

Your Personal Consultancy Private Limited

PRIVACY AND PERSONAL DATA PROTECTION POLICY

Document Type	Corporate Policy
Version	1.0
Effective Date	
Approved By	Board of Directors / Management
Prepared For	Your Personal Consultancy Private Limited

This document sets out the principles governing the collection, use, disclosure, storage and protection of personal data handled by the Company.

Rohit
Kaul

Digitally signed by Rohit Kaul
Date: 2020.03.12
17:11:54 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

1. Introduction

1.1 Background

YOUR PERSONAL CONSULTANCY PRIVATE LIMITED (hereinafter referred to as the "Company", "we", "our" or "us") is a company incorporated under the provisions of the Companies Act, 2013 and is engaged in the business of providing professional immigration consultancy, visa consultancy, documentation assistance, application management, compliance support, administrative assistance and other allied consultancy services relating to immigration, work permits, residence permits, permanent residence applications, citizenship applications and other cross-border mobility matters. The very nature of the Company's business necessitates the collection, receipt, access, examination, verification, processing, storage, transmission and retention of substantial volumes of Personal Data and confidential information belonging to Clients, prospective Clients, authorised representatives, employees, consultants, business associates, vendors and other individuals interacting with the Company. Such information frequently includes official identity documents, immigration records, financial records, educational qualifications, employment history, travel records, government-issued documents and other highly confidential information entrusted to the Company solely for the purpose of providing professional Consultancy Services. The Company recognises that every document, record and item of Personal Data entrusted to it represents an integral part of an individual's identity, legal status, financial affairs, professional background or personal circumstances and that any unauthorised access, misuse, alteration, disclosure or loss of such information may result in significant legal, financial, commercial and personal consequences. Accordingly, the Company regards the protection of Personal Data not merely as a statutory obligation but as a fundamental element of professional responsibility, ethical business conduct and sound corporate governance.

1.2 Need for this Policy

The Company acknowledges that rapid technological advancements, increasing digitalisation of commercial activities, widespread use of electronic communications, cloud-based storage systems, online client management platforms and cross-border exchange of information have fundamentally transformed the manner in which Personal Data is collected, processed, transmitted, stored and protected. At the same time, immigration consultancy services require constant interaction with Government Authorities, Embassies, Consulates, Visa Application Centres, educational institutions, employers, medical examination centres, translation agencies, courier service providers, document verification agencies and numerous other entities situated both within and outside India. Consequently, the Company necessarily processes substantial quantities of Personal Data for the purpose of assessing eligibility, preparing documentation, reviewing applications, facilitating statutory filings, complying with governmental requirements and providing professional advisory and administrative assistance to its Clients. In view of the nature, volume and sensitivity of the Personal Data processed by the Company, it has become imperative to establish a comprehensive legal and operational framework governing every stage of the lifecycle of such information. This Policy has therefore been formulated to prescribe uniform standards, principles, procedures and safeguards governing the lawful collection, receipt, recording, organisation, classification, storage, retrieval, consultation, analysis, verification, use, modification, disclosure, transmission,

retention, archival, anonymisation and destruction of Personal Data processed by the Company while ensuring transparency, accountability and compliance with Applicable Law.

1.3 Company's Commitment to Privacy

The Company is firmly committed to respecting and protecting the privacy of every individual whose Personal Data is collected, received or otherwise processed by the Company. The Company recognises that privacy constitutes an essential component of professional integrity, client confidence and responsible corporate governance and accordingly undertakes to process Personal Data only in a lawful, fair, transparent and accountable manner. The Company shall endeavour to ensure that Personal Data is collected only for legitimate, specific and lawful purposes, processed only to the extent reasonably necessary for such purposes, retained only for so long as is required by Applicable Law or legitimate business necessity, and protected through appropriate technical, organisational, contractual and administrative safeguards designed to prevent unauthorised access, disclosure, misuse, alteration, destruction or accidental loss. The Company further undertakes to cultivate a culture of confidentiality within its organisation and expects every director, officer, employee, consultant, intern, authorised representative, contractor, service provider and other person acting on behalf of the Company to observe the highest standards of confidentiality and to comply strictly with the principles and obligations contained in this Policy.

1.4 Purpose and Objectives of this Policy

The primary purpose of this Privacy & Personal Data Protection Policy is to establish a comprehensive legal and operational framework governing the manner in which Personal Data is collected, received, recorded, organised, classified, stored, retrieved, consulted, analysed, verified, processed, adapted, modified, disclosed, transmitted, transferred, retained, archived, anonymised and securely destroyed by the Company during the course of providing its Consultancy Services. This Policy is intended to promote transparency regarding the Company's data processing practices, inform individuals of the categories of Personal Data collected by the Company, explain the lawful purposes for which such Personal Data is processed, describe the legal basis upon which such processing is undertaken, specify the circumstances in which Personal Data may be disclosed to Government Authorities, Embassies, Consulates, Visa Application Centres, professional advisers, service providers and other authorised recipients, establish the technical and organisational safeguards implemented by the Company for protecting Personal Data against unauthorised access or misuse, prescribe procedures governing the retention and secure disposal of Personal Data, inform Data Principals of the rights available to them under Applicable Law, strengthen internal governance and accountability mechanisms relating to privacy protection, facilitate compliance with statutory and regulatory obligations and reinforce the Company's commitment to maintaining the highest standards of confidentiality, professionalism, integrity and responsible data management.

1.5 Regulatory Philosophy

The Company recognises that responsible processing of Personal Data extends far beyond mere compliance with statutory requirements and forms an essential component of ethical corporate conduct, responsible business administration and long-term client confidence. The Company therefore adopts a privacy-centric approach to its operations and endeavours to ensure that

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:17:25 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

every activity involving Personal Data is undertaken responsibly, proportionately, transparently and in accordance with recognised principles of fairness, accountability, purpose limitation, data minimisation, accuracy, storage limitation, confidentiality and security. The Company shall periodically review its internal policies, operational procedures, technological safeguards, contractual documentation and organisational practices with a view to strengthening its privacy framework, addressing evolving legal and technological developments, mitigating cybersecurity risks and continuously improving its standards of data governance and information security.

1.6 Nature of Personal Data Processed by the Company

Having regard to the nature of the Consultancy Services provided by the Company, the Personal Data processed by the Company may include, amongst other things, identity documents, passports, visas, immigration history, travel records, Aadhaar, Permanent Account Number (PAN), driving licences, photographs, signatures, educational certificates, professional qualifications, curriculum vitae, employment records, salary records, financial statements, bank account details, taxation records, police clearance certificates, medical examination reports where required under Applicable Law, marital status, family information, details relating to dependants, biometric appointment information, correspondence with Government Authorities, embassy communications, electronic communications, contractual records, invoices, payment records, declarations, affidavits, application forms and every other category of information voluntarily submitted by the Client or lawfully obtained by the Company for the purpose of providing Consultancy Services or complying with Applicable Law. The Company recognises that a substantial portion of the foregoing information constitutes highly confidential Personal Data requiring enhanced standards of security, confidentiality and restricted access and accordingly undertakes to implement reasonable measures designed to safeguard such information throughout the period during which it remains under the Company's control or possession.

1.7 Legal and Regulatory Framework

This Policy has been formulated having due regard to the provisions of the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, the rules, regulations, notifications, guidelines and directions issued thereunder, together with all other Applicable Laws governing privacy, confidentiality, cybersecurity, electronic records and information security. The Company shall interpret, administer and implement this Policy in a manner consistent with Applicable Law and shall endeavour to modify or update the provisions of this Policy whenever considered necessary to reflect changes in legislation, judicial pronouncements, governmental policies, technological developments, industry practices or the operational requirements of the Company. In the event that any provision of this Policy is found to be inconsistent with any mandatory requirement of Applicable Law, the relevant statutory provision shall prevail to the extent of such inconsistency without affecting the validity or enforceability of the remaining provisions of this Policy.

1.8 Relationship with Other Corporate Documents

This Policy forms an integral part of the Company's overall contractual, compliance and governance framework and shall be read harmoniously with the General Terms and Conditions of Service, Service Agreements, Engagement Letters, Refund Policy, Authorisation Letters,

Consent Forms, declarations, applications, internal compliance policies, information security policies, document retention policies and every other agreement or document executed, accepted or incorporated into the contractual relationship between the Company and the Client. Nothing contained in this Policy shall be construed as limiting, excluding or derogating from any confidentiality obligation, statutory duty or contractual commitment assumed by either Party under any other agreement unless expressly provided otherwise.

1.9 Acceptance of this Policy

Every individual who engages the Company, seeks Consultancy Services, executes any agreement, signs any declaration or consent, submits any application, provides any document or Personal Data, communicates with the Company through electronic or physical means, accesses the Company's website (*ypconsultancy.com*) or client portal, makes payment for the Services or otherwise voluntarily furnishes Personal Data to the Company shall be deemed to have read, understood and accepted the terms of this Policy. Such acceptance shall constitute an acknowledgement that the individual understands the manner in which the Company may collect, receive, use, process, store, disclose, transfer, retain and otherwise handle Personal Data in accordance with this Policy and Applicable Law, subject always to the rights, protections and safeguards available under Applicable Law.

2. TITLE, COMMENCEMENT AND APPLICABILITY

2.1 Short Title

This document shall be known as the "Privacy & Personal Data Protection Policy of YOUR PERSONAL CONSULTANCY PRIVATE LIMITED" (hereinafter referred to as the "Policy"). This Policy sets out the principles, standards, procedures, safeguards and governance framework adopted by the Company for the lawful collection, receipt, recording, organisation, storage, use, processing, disclosure, transfer, retention and protection of Personal Data processed by the Company in connection with the Consultancy Services provided by it and all activities incidental or ancillary thereto.

2.2 Effective Date

This Policy shall come into force with effect from the date approved by the Board of Directors or such other date as may be notified by the Company and shall remain in force unless amended, replaced or withdrawn by the Company in accordance with Applicable Law. Every amendment, modification or revision made to this Policy shall become effective from the date specified therein unless otherwise expressly provided.

2.3 Applicability

This Policy shall apply to every instance of collection, receipt, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, transmission, sharing, cross-border transfer, archival, retention, anonymisation, erasure and destruction of Personal Data undertaken by or on behalf of the Company in the course of carrying on its business. This Policy shall govern the processing of Personal Data irrespective of whether such processing is undertaken manually, electronically, digitally, through automated means, cloud-based platforms, physical records, document management systems, communication platforms or any other lawful medium. The provisions of this Policy shall apply to every department, division, branch office, employee, consultant, authorised representative, contractor, subcontractor and

**Rohit
Kaul**
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:18:30

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

third-party service provider acting on behalf of the Company to the extent they collect, access, process or otherwise handle Personal Data in connection with the Company's business operations.

