/Information:

A) The Firm may collect data directly from individuals.
B) During the course of Firm's business relationship.
C) Information collected from Firm's website. i.e., cookies, saved preference etc.
D) When you register to use any of Firm's services. i.e., records made by interactions.

All rights reserved

E) Firm may also receive Personal Data about you from third parties i.e., Law enforcement agencies.

1.2 Collection of Sensitive Data

Sensitive Data is highly confidential and is collected transparently and lawfully. Such data may be processed in the Firm's ordinary course of business, such as processing personal sensitive data is necessary for the establishment, exercise, or defense of legal rights. Prior Express Consent will be obtained before processing any such Personal Sensitive Data.

2. Purpose for Processing

Purpose of processing Personal Data is broadly for the following purposes of operating our business, providing our legal services to our clients, business communications, compliance to applicable laws and managing our IT services and website. The Firm is well-regulated and has a legitimate interest in using information gained from clients where it is necessary or appropriate to provide legal advice.

3. Data Protection Officer

DPOs assists in monitoring internal compliance, observe data protection obligations and provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Data Protection Regulatory Authorities. The Firm has a data protection officer whose job is to oversee our data protection compliance. She can be contacted via her email ID: raka@galadarilaw.com

4. Sharing of Personal Data with Third Parties

We may disclose received Personal Data to other Galadari entities, for legitimate business purposes, in accordance with applicable law and subject to applicable professional and regulatory requirements regarding confidentiality and professional secrecy. In addition, we may disclose your Personal Data to

A) Accountants, Auditors, Lawyers and other outside professional advisors to Galadari Advocates and Legal Consultants;
B) Any relevant party for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security;
C) In the course of providing our legal services, we may require the assistance of various external providers of professional services and of support services, i.e., such as word processing, translation, document review, and photocopying). The use of these services might involve the service provider receiving your relevant information from us;
D) Legal and regulatory authorities, upon request, or for the purposes of reporting any actual or suspected breach of applicable law or regulation.

All rights reserved

5. Cross border transfer of information:

In the course of working of the Firm, we may require an inter-country transmission of the personal data for the facilitation of the Firm's business. This may require sharing such information to other professionals in different territories. This will entail a transfer of personal information from within the Dubai to recipients outside.

The level of personal information protection in the various jurisdictions in which the Firm operate varies, and in some instances may not provide an adequate level of protection from an international perspective. To address this, the Firm have procedures and safeguards in place to ensure the protection of personal information. These procedures include contractual obligations to ensure that all such entities safeguard your personal information and use it only for the purposes that the Firm have specified and communicated to you. When we transfer your information to other countries, we will use, share and safeguard that information as described in this Privacy Notice.

6. Data Retention

1. The Firm does not keep your personal information indefinitely. In the course of carrying out various business activities, we collect information from a wide range of sources and generate a substantial volume of data that is retained as physical paper and/or electronic records. We have incorporated appropriate systems and processes in place for the preservation and timely disposal of documents and records in line with business requirements and relevant legislation. In keeping with this, personal data will be erased either on request of the client under circumstances or every five years.

7. Information Security

We have implemented security policies, rules, and technical measures to protect the personal data that we have under our control from unauthorized access, improper use and disclosure, unauthorized destruction, or accidental loss. We also have procedures in place to deal with any suspected data breach. We will notify you and any applicable regulator or authority of a suspected data security breach where we are legally required to do so.

8. Changes to Privacy Policy

Galadari Advocates and Legal Consultants reserves the right to modify or amend the Privacy Policy at any time and for any reason. Please check back to this Privacy Policy from time to time to stay informed. It is your obligation to regularly check the Privacy Policy.

All rights reserved