2.4 Persons to whom this Policy Applies

third-party service provider acting on behalf of the Company to the extent they collect, access, process or otherwise handle Personal Data in connection with the Company's business operations.

2.4 Persons to whom this Policy Applies

This Policy shall apply to every natural person whose Personal Data is collected, received or otherwise processed by the Company, including but not limited to existing Clients, prospective Clients, Candidates seeking immigration or visa consultancy services, authorised representatives, employees, directors, consultants, interns, contractual personnel, vendors, service providers, business associates, visitors to the Company's offices, users of the Company's website, users of the Company's electronic communication platforms and every other individual who voluntarily provides Personal Data to the Company or whose Personal Data is otherwise lawfully received by the Company in connection with the provision of Consultancy Services or the conduct of its business.

Nothing contained in this Policy shall be construed as creating any contractual relationship between the Company and any person solely by reason of the applicability of this Policy unless such relationship otherwise exists under Applicable Law or under a separate written agreement.

2.5 Territorial Scope

This Policy shall apply to the processing of Personal Data undertaken by the Company within the territory of India as well as, where applicable, to the processing of Personal Data relating to individuals situated outside India in connection with the provision of Consultancy Services by the Company, subject always to Applicable Law. The Company acknowledges that immigration consultancy services frequently involve the exchange of information with Government Authorities, Embassies, Consulates, Visa Application Centres, educational institutions, employers and other authorised organisations located in foreign jurisdictions. Accordingly, Personal Data may, where necessary for the provision of the Consultancy Services or compliance with Applicable Law, be transmitted, disclosed or otherwise processed across international borders in accordance with this Policy and Applicable Law.

Where the laws of any foreign jurisdiction impose mandatory obligations relating to the processing of Personal Data, the Company shall endeavour, to the extent reasonably practicable and legally permissible, to comply with such obligations insofar as they are applicable to the particular processing activity.

2.6 Processing Activities Covered

Without limiting the generality of the foregoing provisions, this Policy shall apply to every activity undertaken by or on behalf of the Company involving Personal Data, including the collection, receipt, recording, classification, indexing, organisation, verification, review, consultation, analysis, adaptation, modification, updating, storage, retrieval, compilation, use, disclosure, sharing, transmission, dissemination, cross-border transfer, archival, retention, anonymisation, masking, restriction of processing, secure deletion and destruction of Personal Data, together with every other activity constituting "processing" under Applicable Law.

The Company shall endeavour to ensure that each stage of the processing lifecycle is carried out in accordance with the principles of lawfulness, fairness, transparency, proportionality,

**Rohit
Kaul**
Digitally
signed by
Rohit Kaul
Date:
2026.07.17
17:18:48
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

accountability, confidentiality and information security as recognised under this Policy and Applicable Law.

2.7 Relationship with Other Corporate Documents

This Policy shall be read together with and forms an integral part of the Company's General Terms and Conditions of Service, Service Agreements, Engagement Letters, Client Declarations, Consent Forms, Refund Policy, Authorisation Letters, internal information security policies, document retention policies and every other contractual or corporate document governing the relationship between the Company and its Clients or regulating the Company's business operations. In the event of any inconsistency between this Policy and any separately executed written agreement between the Company and a Client, the provisions of such written agreement shall prevail to the extent of the inconsistency, unless such interpretation would be contrary to Applicable Law.

2.8 Compliance with Applicable Law

Nothing contained in this Policy shall be interpreted as limiting, excluding or otherwise affecting any obligation imposed upon the Company under the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000 or any other Applicable Law governing privacy, confidentiality, electronic records, cybersecurity or information security. Where any provision of this Policy becomes inconsistent with any mandatory statutory requirement, the relevant statutory provision shall prevail to the extent of such inconsistency, and the remaining provisions of this Policy shall continue to remain valid and enforceable.

3. DEFINITIONS

3.1 Incorporation of Definitions

Unless the context otherwise requires, all capitalised words and expressions used but not specifically defined in this Policy shall have the meanings respectively assigned to them in the General Terms and Conditions of Service of the Company, as amended, supplemented or replaced from time to time. The definitions contained in the General Terms and Conditions are hereby incorporated into this Policy by reference and shall apply to this Policy with the same force and effect as if they were expressly reproduced herein. In the event of any inconsistency between a definition contained in this Policy and a definition contained in the General Terms and Conditions, the definition specifically contained in this Policy shall prevail solely for the purposes of this Policy and only to the extent of such inconsistency.

3.2 Additional Definitions

For the purposes of this Policy, unless the context otherwise requires, the following words and expressions shall have the meanings assigned to them below:

3.2.1 "Anonymisation" means the irreversible process of transforming Personal Data in such a manner that the identity of the Data Principal cannot reasonably be identified, directly or indirectly, by the Company or by any other person, whether through available technology or by reference to any other information.

3.2.2 "Applicable Data Protection Laws" means the Digital Personal Data Protection Act, 2023, the rules, regulations, notifications, guidelines, directions and circulars issued thereunder, together with every other applicable law governing the collection, processing,

storage, disclosure, transfer, retention, protection and security of Personal Data, whether presently in force or enacted in substitution thereof.

3.2.3 "Consent" means a free, specific, informed, unconditional and unambiguous indication of the wishes of the Data Principal whereby the Data Principal signifies agreement, by a clear affirmative action, to the processing of his or her Personal Data for one or more specified lawful purposes in accordance with Applicable Data Protection Laws.

3.2.4 "Consent Manager" means any person or entity duly registered or recognised under Applicable Data Protection Laws to enable a Data Principal to give, manage, review or withdraw consent for the processing of Personal Data through an accessible, transparent and interoperable platform.

3.2.5 "Cross-Border Transfer" means any disclosure, transmission, sharing, access, storage or other transfer of Personal Data by the Company from India to any foreign country or territory or to any person located outside India for the purpose of providing Consultancy Services, complying with Applicable Law or fulfilling any lawful contractual obligation.

3.2.6 "Data Fiduciary" means the Company, being the person who alone or in conjunction with others determines the purpose and means of processing Personal Data in connection with the Consultancy Services and its business operations.

3.2.7 "Data Principal" means the individual to whom the Personal Data relates and shall include, where applicable, the lawful guardian of a child or of a person with a disability acting on behalf of such individual in accordance with Applicable Law.

3.2.8 "Data Processor" means any natural or legal person who processes Personal Data on behalf of the Company pursuant to a lawful arrangement, including but not limited to information technology service providers, cloud service providers, document management service providers, software vendors, consultants, professional advisers and other authorised service providers engaged by the Company.

3.2.9 "Digital Personal Data" means Personal Data in digital form or Personal Data that is digitised after being collected in physical form and includes information stored, processed, transmitted or otherwise handled through electronic systems, cloud platforms, databases, document management systems, communication platforms or any other digital medium.

3.2.10 "Erasure" means the deletion, destruction, anonymisation or permanent removal of Personal Data from the Company's records or systems in such manner that the Personal Data can no longer be retrieved, reconstructed or associated with the Data Principal, except where retention is required under Applicable Law or for the establishment, exercise or defence of legal rights.

3.2.11 "Grievance Officer" means the officer designated by the Company for receiving, acknowledging, examining and resolving complaints, grievances, requests and other communications relating to the processing of Personal Data and for performing such functions as may be prescribed under Applicable Data Protection Laws.

3.2.12 "Notice" means any communication issued by the Company to a Data Principal explaining the categories of Personal Data proposed to be collected, the purposes for which

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:19:24 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

such Personal Data will be processed, the rights available to the Data Principal and such other information as may be required under Applicable Law.

3.2.13 "Personal Data" means any data about an individual who is identifiable by or in relation to such data and includes any information, whether in physical or digital form, relating to the identity, contact details, nationality, immigration status, passport particulars, visa history, educational qualifications, employment records, financial information, tax records, travel history, family particulars, photographs, declarations, electronic communications and every other category of information relating to an identifiable natural person processed by the Company in connection with its Consultancy Services.

3.2.14 "Personal Data Breach" means any unauthorised or accidental acquisition, access, disclosure, alteration, destruction, loss, misuse, transmission or compromise of Personal Data that affects the confidentiality, integrity or availability of such Personal Data, irrespective of whether such incident arises from technological failure, human error, cyberattack, system malfunction or any other cause.

3.2.15 "Processing" means any operation or set of operations performed upon Personal Data, whether by automated means or otherwise, including collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, sharing, alignment, combination, restriction, archival, retention, anonymisation, erasure or destruction.

3.2.16 "Recipient" means any natural or legal person, Government Authority, Embassy, Consulate, Visa Application Centre, educational institution, employer, professional adviser, service provider or any other person to whom Personal Data is lawfully disclosed by the Company pursuant to this Policy, the Agreement or Applicable Law.

3.2.17 "Security Safeguards" means the technical, organisational, contractual, administrative and physical measures implemented by the Company for protecting Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access, misuse or any other form of unlawful processing.

3.2.18 "Third-Party Service Provider" means any external individual, organisation or professional engaged by the Company for assisting in the provision of Consultancy Services or supporting the Company's business operations, including cloud service providers, information technology vendors, software providers, translators, notaries, courier agencies, document verification agencies, payment gateway providers, cybersecurity service providers and professional consultants.

3.2.19 "Verification" means the process undertaken by the Company to confirm, to the extent reasonably practicable, the identity of a Data Principal, the authenticity of documents, the correctness of information supplied or the authority of any person acting on behalf of another individual.

3.2.20 "Website" means the official website, client portal, mobile application or any other digital platform owned, operated or controlled by the Company through which the Company provides information, facilitates communication, delivers services or collects Personal Data.

4. INTERPRETATION

Rohit
Kaul

Digitally
signed by
Rohit Kaul
Date:
2026.07.17
17:19:47
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

4.1 Interpretation

Unless the context otherwise requires:

4.1.1 the headings, titles and sub-headings contained in this Policy are inserted solely for convenience of reference and shall not affect the interpretation, construction or meaning of any provision contained herein;

4.1.2 words importing the singular shall include the plural and vice versa, and words importing one gender shall include every gender;

4.1.3 references to an "individual", "person", "Data Principal", "Client" or any similar expression shall include, where the context so permits, his or her lawful guardian, authorised representative, legal heir, executor, administrator, successor and permitted assigns;

4.1.4 references to the "Company" shall include its holding company, subsidiary companies, affiliate companies, successors, permitted assigns, directors, officers, employees, consultants, authorised representatives and every person lawfully acting on its behalf to the extent consistent with the context;

4.1.5 references to any statute, legislation, rule, regulation, notification, guideline, circular, governmental direction or judicial pronouncement shall include every amendment, modification, substitution, re-enactment or successor thereto for the time being in force;

4.1.6 references to "Applicable Law" shall include every law, regulation, governmental direction, judicial order and regulatory requirement applicable to the processing of Personal Data by the Company in India and, where applicable, in any foreign jurisdiction in connection with the Consultancy Services provided by the Company;

4.1.7 the words "include", "includes", "including", "such as", "for example" and similar expressions shall be construed as being illustrative only and shall be deemed to mean "including, without limitation";

4.1.8 references to clauses, sub-clauses, schedules, annexures or appendices shall, unless expressly stated otherwise, be construed as references to the corresponding clauses, sub-clauses, schedules, annexures or appendices of this Policy;

4.1.9 where any obligation, representation, warranty, undertaking or responsibility is imposed upon two or more persons jointly, such obligation shall, unless the context otherwise requires, be construed as joint and several;

4.1.10 references to "writing" or "written" shall include physical documents, electronic records, electronic communications, emails, scanned copies, digital documents, electronic signatures, communications through secure client portals and every other mode of communication capable of being retained and reproduced for future reference;

4.1.11 every reference to the collection, receipt, recording, organisation, storage, use, processing, disclosure, transfer, retention, archival, deletion, destruction or any other activity relating to Personal Data shall be interpreted broadly so as to include every activity constituting "processing" under Applicable Data Protection Laws;

4.1.12 references to "Personal Data" shall include Personal Data existing in physical form, electronic form, digital records, scanned documents, cloud-based storage systems, emails, messaging applications, databases, document management systems, audio recordings, video recordings, photographs and every other medium capable of storing or transmitting information;

4.1.13 where Personal Data is processed by or through any Third-Party Service Provider, cloud service provider, software platform, payment gateway, document management system, professional adviser or other authorised intermediary acting on behalf of the Company, such processing shall, unless the context otherwise requires, be deemed to constitute processing by the Company for the purposes of this Policy, subject to Applicable Law and the contractual arrangements governing such engagement;

4.1.14 any reference to obtaining, collecting or receiving Personal Data shall include Personal Data voluntarily provided by the Data Principal, lawfully received from an authorised representative, employer, educational institution, Government Authority, Embassy, Consulate, Visa Application Centre or any other lawful source, as well as Personal Data generated during the course of providing the Consultancy Services;

4.1.15 any reference to the disclosure or transfer of Personal Data shall be construed as referring only to disclosures or transfers undertaken for lawful purposes, in accordance with Applicable Law, contractual obligations, valid consent where required, or any lawful direction issued by a competent Government Authority;

4.1.16 if any provision of this Policy is declared invalid, illegal or unenforceable by any court of competent jurisdiction, tribunal or regulatory authority, such invalidity, illegality or unenforceability shall not affect the validity or enforceability of the remaining provisions of this Policy, all of which shall continue in full force and effect to the fullest extent permitted by Applicable Law;

4.1.17 in the event of any inconsistency between this Policy and any mandatory provision of Applicable Law governing the protection or processing of Personal Data, the relevant provision of Applicable Law shall prevail to the extent of such inconsistency, and this Policy shall be construed, to the maximum extent possible, in a manner consistent with such Applicable Law; and

4.1.18 this Policy shall be interpreted in a manner that promotes lawful, fair, transparent, secure and accountable processing of Personal Data, while protecting the legitimate rights and interests of Data Principals and enabling the Company to provide its Consultancy Services efficiently, effectively and in compliance with Applicable Law.

5. PRIVACY PRINCIPLES

5.1 General Principles

The Company shall collect, receive, access, record, organise, classify, store, retrieve, consult, use, process, disclose, transmit, transfer, retain, archive and otherwise handle Personal Data only in accordance with the principles set out in this Clause. These principles shall govern every stage of the lifecycle of Personal Data processed by or on behalf of the Company and shall apply to every director, officer, employee, consultant, intern, authorised representative,

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2025.07.17
17:20:36
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

contractor, Third-Party Service Provider and every other person acting on behalf of the Company.

5.2 Principle of Lawfulness

The Company shall process Personal Data only for lawful purposes and in accordance with Applicable Law. The Company shall not knowingly collect, use or disclose Personal Data in a manner that is prohibited by law or inconsistent with the legitimate purposes for which such Personal Data was collected. Every processing activity undertaken by the Company shall have a lawful basis recognised under Applicable Law or shall otherwise be authorised by the Data Principal, a valid contractual arrangement, a statutory obligation or any other lawful authority.

5.3 Principle of Fairness

The Company shall endeavour to process Personal Data fairly, honestly and responsibly while maintaining due regard to the legitimate rights, interests and reasonable expectations of the Data Principal. The Company shall not knowingly adopt deceptive, misleading, coercive or unlawful practices while collecting or processing Personal Data and shall ensure that its processing activities remain proportionate to the nature and purpose of the Consultancy Services being provided.

5.4 Principle of Transparency

The Company shall endeavour to maintain transparency regarding its processing activities by informing Data Principals, through this Policy, contractual documentation, notices, consent forms or other lawful means, of the categories of Personal Data collected, the purposes for which such Personal Data is processed, the circumstances in which such information may be disclosed, the rights available to the Data Principal and such other information as may reasonably be required under Applicable Law. The Company shall make reasonable efforts to ensure that such information is communicated in a clear, accessible and understandable manner.

5.5 Principle of Purpose Limitation

The Company shall collect and process Personal Data solely for specified, lawful and legitimate purposes connected with the provision of Consultancy Services, compliance with Applicable Law, fulfilment of contractual obligations, maintenance of internal business operations, prevention of fraud, protection of legal rights, resolution of disputes and such other lawful purposes as may be communicated to the Data Principal or otherwise permitted under Applicable Law. The Company shall not knowingly process Personal Data for purposes that are incompatible with the purposes for which such Personal Data was originally collected, unless otherwise authorised by Applicable Law or by the Data Principal.

5.6 Principle of Data Minimisation

The Company shall endeavour to collect and process only such Personal Data as is reasonably necessary, relevant and proportionate for achieving the specific purposes for which such Personal Data is required. The Company shall not intentionally require the submission of excessive, unnecessary or irrelevant information where the legitimate purpose can reasonably be achieved through the collection of a lesser amount of Personal Data. However, where Government Authorities, Embassies, Consulates, Visa Application Centres or Applicable Law

require additional documentation or information, the Company may request such information from the Client to the extent reasonably necessary for providing the Consultancy Services.

5.7 Principle of Accuracy

The Company shall take reasonable steps to ensure that the Personal Data processed by it remains accurate, complete and, where necessary, updated having regard to the purposes for which such Personal Data is processed. The Company shall ordinarily rely upon the information and documents furnished by the Client or the Data Principal and shall not be under any obligation to independently investigate or verify the correctness, authenticity or completeness of such information unless expressly agreed otherwise in writing or required under Applicable Law. The Data Principal shall remain responsible for promptly informing the Company of any material change affecting the accuracy or completeness of the Personal Data previously supplied.

5.8 Principle of Storage Limitation

The Company shall retain Personal Data only for so long as is reasonably necessary for the purposes for which such Personal Data was collected, for complying with Applicable Law, fulfilling contractual obligations, establishing, exercising or defending legal rights, complying with regulatory requirements, maintaining internal records or such other lawful purposes as may justify continued retention. Upon expiry of the applicable retention period, the Company shall, subject to Applicable Law and its internal record retention policies, securely delete, anonymise or otherwise dispose of the Personal Data in an appropriate manner.

5.9 Principle of Integrity and Confidentiality

The Company shall implement and maintain reasonable technical, organisational, contractual, physical and administrative safeguards designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised access, unauthorised disclosure, misuse or any other unlawful processing. Access to Personal Data shall be restricted to those persons who have a legitimate business requirement or lawful authority to access such information in connection with the provision of the Consultancy Services or the performance of their official duties.

5.10 Principle of Accountability

The Company acknowledges that the responsibility for ensuring compliance with Applicable Data Protection Laws rests with the Company and accordingly undertakes to establish appropriate internal policies, procedures, governance mechanisms, contractual safeguards, employee awareness measures, information security controls and compliance practices designed to promote responsible processing of Personal Data. The Company shall endeavour to periodically review and update its privacy practices in light of changes in Applicable Law, technological developments, operational requirements, cybersecurity risks and recognised industry standards.

5.11 Principle of Security by Design

The Company shall, to the extent reasonably practicable having regard to the nature, scope and complexity of its operations, endeavour to incorporate privacy and information security considerations into the design, implementation and operation of its business processes,

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:21:24
+05'30'

document management systems, information technology infrastructure, communication platforms and administrative procedures so as to minimise privacy risks and strengthen the protection of Personal Data throughout its lifecycle.

5.12 Principle of Good Faith and Professional Responsibility

The Company shall process Personal Data in good faith and solely for legitimate professional purposes connected with the Consultancy Services. Nothing contained in this Policy shall be construed as authorising the Company to exploit, commercially trade, unlawfully disclose or otherwise misuse Personal Data entrusted to it by any Client or Data Principal. Every person acting on behalf of the Company shall be expected to uphold the highest standards of professionalism, confidentiality and ethical conduct while handling Personal Data.

6. CATEGORIES OF PERSONAL DATA COLLECTED

6.1 General

In the ordinary course of providing Consultancy Services, the Company may collect, receive, obtain, verify, generate, access, record, organise, store, use and otherwise process various categories of Personal Data relating to Clients, prospective Clients, authorised representatives, employees, consultants, vendors, business associates and other individuals interacting with the Company. The categories of Personal Data collected by the Company shall depend upon the nature of the Consultancy Services requested, the immigration programme involved, the requirements prescribed by the relevant Government Authority, Embassy, Consulate or Visa Application Centre, Applicable Law, contractual obligations and the information voluntarily furnished by the Data Principal or otherwise lawfully obtained by the Company.

Without limiting the generality of the foregoing, the Company may collect and process one or more of the following categories of Personal Data.

6.2 Identity and Personal Particulars

The Company may collect Personal Data relating to the identity of the Data Principal, including the full name, previous names, date of birth, age, gender, nationality, place of birth, marital status, photograph, signature, residential status, passport-size photographs, specimen signatures and every other information reasonably necessary for establishing the identity of the Data Principal or for complying with immigration, visa or statutory requirements.

6.3 Government-issued Identification Documents

The Company may collect and process copies or particulars of passports, Aadhaar, Permanent Account Number (PAN), voter identity cards, driving licences, Overseas Citizen of India (OCI) cards, Person of Indian Origin (PIO) cards, national identity cards issued by foreign jurisdictions and every other government-issued document required for the provision of Consultancy Services or compliance with Applicable Law.

6.4 Passport, Visa and Immigration Information

The Company may collect and process passport particulars, passport validity details, previous passports, visa history, previous visa refusals, immigration history, travel records, previous immigration applications, work permits, residence permits, permanent residence status, citizenship records, deportation history, removal orders, overstays, immigration investigations,

entry and exit records and every other information relating to the immigration status or travel history of the Data Principal which may be relevant for the provision of Consultancy Services.

6.5 Contact Information

The Company may collect the residential address, correspondence address, office address, telephone numbers, mobile numbers, electronic mail addresses, emergency contact details and every other contact information reasonably necessary for communicating with the Data Principal during the course of the Engagement.

6.6 Educational Information

The Company may collect educational certificates, academic transcripts, mark sheets, degree certificates, diplomas, vocational qualifications, professional certifications, language proficiency certificates, educational credential assessments, student records and every other information relating to the educational background of the Data Principal where such information is relevant to the Consultancy Services.

6.7 Employment and Professional Information

The Company may collect curriculum vitae, employment contracts, appointment letters, experience certificates, salary slips, employer reference letters, professional licences, employment history, designation, job description, employer details, business ownership records and every other information relating to the employment or professional background of the Data Principal.

6.8 Financial Information

The Company may collect bank statements, salary statements, income tax returns, income proofs, fixed deposit records, investment statements, proof of funds, financial declarations, sponsorship documents, education loan documents, financial affidavits, net-worth statements and every other financial information reasonably required for immigration, visa or residence permit applications.

6.9 Taxation Information

The Company may collect Permanent Account Number (PAN), Tax Deduction Account Number (TAN), Goods and Services Tax (GST) particulars where applicable, income tax returns, tax residency certificates, tax assessments and every other taxation information required under Applicable Law or by the relevant Government Authority.

6.10 Family Information

The Company may collect information relating to spouses, children, parents, dependants, guardians and other family members, including their names, dates of birth, nationality, passport particulars, immigration status, marital status and such other information as may be required for family sponsorship, dependent visas or other immigration-related purposes.

6.11 Medical Information

Where required by Applicable Law or by any Government Authority, Embassy, Consulate or Visa Application Centre, the Company may collect medical examination reports, vaccination certificates, medical fitness certificates, health declarations and every other medical

Rohit Kaul
Digitally signed
by Rohit Kaul
Date: 2026.07.17
17:22:10 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

information lawfully required for processing immigration or visa applications. The Company shall endeavour to process such information with an enhanced degree of confidentiality consistent with Applicable Law.

6.12 Police Clearance and Background Verification Information

The Company may collect police clearance certificates, criminal record declarations, court records, litigation history, background verification reports and other information relating to criminal proceedings or law enforcement records only where such information is required under Applicable Law or by the relevant Government Authority for immigration or visa purposes.

6.13 Electronic Communications

The Company may collect and retain correspondence exchanged through electronic mail, messaging applications, client portals, video conferencing platforms, telephone conversations where lawfully recorded, online forms, support requests and every other communication relating to the provision of Consultancy Services.

6.14 Technical and Electronic Information

Where the Data Principal accesses the Company's website, client portal or electronic systems, the Company may collect technical information including internet protocol (IP) addresses, browser type, operating system, device identifiers, log files, website usage information, session information, cookies and similar technologies to the extent necessary for maintaining system security, improving user experience, preventing fraud, diagnosing technical issues and administering the Company's electronic platforms.

6.15 Payment Information

The Company may collect payment confirmations, invoices, receipts, transaction references, banking details, payment gateway information and every other information reasonably necessary for processing payments, maintaining accounting records, complying with taxation laws and administering the contractual relationship between the Company and the Client. The Company shall not intentionally store complete payment card information except to the extent lawfully permitted or required for the provision of the Consultancy Services.

6.16 Documents Submitted During the Engagement

The Company may collect and retain declarations, affidavits, authorisation letters, consent forms, statutory forms, application forms, translations, notarised documents, legalised documents, apostilled documents, embassy correspondence, Government communications and every other document voluntarily submitted by or on behalf of the Client during the course of the Engagement.

6.17 Information Generated During the Provision of Consultancy Services

The Company may generate, compile and maintain internal notes, eligibility assessments, document verification records, compliance records, due diligence reports, communication logs, file movement records, application tracking information, internal observations, risk assessments and other records created by the Company during the ordinary course of providing Consultancy Services. Such internally generated records shall constitute part of the Company's

professional records and may contain Personal Data to the extent necessary for the lawful provision of the Consultancy Services.

6.18 No Obligation to Collect Every Category of Personal Data

The categories of Personal Data described in this Clause are illustrative of the types of information that may be processed by the Company and shall not necessarily be collected in every Engagement. The nature and extent of Personal Data collected shall always depend upon the Consultancy Services requested by the Client, the requirements prescribed by Applicable Law or the relevant Government Authority, the contractual relationship between the Parties and the legitimate purposes for which such Personal Data is required. The Company shall endeavour to collect only such Personal Data as is reasonably necessary and proportionate for the purposes for which it is processed in accordance with this Policy and Applicable Law.

7. SPECIAL CATEGORIES OF PERSONAL DATA

7.1 General

The Company acknowledges that certain categories of Personal Data, by reason of their nature, content or intended use, require a higher standard of confidentiality, security and protection than ordinary Personal Data. In the course of providing Consultancy Services, the Company may be required to collect, receive, access, review, verify, store, process, transmit or otherwise handle such information solely to the extent reasonably necessary for the provision of the Consultancy Services, compliance with Applicable Law, fulfilment of contractual obligations or compliance with the documentary requirements prescribed by the relevant Government Authority, Embassy, Consulate, Visa Application Centre or other competent authority.

The Company shall endeavour to ensure that every category of Personal Data falling within this Clause is processed strictly on a need-to-know basis, with restricted access, appropriate technical and organisational safeguards and only for lawful purposes consistent with this Policy and Applicable Law.

7.2 Medical and Health Information

Where required for immigration, visa, residence permit, work permit, permanent residence, citizenship or any other lawful purpose, the Company may collect and process medical examination reports, health declarations, vaccination records, disability certificates, medical fitness certificates, laboratory reports and other medical information required by the relevant Government Authority or authorised institution. The Company shall process such information only to the extent reasonably necessary for the relevant immigration process and shall endeavour to restrict access to such information to authorised personnel directly involved in providing the Consultancy Services.

7.3 Police Clearance and Criminal Record Information

The Company may collect and process Police Clearance Certificates, criminal record declarations, court orders, judicial records, information relating to pending criminal proceedings, previous convictions, immigration offences, deportation records or other law enforcement records only where such information is expressly required under Applicable Law or by the relevant Government Authority, Embassy, Consulate, Visa Application Centre or other competent authority. The Company shall not collect or process such information unless

**Rohit
Kaul**
Digitally
signed by
Rohit Kaul
Date:
2026.07.17
17:23:00

Your Personal Consultancy Firm's Address
Office No 102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

reasonably necessary for the purposes of the relevant Engagement or otherwise authorised by Applicable Law.

7.4 Immigration Compliance Information

The Company may collect and process information relating to previous visa refusals, immigration investigations, deportation orders, removal proceedings, overstays, immigration violations, cancellation of visas or permits, previous asylum applications, refugee claims, immigration appeals, exclusion orders or any other immigration compliance records which may affect the eligibility of the Client or which are required to be disclosed under Applicable Law or the requirements of the destination country.

7.5 Financial and Asset Information

Where required by the applicable immigration programme or the relevant Government Authority, the Company may collect and process detailed financial information including bank statements, investment portfolios, proof of funds, income records, property ownership documents, taxation records, sponsorship documents, loan records, financial affidavits, source of funds declarations and other financial documents necessary to demonstrate financial eligibility or compliance with immigration requirements. Such information shall be processed solely for the lawful purposes connected with the relevant Consultancy Services.

7.6 Biometric and Identity Verification Information

The Company may receive or process information relating to biometric appointments, biometric confirmation receipts, biometric enrolment records or identity verification documents where such information is required for immigration or visa purposes. The Company shall not independently collect fingerprints, iris scans, facial recognition data or other biometric identifiers unless expressly authorised by Applicable Law or unless such processing forms an essential and lawful component of the Consultancy Services requested by the Client.

7.7 Family and Dependent Information

The Company may collect and process Personal Data relating to spouses, children, parents, dependants or other family members of the Client where such information is necessary for dependent visa applications, family sponsorship programmes, permanent residence applications, citizenship applications or any other immigration process involving family members. The Company shall endeavour to ensure that such information is collected only to the extent reasonably necessary for the relevant purpose.

7.8 Information Relating to Minors

Where the Consultancy Services relate to a child or involve the processing of Personal Data relating to a child, the Company shall process such Personal Data only in accordance with Applicable Law and upon receiving the necessary consent, authorisation or instructions from the parent, lawful guardian or other person legally authorised to act on behalf of the child. The Company shall exercise reasonable care while processing Personal Data relating to children and shall endeavour to ensure that such information is used solely for lawful purposes connected with the Consultancy Services.

7.9 Documents Received from Third Parties

Rohit Kaul
Digitally signed by Rohit Kaul
Date: 2026.07.17 17:23:21
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company may receive Personal Data from employers, educational institutions, Government Authorities, Embassies, Consulates, Visa Application Centres, professional advisers, authorised representatives or other third parties lawfully authorised to provide such information. The Company shall process such information only for the purposes for which it was lawfully received and in accordance with this Policy, the applicable contractual arrangements and Applicable Law.

7.10 Enhanced Protection Measures

The Company recognises that the categories of Personal Data referred to in this Clause require enhanced standards of protection. Accordingly, the Company shall endeavour to implement additional technical, organisational and administrative safeguards, including restricted access controls, role-based permissions, secure storage mechanisms, controlled document handling procedures, confidentiality obligations applicable to personnel and other reasonable security measures appropriate to the nature of the information being processed. Access to such Personal Data shall ordinarily be limited to those persons whose official responsibilities require such access for the provision of the Consultancy Services or compliance with Applicable Law.

7.11 No Collection Beyond Lawful Necessity

The Company shall not intentionally collect or retain any category of Personal Data referred to in this Clause unless such collection or retention is reasonably necessary for the provision of the Consultancy Services, compliance with Applicable Law, fulfilment of contractual obligations, protection of legal rights or compliance with the documentary requirements prescribed by the relevant Government Authority, Embassy, Consulate, Visa Application Centre or other competent authority. Where the Company determines that particular information is no longer reasonably necessary for such purposes, it shall deal with such information in accordance with its record retention and data destruction policies, subject always to Applicable Law.

8. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

8.1 General

The Company shall process Personal Data only where such processing is lawful, necessary and reasonably connected with the provision of the Consultancy Services, the performance of contractual obligations, compliance with Applicable Law or any other lawful purpose recognised under Applicable Data Protection Laws. The Company shall endeavour to ensure that every processing activity undertaken by it is supported by an appropriate lawful basis having regard to the nature of the Personal Data, the purpose of processing, the relationship between the Company and the Data Principal and the applicable statutory or contractual requirements governing such processing.

Nothing contained in this Policy shall be construed as authorising the Company to process Personal Data in a manner inconsistent with Applicable Law or for any purpose that is unlawful, arbitrary or incompatible with the legitimate purposes for which such Personal Data was collected.

8.2 Processing Based on Consent

Rohit
Kaul

Digitally
signed by
Rohit Kaul
Date:
2026.07.17
17:23:45
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

Where Applicable Law requires the consent of the Data Principal, the Company shall process Personal Data only after obtaining such consent through lawful means. Such consent may be obtained through executed Service Agreements, Engagement Letters, Consent Forms, Authorisation Letters, declarations, application forms, electronic communications, website interfaces, client portals, digital acknowledgements or any other legally recognised method capable of demonstrating the Data Principal's intention to permit the processing of Personal Data.

The Company shall endeavour to ensure that consent, wherever required, is free, specific, informed, unconditional and evidenced by a clear affirmative act. The scope of the consent obtained shall be limited to the purposes communicated to the Data Principal unless further processing is otherwise authorised by Applicable Law.

8.3 Processing for the Provision of Consultancy Services

The Company may process Personal Data where such processing is reasonably necessary for providing the Consultancy Services requested by the Client. Such processing may include evaluating eligibility for immigration programmes, reviewing documentation, preparing applications, communicating with Government Authorities, arranging appointments, monitoring application progress, responding to queries, maintaining client records and performing every other activity reasonably necessary for the proper discharge of the Company's professional responsibilities.

The Data Principal acknowledges that the provision of accurate and complete Consultancy Services would not ordinarily be possible without the processing of Personal Data relevant to the particular Engagement.

8.4 Processing for Compliance with Applicable Law

The Company may process Personal Data where such processing is necessary for complying with any obligation imposed under Applicable Law, judicial orders, governmental directions, regulatory requirements, statutory reporting obligations, lawful requests made by Government Authorities or any other legal requirement binding upon the Company.

Where Applicable Law requires the Company to disclose Personal Data to a Government Authority, regulatory body, law enforcement agency, court, tribunal or any other competent authority, the Company may make such disclosure without obtaining any additional consent to the extent permitted or required by Applicable Law.

8.5 Processing for Performance of Contractual Obligations

The Company may process Personal Data where such processing is reasonably necessary for entering into, performing, administering or enforcing any Service Agreement, Engagement Letter, consultancy arrangement or any other contractual relationship between the Company and the Client. Such processing may include maintaining engagement records, communicating with the Client, issuing invoices, processing payments, verifying documents, responding to contractual requests, resolving disputes and exercising or enforcing contractual rights.

8.6 Processing for Legitimate Business Operations

The Company may process Personal Data to the extent reasonably necessary for the efficient administration of its lawful business operations, including client relationship management.

document management, information technology administration, internal compliance, quality assurance, staff training, cybersecurity, prevention of fraud, audit functions, business continuity planning, record management, risk assessment and other legitimate operational activities directly connected with the Company's business.

The Company shall endeavour to ensure that such processing remains proportionate and does not unreasonably prejudice the rights or legitimate interests of the Data Principal.

8.7 Processing for Establishment, Exercise or Defence of Legal Rights

The Company may process Personal Data where such processing is reasonably necessary for establishing, exercising or defending any legal right, contractual right or legitimate claim of the Company or the Client. Such processing may include responding to legal proceedings, arbitration, regulatory investigations, governmental enquiries, disciplinary proceedings, complaints, audits, insurance claims or any other dispute resolution process.

8.8 Processing for Fraud Prevention and Security

The Company may process Personal Data for the purpose of preventing, detecting, investigating or responding to fraud, identity theft, document forgery, cyber incidents, unauthorised access, misuse of the Company's systems, breaches of contractual obligations or any other activity which may expose the Company, its Clients or any third party to legal, financial or reputational risk.

The Company may also process Personal Data for maintaining the security, integrity and availability of its information technology systems, communication platforms, client databases and document management systems.

8.9 Processing for Communication with Government Authorities and Third Parties

Where reasonably necessary for the provision of the Consultancy Services, the Company may process Personal Data for the purpose of communicating with Government Authorities, Embassies, Consulates, Visa Application Centres, educational institutions, employers, professional advisers, translators, courier agencies, notaries, document verification agencies and other authorised third parties engaged in connection with the relevant immigration or visa process.

Such processing shall be limited to the extent reasonably necessary for the lawful performance of the Consultancy Services and shall be undertaken in accordance with this Policy, the Agreement and Applicable Law.

8.10 Processing of Information Voluntarily Provided

Where a Data Principal voluntarily submits Personal Data, documents, declarations, communications or any other information to the Company for the purpose of obtaining Consultancy Services or otherwise interacting with the Company, the Company may process such information to the extent reasonably necessary for responding to the request, providing the requested Services, maintaining appropriate records and complying with Applicable Law.

Rohi
t
Kaul

Digitally
signed by
Rohit Kaul
Date:
2026.07.17
17:24:31
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The submission of such information shall not, by itself, require the Company to process Personal Data for purposes unrelated to the reason for which such information was voluntarily provided.

8.11 No Processing for Unlawful Purposes

The Company shall not knowingly process Personal Data for any unlawful, fraudulent, deceptive, discriminatory or unethical purpose. The Company shall not sell, commercially exploit, lease or otherwise deal in Personal Data in a manner inconsistent with this Policy, the contractual arrangements governing the relationship between the Company and the Client or Applicable Law.

Where the Company reasonably believes that any request involving Personal Data is unlawful, fraudulent or inconsistent with Applicable Law, the Company reserves the right to refuse such request, suspend the relevant processing activity or take such other lawful action as may be considered appropriate.

8.12 Continuing Obligation

The lawful basis upon which Personal Data is processed shall continue throughout the period during which the Company retains or processes such Personal Data. Where the circumstances giving rise to the lawful basis materially change, the Company may review the continued necessity of such processing and take such steps as may be appropriate under Applicable Law, including obtaining fresh consent where required, restricting further processing, anonymising the Personal Data or securely deleting such Personal Data in accordance with this Policy and the Company's record retention practices.

9. CONSENT

9.1 General

The Company recognises that the Personal Data entrusted to it belongs to the Data Principal and acknowledges the importance of obtaining valid consent wherever such consent is required under Applicable Data Protection Laws. Accordingly, the Company shall endeavour to obtain the consent of the Data Principal prior to collecting, receiving, using or otherwise processing Personal Data where such consent is required under Applicable Law. Such consent shall ordinarily be obtained before the commencement of the relevant processing activity unless Applicable Law expressly permits processing without prior consent.

Nothing contained in this Policy shall prevent the Company from processing Personal Data without obtaining fresh consent where such processing is otherwise authorised or required under Applicable Law or is necessary for any legitimate use recognised under Applicable Data Protection Laws.

9.2 Characteristics of Consent

Where consent is required under Applicable Law, the Company shall endeavour to ensure that such consent is free, specific, informed, unconditional, unambiguous and evidenced by a clear affirmative action on the part of the Data Principal. The Company shall not knowingly obtain consent by fraud, coercion, misrepresentation, undue influence or any other unlawful means.

**Rohit
Kaul**

Digitally
signed by
Rohit Kaul
Date:
2026.07.17
17:25:12
INDIA

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company shall also endeavour to ensure that the request for consent is presented in a clear and intelligible manner so that the Data Principal is reasonably informed of the nature of the Personal Data proposed to be processed, the purposes for which such processing is intended and the rights available under Applicable Law.

9.3 Manner of Obtaining Consent

Subject to Applicable Law, consent may be obtained by the Company through one or more lawful methods, including the execution of a Service Agreement, Engagement Letter, Consent Form, Authorisation Letter, declaration, application form, client onboarding documents, physical signatures, electronic signatures, digital acknowledgements, client portal confirmations, website acceptance mechanisms, electronic communications, electronic document management systems or any other legally recognised method capable of evidencing the intention of the Data Principal to permit the processing of Personal Data.

Where the Company reasonably relies upon an authorised representative acting on behalf of the Data Principal, the Company may presume that such representative possesses the necessary authority unless the Company has actual knowledge to the contrary.

9.4 Scope of Consent

Consent obtained by the Company shall extend only to the lawful purposes communicated to the Data Principal or otherwise permitted under Applicable Law. Such consent shall ordinarily include the collection, verification, organisation, storage, review, processing, disclosure, transmission, retention and other handling of Personal Data reasonably necessary for the provision of the Consultancy Services, compliance with Applicable Law, fulfilment of contractual obligations, communication with Government Authorities and authorised third parties, maintenance of records and protection of the Company's legal rights.

The Company shall not knowingly process Personal Data for purposes materially inconsistent with the purposes for which consent was originally obtained unless additional consent is obtained where required or such processing is otherwise authorised by Applicable Law.

9.5 Continuing Consent

Unless withdrawn in accordance with Applicable Law or unless otherwise limited by its terms, consent once validly granted shall continue throughout the duration of the Engagement and, where reasonably necessary, for such additional period as may be required for completing the Consultancy Services, complying with statutory obligations, maintaining records, responding to Government Authorities, establishing, exercising or defending legal rights or complying with Applicable Law.

The completion, suspension or termination of the Consultancy Services shall not automatically invalidate any processing that is lawfully undertaken after such completion or termination where such continued processing is authorised by Applicable Law or reasonably necessary for the purposes specified in this Policy.

9.6 Consent for Cross-Border Processing

The Data Principal acknowledges that immigration and visa consultancy services frequently require the disclosure, transmission or transfer of Personal Data to Government Authorities,

Embassies, Consulates, Visa Application Centres, employers, educational institutions, professional advisers and other authorised organisations situated outside India.

Where the Company is required to process Personal Data outside India in connection with the Consultancy Services, the Data Principal expressly acknowledges that such processing may involve cross-border transfer of Personal Data in accordance with Applicable Law and the provisions of this Policy.

9.7 Consent for Third-Party Disclosures

The Data Principal acknowledges that the Company may disclose Personal Data to Third-Party Service Providers, translators, notaries, courier agencies, document verification agencies, payment service providers, information technology service providers, cloud service providers, professional advisers or other persons engaged by the Company for assisting in the provision of the Consultancy Services.

Such disclosures shall be limited to the extent reasonably necessary for the relevant purpose and shall be made subject to appropriate contractual, professional or statutory obligations of confidentiality wherever reasonably practicable.

9.8 Withdrawal of Consent

Subject to Applicable Law, the Data Principal may withdraw consent previously granted for the processing of Personal Data by giving written notice to the Company or by using such mechanism as may be made available by the Company from time to time.

Withdrawal of consent shall operate prospectively and shall not affect the lawfulness of any processing undertaken prior to the receipt of such withdrawal by the Company.

9.9 Consequences of Withdrawal of Consent

The Data Principal acknowledges that the withdrawal of consent may materially affect the Company's ability to continue providing the Consultancy Services. Where the processing of Personal Data is reasonably necessary for preparing, reviewing, submitting or managing immigration, visa, work permit, residence permit, citizenship or other related applications, the Company may be unable to continue or complete the Engagement following the withdrawal of consent.

The Company shall not be liable for any delay, interruption, suspension, rejection of an application, inability to provide the Consultancy Services or any other consequence directly arising from the withdrawal of consent by the Data Principal. The withdrawal of consent shall not relieve the Client from any obligation to pay Professional Fees, Third-Party Charges or other amounts lawfully payable under the Agreement in respect of Services already rendered.

9.10 Consent Relating to Third Parties

Where the Client submits Personal Data relating to a spouse, child, dependant, employee, business associate or any other third party, the Client represents and warrants that he, she or it has obtained all necessary permissions, authorisations or consents required under Applicable Law to disclose such Personal Data to the Company and to permit the Company to process such Personal Data for the purposes of the Consultancy Services.

**Rohit
Kaul**
Digitally
signed by
Rohit Kaul
Date:
2026.07.17
17:26:02
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company shall be entitled to rely upon such representation unless it has actual knowledge that the same is false or misleading.

9.11 Refusal to Provide Consent

Where the Data Principal refuses to provide consent for the processing of Personal Data that is reasonably necessary for the provision of the Consultancy Services, the Company reserves the right to decline the Engagement, suspend the Consultancy Services, refuse to accept or process any Application or terminate the contractual relationship in accordance with the Agreement and Applicable Law.

9.12 No Waiver of Statutory Rights

Nothing contained in this Clause shall be construed as limiting, excluding or waiving any right available to a Data Principal under Applicable Data Protection Laws. Similarly, nothing contained herein shall prevent the Company from processing Personal Data where such processing is authorised without consent under Applicable Law or where consent is not the lawful basis for processing.

10. PURPOSES OF COLLECTION AND PROCESSING OF PERSONAL DATA

10.1 General

The Company shall collect, receive, record, organise, verify, use, process, disclose, retain and otherwise handle Personal Data only for lawful, specified and legitimate purposes connected with the provision of the Consultancy Services, the performance of contractual obligations, compliance with Applicable Law, protection of legal rights, maintenance of internal business operations and such other lawful purposes as may be reasonably necessary in the ordinary course of the Company's business.

The Company shall endeavour to ensure that Personal Data is processed only to the extent reasonably necessary for the purpose for which it was collected and shall not knowingly process Personal Data in a manner that is incompatible with the purposes communicated to the Data Principal or otherwise authorised under Applicable Law.

10.2 Provision of Consultancy Services

The Company may collect and process Personal Data for the purpose of assessing eligibility, providing immigration consultancy, visa consultancy, documentation assistance, application management, compliance support, administrative assistance, pre-departure guidance, post-landing advisory services where agreed, and every other Consultancy Service requested by the Client under the Agreement.

Such processing may include reviewing documents, analysing eligibility, preparing applications, maintaining client files, coordinating with Government Authorities, scheduling appointments, responding to client queries and monitoring the progress of applications.

10.3 Preparation and Submission of Applications

The Company may process Personal Data for preparing, reviewing, verifying, compiling, translating, correcting, organising and submitting applications relating to visas, work permits, residence permits, permanent residence, citizenship, visitor visas, student visas, business visas,

Rohi
t
Kaul
Digitally
signed by
Rohit Kaul
Date:
2026.07.17
17:26:27
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

dependent visas and every other immigration-related application before the competent Government Authority, Embassy, Consulate, Visa Application Centre or other authorised institution.

10.4 Verification of Information and Documents

The Company may process Personal Data for verifying the identity of the Client, conducting preliminary document reviews, carrying out internal due diligence, identifying inconsistencies, ensuring completeness of documentation, preventing fraudulent submissions and determining whether the documents and information provided appear suitable for the intended immigration process.

Nothing contained in this Clause shall impose upon the Company any obligation to independently certify the authenticity or legality of documents submitted by the Client unless expressly agreed in writing.

10.5 Compliance with Immigration Requirements

The Company may process Personal Data for complying with immigration laws, visa regulations, documentary requirements, Government directions, Embassy instructions, Consular requirements, Visa Application Centre procedures and every other legal or administrative requirement applicable to the Consultancy Services requested by the Client.

10.6 Communication with Government Authorities and Other Authorised Bodies

The Company may process Personal Data for communicating, corresponding, responding or submitting information to Government Authorities, Embassies, Consulates, Visa Application Centres, immigration departments, employers, educational institutions, licensing authorities, professional bodies, document verification agencies and other authorised organisations involved in the immigration or visa process.

10.7 Client Communication and Relationship Management

The Company may process Personal Data for communicating with Clients regarding appointments, consultations, document requirements, deficiencies in documentation, payment reminders, application status, requests for additional information, changes in immigration requirements, updates issued by Government Authorities and every other matter reasonably connected with the Engagement.

The Company may also process Personal Data for maintaining appropriate client records, responding to enquiries, addressing grievances, obtaining instructions and administering the contractual relationship between the Parties.

10.8 Compliance with Applicable Law

The Company may process Personal Data where such processing is reasonably necessary for complying with Applicable Law, judicial orders, regulatory requirements, Government notifications, lawful directions issued by competent authorities, statutory reporting obligations, tax laws, anti-money laundering requirements, Know Your Customer (KYC) requirements, audit requirements and every other legal obligation binding upon the Company.

10.9 Internal Administration and Business Operations

The Company may process Personal Data for maintaining internal records, managing client files, conducting quality assurance reviews, staff training, operational administration, accounting, billing, document management, information technology administration, business continuity planning, cybersecurity management, internal audits, compliance monitoring, risk management and every other legitimate business activity reasonably necessary for the efficient operation of the Company.

10.10 Prevention of Fraud and Protection of Legal Rights

The Company may process Personal Data for preventing fraud, detecting forged or altered documents, identifying suspicious activities, protecting the integrity of immigration applications, safeguarding the Company's systems and records, investigating complaints, establishing, exercising or defending legal rights, resolving disputes and protecting the lawful interests of the Company, its Clients and other affected persons.

10.11 Record Retention and Regulatory Compliance

The Company may retain and process Personal Data after completion of the Consultancy Services where such retention is reasonably necessary for complying with Applicable Law, maintaining professional records, responding to Government enquiries, dealing with regulatory inspections, resolving disputes, enforcing contractual rights, defending legal proceedings or complying with internal record retention policies.

10.12 Information Technology, Website Administration and Security

The Company may process Personal Data generated through its website, client portal, electronic communication systems, information technology infrastructure and document management systems for maintaining system security, preventing unauthorised access, monitoring system performance, detecting cybersecurity incidents, maintaining audit logs, troubleshooting technical issues, improving user experience and administering the Company's digital platforms.

10.13 Research, Training and Service Improvement

Subject to Applicable Law and appropriate safeguards, the Company may process Personal Data for internal research, staff training, quality assurance, development of operational procedures, improvement of Consultancy Services, enhancement of document management practices and evaluation of service delivery standards, provided that such processing is carried out responsibly and only to the extent reasonably necessary for such purposes.

10.14 Purposes Permitted by Applicable Law

The Company may process Personal Data for every other purpose expressly authorised, required or permitted under Applicable Law, judicial orders, regulatory directions or any other lawful authority, provided that such processing remains consistent with the principles set out in this Policy.

10.15 Restriction on Use

**Rohit
Kaul**
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:27:42
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

Except as expressly provided in this Policy, the Agreement or Applicable Law, the Company shall not knowingly process Personal Data for purposes unrelated to the Consultancy Services or otherwise use Personal Data in a manner that is unlawful, fraudulent, misleading or materially inconsistent with the purposes for which such Personal Data was originally collected.

11. SOURCES OF PERSONAL DATA

11.1 General

The Company may collect, receive, obtain or otherwise lawfully acquire Personal Data from one or more sources depending upon the nature of the Consultancy Services requested, the immigration programme involved, the contractual relationship between the Parties, the documentary requirements prescribed by the relevant Government Authority, Embassy, Consulate, Visa Application Centre or other competent authority and the circumstances of the particular Engagement. The Company shall endeavour to ensure that Personal Data is collected only from lawful sources and only to the extent reasonably necessary for the purposes specified in this Policy, the Agreement or Applicable Law.

11.2 Personal Data Obtained Directly from the Data Principal

The Company may collect Personal Data directly from the Data Principal through consultations, meetings, interviews, client onboarding procedures, application forms, questionnaires, declarations, affidavits, correspondence, emails, telephone conversations, video conferences, electronic communications, client portals, website submissions, mobile applications, physical documents and every other lawful mode through which the Data Principal voluntarily provides Personal Data for the purpose of obtaining the Consultancy Services.

11.3 Personal Data Obtained from the Client

Where the Client is a body corporate, partnership firm, educational institution, employer or any other legal entity engaging the Company for Consultancy Services relating to one or more individuals, the Company may receive Personal Data from such Client in connection with the relevant Engagement. The Client shall remain responsible for ensuring that it possesses the lawful authority and all necessary permissions required under Applicable Law to disclose such Personal Data to the Company.

11.4 Personal Data Obtained from Authorised Representatives

The Company may receive Personal Data from any person authorised by the Data Principal to act on his or her behalf, including attorneys, guardians, parents, legal representatives, family members, employers, human resource personnel, immigration coordinators or any other authorised representative. The Company shall be entitled to rely upon the authority of such representative unless the Company has actual knowledge that such authority is invalid, withdrawn or otherwise defective.

11.5 Personal Data Obtained from Employers and Business Organisations

Where the Consultancy Services relate to employment-based immigration, intra-company transfers, overseas assignments, work permits, business visas or similar immigration programmes, the Company may receive Personal Data from employers, group companies,

human resource departments, recruitment agencies, staffing organisations, payroll administrators or other authorised business organisations for the purpose of providing the Consultancy Services.

11.6 Personal Data Obtained from Educational Institutions

Where the Consultancy Services relate to student visas, educational migration, academic admissions or qualification assessments, the Company may receive Personal Data from schools, colleges, universities, educational boards, examination authorities, credential assessment organisations or other educational institutions lawfully authorised to disclose such information.

11.7 Personal Data Obtained from Government Authorities

The Company may receive Personal Data from Government Authorities, immigration departments, passport authorities, tax authorities, law enforcement agencies or other public authorities where such disclosure is authorised or required under Applicable Law or forms part of the immigration process undertaken on behalf of the Client.

11.8 Personal Data Obtained from Embassies, Consulates and Visa Application Centres

The Company may receive Personal Data, correspondence, communications, application updates, appointment confirmations, requests for additional documents, notices, decisions or any other information from Embassies, Consulates, Visa Application Centres or other authorised immigration agencies for the purpose of facilitating the Consultancy Services requested by the Client.

11.9 Personal Data Obtained from Third-Party Service Providers

The Company may receive Personal Data from translators, interpreters, notaries, document verification agencies, courier service providers, medical examination centres, payment gateway providers, information technology service providers, cloud service providers, cybersecurity service providers, professional advisers or other Third-Party Service Providers engaged in connection with the Consultancy Services, provided that such receipt of Personal Data is lawful and reasonably necessary for the purposes of the Engagement.

11.10 Personal Data Obtained through the Company's Website and Electronic Platforms

Where a person visits the Company's website, client portal, mobile application or any other electronic platform operated by the Company, the Company may automatically collect certain technical information including internet protocol (IP) addresses, browser information, device identifiers, operating system details, session information, website usage information, cookies, log files and other technical data through lawful technological means for the purposes of system administration, cybersecurity, fraud prevention, analytics, service improvement and maintenance of the Company's digital infrastructure.

11.11 Personal Data Obtained from Publicly Available Sources

The Company may collect or verify Personal Data from publicly available and lawfully accessible sources where such collection is reasonably necessary for the provision of the Consultancy Services, verification of information supplied by the Client, compliance with Applicable Law, prevention of fraud or protection of the legitimate interests of the Company.

Such sources may include official Government databases, public registers, regulatory records, publicly available professional profiles, corporate records or other publicly accessible information lawfully available to the Company.

11.12 Personal Data Generated During the Course of the Engagement

The Company may generate, compile or create Personal Data during the course of providing the Consultancy Services, including internal file notes, document review records, eligibility assessments, compliance observations, due diligence reports, communication logs, appointment records, application tracking information, billing records, audit records, internal correspondence, quality assurance reports and other records reasonably necessary for the administration of the Engagement. Such information shall be treated as Personal Data to the extent that it relates to an identifiable individual.

11.13 Responsibility for Accuracy of Information

The Company shall ordinarily rely upon the Personal Data supplied by the Data Principal, the Client or other lawful sources and shall not be under any general obligation to independently investigate, certify or guarantee the accuracy, authenticity or completeness of such information unless expressly agreed otherwise in writing or required under Applicable Law. The Data Principal and the Client shall remain responsible for ensuring that the Personal Data supplied to the Company is true, accurate, complete and up to date.

11.14 Lawful Collection

The Company shall endeavour to collect Personal Data only through lawful means and from lawful sources. The Company shall not knowingly collect Personal Data through fraudulent, deceptive, coercive, unlawful or unethical means. Where the Company becomes aware that Personal Data has been obtained in violation of Applicable Law, the Company reserves the right to decline the Engagement, suspend the Consultancy Services, refuse to process such Personal Data or take such other action as may be considered appropriate under Applicable Law and the Agreement.

12. COLLECTION OF PERSONAL DATA

12.1 General

The Company shall collect Personal Data only through lawful, fair and transparent means and only to the extent reasonably necessary for the provision of the Consultancy Services, compliance with Applicable Law, fulfilment of contractual obligations, protection of the legitimate interests of the Company, establishment, exercise or defence of legal rights or for such other lawful purposes as are recognised under this Policy and Applicable Law. The Company shall endeavour to ensure that the collection of Personal Data is proportionate to the nature of the Consultancy Services requested and is limited to information reasonably required for the relevant Engagement.

12.2 Collection During Client Onboarding

The Company may collect Personal Data during the client onboarding process through client registration forms, consultation forms, engagement letters, service agreements, client information sheets, KYC documentation, declarations, authorisation letters, consent forms and other onboarding documents executed by or on behalf of the Client.

The Company may also collect additional Personal Data where required to establish the identity of the Client, verify eligibility for the requested Consultancy Services or comply with Applicable Law.

12.3 Collection During Consultations

Personal Data may be collected during physical meetings, online consultations, telephone calls, video conferences, interviews, conferences or any other interaction between the Company and the Client where such collection is reasonably necessary for assessing eligibility, understanding the Client's requirements, providing professional advice or rendering the Consultancy Services.

The Company may maintain written records, consultation notes or electronic records of such interactions for legitimate business purposes and in accordance with this Policy.

12.4 Collection Through Documents Submitted by the Client

The Company may collect Personal Data through passports, visas, identity documents, educational certificates, employment records, financial documents, taxation records, medical reports, police clearance certificates, affidavits, declarations, translations, photographs and every other document voluntarily submitted by or on behalf of the Client during the course of the Engagement.

The Company may retain copies of such documents in accordance with its record retention policy and Applicable Law.

12.5 Collection Through Electronic Communications

The Company may collect Personal Data communicated through electronic mail, messaging applications, SMS, client portals, online meeting platforms, electronic document management systems, electronic signatures, digital forms, scanned documents and every other lawful electronic communication channel used by the Client or the Company during the course of the Engagement.

Electronic communications may be retained by the Company where reasonably necessary for maintaining records, evidencing instructions, complying with legal obligations or protecting the Company's legal rights.

12.6 Collection Through the Company's Website and Digital Platforms

Where a person visits the Company's website, client portal, mobile application or any other digital platform operated by the Company, the Company may collect Personal Data voluntarily submitted through enquiry forms, consultation requests, appointment booking systems, contact forms, newsletter subscriptions, online chat facilities, document upload portals or other interactive features available on such platforms.

The Company may also automatically collect certain technical information through cookies, server logs and similar technologies in accordance with this Policy and the Company's Cookies Policy.

12.7 Collection During the Provision of Consultancy Services

The Company may continue to collect Personal Data throughout the duration of the Engagement whenever additional information or documentation becomes necessary for

preparing applications, responding to Government Authorities, satisfying documentary deficiencies, complying with revised immigration requirements, processing additional applications or otherwise providing the Consultancy Services.

The Client acknowledges that immigration procedures frequently require supplementary documentation after commencement of the Engagement and agrees to provide such information where reasonably requested by the Company.

12.8 Collection from Government Authorities and Third Parties

Where authorised by the Client or otherwise permitted under Applicable Law, the Company may collect Personal Data from Government Authorities, Embassies, Consulates, Visa Application Centres, employers, educational institutions, professional advisers, document verification agencies, medical examination centres, language testing organisations and other authorised third parties whenever such information is reasonably necessary for the Consultancy Services.

The Company shall endeavour to ensure that such collection is undertaken only through lawful channels.

12.9 Collection for Verification and Compliance

The Company may collect additional Personal Data where reasonably necessary for carrying out identity verification, Know Your Customer (KYC) procedures, document verification, sanctions screening, fraud prevention measures, compliance reviews, internal due diligence, regulatory compliance or other verification procedures considered appropriate by the Company or required under Applicable Law.

Nothing contained in this Clause shall impose upon the Company any obligation to independently verify every document or statement supplied by the Client unless expressly agreed in writing or required under Applicable Law.

12.10 Collection of Information Generated During the Engagement

The Company may generate and collect additional Personal Data during the course of providing the Consultancy Services, including internal file notes, eligibility assessments, compliance observations, application tracking records, communication logs, billing records, appointment records, document review records, quality assurance reports, internal correspondence and every other record reasonably necessary for the efficient administration of the Engagement.

Such records shall constitute part of the Company's professional records and may continue to be retained in accordance with this Policy and the Company's record retention practices.

12.11 Collection of Personal Data Relating to Family Members and Dependants

Where the Consultancy Services relate to dependent visas, family sponsorship, permanent residence applications, citizenship applications or any immigration process involving more than one individual, the Company may collect Personal Data relating to spouses, children, parents, guardians or other dependants to the extent reasonably necessary for the relevant immigration process.

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:30:09 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Client represents that he or she possesses the necessary authority to provide such information to the Company or has otherwise obtained the permissions required under Applicable Law.

12.12 No Obligation to Collect Unnecessary Personal Data

The Company shall endeavour to avoid collecting Personal Data that is excessive, irrelevant or unnecessary for the provision of the Consultancy Services or compliance with Applicable Law. Where the Company determines that certain Personal Data is not reasonably necessary for the relevant purpose, it may decline to collect such information or may securely dispose of such information in accordance with its internal policies and Applicable Law.

12.13 Refusal to Provide Personal Data

The Client acknowledges that certain categories of Personal Data are essential for the provision of immigration and visa consultancy services. Where the Client refuses or fails to provide Personal Data reasonably required by the Company, the relevant Government Authority, Embassy, Consulate, Visa Application Centre or Applicable Law, the Company may be unable to commence or continue the Consultancy Services, prepare or submit applications, respond to governmental requirements or otherwise perform its contractual obligations. In such circumstances, the Company shall not be responsible for any delay, suspension, rejection of applications or inability to provide the Consultancy Services arising directly from the Client's refusal or failure to provide the required Personal Data.

12.14 Collection in Good Faith

The Company shall collect Personal Data in good faith and solely for legitimate purposes connected with its business operations. The Company shall not knowingly collect Personal Data by unlawful, deceptive, misleading, coercive or unethical means and shall endeavour to maintain appropriate standards of transparency, professionalism and fairness throughout the collection process.

13. USE AND PROCESSING OF PERSONAL DATA

13.1 General

The Company shall use, process, analyse, organise, verify, classify, retrieve, consult, transmit, disclose, store, retain, archive and otherwise handle Personal Data only to the extent reasonably necessary for the lawful purposes specified in this Policy, the Agreement, Applicable Law or any other lawful purpose connected with the provision of the Consultancy Services. The Company shall endeavour to ensure that every processing activity is proportionate, relevant and consistent with the legitimate purpose for which the Personal Data was originally collected.

The Company shall not knowingly process Personal Data in a manner that is unlawful, fraudulent, deceptive, arbitrary or materially inconsistent with the purposes communicated to the Data Principal or otherwise authorised under Applicable Law.

13.2 Processing for Immigration and Visa Consultancy Services

The Company may process Personal Data for evaluating the eligibility of the Client under various immigration programmes, providing professional advice relating to immigration laws and procedures, preparing immigration strategies, reviewing documentary requirements,

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:30:47
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

preparing visa applications, residence permit applications, work permit applications, permanent residence applications, citizenship applications and every other application or representation reasonably connected with the Consultancy Services requested by the Client.

The Company may further process Personal Data for monitoring the progress of applications, responding to communications received from Government Authorities, advising the Client regarding documentary deficiencies and assisting the Client throughout the immigration process.

13.3 Processing for Document Preparation and Verification

The Company may process Personal Data for preparing, reviewing, organising, translating, formatting, correcting, verifying, certifying, compiling and maintaining documents required for immigration or visa purposes. Such processing may include comparing information contained in different documents, identifying discrepancies, requesting clarification from the Client, verifying the completeness of documentation and ensuring that applications are prepared in accordance with the documentary requirements prescribed by the relevant Government Authority or other competent authority.

The Company shall not, however, be responsible for independently certifying the authenticity or legal validity of documents supplied by the Client except where expressly agreed in writing.

13.4 Processing for Communication and Correspondence

The Company may process Personal Data for communicating with Clients, authorised representatives, Government Authorities, Embassies, Consulates, Visa Application Centres, employers, educational institutions, professional advisers and other authorised persons in connection with the Consultancy Services. Such processing may include responding to queries, issuing reminders, requesting additional documentation, scheduling consultations or appointments, forwarding Government communications, providing status updates and maintaining records of correspondence.

13.5 Processing for Regulatory and Statutory Compliance

The Company may process Personal Data where such processing is reasonably necessary for complying with Applicable Law, judicial orders, regulatory directions, Government notifications, tax laws, anti-money laundering requirements, Know Your Customer (KYC) obligations, audit requirements or any other statutory obligation applicable to the Company or the Consultancy Services.

Where the Company is required by law to retain, disclose or otherwise process Personal Data, such processing shall be deemed to be authorised under this Policy.

13.6 Processing for Internal Administration

The Company may process Personal Data for maintaining client files, administering engagements, managing document repositories, preparing invoices, maintaining accounting records, conducting internal audits, quality assurance reviews, operational planning, business continuity management, employee training, compliance monitoring, cybersecurity management, information technology administration and every other internal administrative activity reasonably necessary for the efficient operation of the Company's business.

13.7 Processing for Fraud Prevention and Risk Management

The Company may process Personal Data for identifying forged or altered documents, detecting suspicious activities, preventing identity theft, investigating fraudulent conduct, assessing operational risks, protecting confidential information, safeguarding the Company's information systems and maintaining the integrity of immigration applications and business operations.

The Company reserves the right to suspend processing or decline the Engagement where it reasonably believes that any Personal Data, document or information supplied by the Client is false, misleading, fraudulent or otherwise inconsistent with Applicable Law.

13.8 Processing by Automated Systems

The Company may utilise information technology systems, document management software, cloud-based platforms, customer relationship management systems, communication platforms, artificial intelligence-assisted tools, workflow automation software and other technological solutions for the purpose of storing, organising, retrieving, processing and managing Personal Data.

The use of such systems shall not diminish the Company's obligation to implement reasonable technical and organisational safeguards for the protection of Personal Data.

13.9 Processing by Employees and Authorised Personnel

Personal Data may be processed by directors, officers, employees, consultants, interns, authorised representatives, professional advisers, contractors and Third-Party Service Providers engaged by the Company strictly on a need-to-know basis and only to the extent reasonably necessary for the performance of their respective duties or the provision of the Consultancy Services.

The Company shall endeavour to ensure that such persons remain bound by contractual, professional or statutory obligations of confidentiality and comply with the requirements of this Policy.

13.10 Processing for Legal Proceedings and Dispute Resolution

The Company may process Personal Data where reasonably necessary for establishing, exercising or defending legal rights, responding to legal proceedings, arbitration, mediation, regulatory investigations, governmental enquiries, disciplinary proceedings, insurance claims, complaints or any other judicial, quasi-judicial or administrative process involving the Company or the Client.

13.11 Processing for Record Retention and Historical Reference

The Company may continue to process and retain Personal Data after completion or termination of the Consultancy Services where such processing is reasonably necessary for maintaining professional records, responding to future enquiries from Government Authorities, complying with statutory retention requirements, enforcing contractual rights, defending legal claims or complying with the Company's internal record retention policies.

13.12 Processing Subject to Confidentiality

**Rohit
Kaul**
Digitally signed by
Rohit Kaul
Date:
2026.07.17
17:32:10
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company shall endeavour to ensure that every activity involving the processing of Personal Data is carried out in accordance with appropriate standards of confidentiality, information security and professional responsibility. Access to Personal Data shall ordinarily be restricted to those persons whose official responsibilities reasonably require such access for the provision of the Consultancy Services or compliance with Applicable Law.

13.13 No Processing Beyond Lawful Necessity

The Company shall not knowingly process Personal Data for purposes that are excessive, unrelated or incompatible with the purposes for which such Personal Data was originally collected unless such processing is otherwise authorised by Applicable Law or by the Data Principal. Where the Company determines that continued processing is no longer reasonably necessary, it shall take appropriate steps to restrict, anonymise, erase or otherwise dispose of such Personal Data in accordance with this Policy and Applicable Law.

14. DISCLOSURE OF PERSONAL DATA

14.1 General

The Company recognises that Personal Data entrusted to it is confidential in nature and shall not disclose, publish, release, distribute, communicate, transmit, transfer or otherwise make such Personal Data available to any person except where such disclosure is reasonably necessary for the provision of the Consultancy Services, is authorised by the Data Principal, is required or permitted under Applicable Law, is necessary for the performance of contractual obligations or is otherwise carried out in accordance with this Policy.

The Company shall endeavour to ensure that every disclosure of Personal Data is proportionate, limited to the minimum information reasonably necessary for the relevant purpose and made only to persons or entities having a legitimate need or lawful authority to receive such information.

14.2 Disclosure for the Provision of Consultancy Services

The Company may disclose Personal Data where such disclosure is reasonably necessary for providing the Consultancy Services requested by the Client, including the preparation, submission, processing, follow-up, monitoring or completion of immigration, visa, work permit, residence permit, permanent residence, citizenship or other immigration-related applications.

Such disclosure may include the transmission of documents, supporting records, correspondence, explanations or clarifications required for the proper execution of the Engagement.

14.3 Disclosure to Government Authorities

The Company may disclose Personal Data to Government Authorities, immigration departments, passport authorities, taxation authorities, regulatory bodies, law enforcement agencies, courts, tribunals or any other competent public authority where such disclosure is required or authorised under Applicable Law, pursuant to a judicial order, governmental direction, statutory requirement or lawful request issued by such authority.

**Rohit
Kaul**
Digitally
signed by
Rohit Kaul
Date:
2026.07.17
17:32:44
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company shall not be responsible for the subsequent processing of Personal Data by such authorities once the information has been lawfully disclosed.

14.4 Disclosure to Embassies, Consulates and Visa Application Centres

The Company may disclose Personal Data to Embassies, Consulates, High Commissions, Visa Application Centres, immigration processing agencies and other authorised organisations involved in the immigration process where such disclosure is reasonably necessary for preparing, submitting, processing or supporting the relevant immigration or visa application.

The Client acknowledges that the Company cannot control the manner in which such authorities subsequently process, retain or disclose Personal Data after its lawful submission.

14.5 Disclosure to Employers, Educational Institutions and Sponsoring Organisations

Where reasonably necessary for the provision of the Consultancy Services, the Company may disclose Personal Data to employers, prospective employers, educational institutions, licensing authorities, sponsoring organisations, scholarship providers or other organisations directly connected with the immigration process for the purpose of obtaining confirmations, completing formalities, verifying documents or facilitating the relevant application.

14.6 Disclosure to Third-Party Service Providers

The Company may disclose Personal Data to Third-Party Service Providers engaged for assisting in the provision of the Consultancy Services, including translators, interpreters, document verification agencies, notaries, apostille service providers, courier agencies, payment gateway providers, cloud service providers, information technology service providers, cybersecurity consultants, legal advisers, chartered accountants, auditors and other professional advisers.

The Company shall endeavour, wherever reasonably practicable, to ensure that such persons remain subject to appropriate contractual, statutory or professional obligations of confidentiality.

14.7 Disclosure with the Consent or Instructions of the Client

The Company may disclose Personal Data where the Client or the Data Principal has expressly instructed, authorised or requested the Company to communicate with any specified individual, organisation or Government Authority or has otherwise consented to such disclosure in accordance with Applicable Law.

The Company shall be entitled to rely upon such instructions unless it has actual knowledge that the same are unlawful or have been validly withdrawn.

14.8 Disclosure for Compliance with Legal Obligations

The Company may disclose Personal Data where such disclosure is reasonably necessary for complying with Applicable Law, responding to judicial proceedings, regulatory investigations, governmental enquiries, statutory audits, taxation requirements, anti-money laundering obligations, Know Your Customer (KYC) requirements or any other legal or regulatory obligation binding upon the Company.

14.9 Disclosure for Protection of Legal Rights

**Rohit
Kaul**
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:33:13
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company may disclose Personal Data where reasonably necessary for establishing, exercising or defending the legal or contractual rights of the Company, its directors, employees, professional advisers or Clients, including disclosures made in connection with arbitration proceedings, judicial proceedings, insurance claims, debt recovery proceedings, regulatory investigations or dispute resolution mechanisms.

14.10 Disclosure During Corporate Transactions

In the event of any merger, amalgamation, demerger, restructuring, acquisition, business transfer, sale of assets, succession, insolvency proceedings or any other corporate transaction affecting the Company, Personal Data may be disclosed to the proposed transferee, successor entity, professional advisers, financial institutions, regulatory authorities or other persons involved in such transaction to the extent reasonably necessary for evaluating, implementing or completing the transaction, subject to Applicable Law.

14.11 Disclosure to Prevent Fraud or Illegal Activities

The Company may disclose Personal Data where it reasonably believes that such disclosure is necessary for preventing fraud, identity theft, document forgery, cybercrime, money laundering, terrorism financing, misuse of immigration processes or any other unlawful activity or for protecting the safety, security, property or lawful interests of the Company, its Clients or any other person.

14.12 Disclosure of Aggregated or Anonymised Information

Nothing contained in this Policy shall prohibit the Company from using or disclosing information that has been anonymised or aggregated in such a manner that no individual can reasonably be identified, provided that such use or disclosure is otherwise consistent with Applicable Law.

14.13 Limitation of Responsibility After Lawful Disclosure

Where Personal Data has been lawfully disclosed by the Company to any Government Authority, Embassy, Consulate, Visa Application Centre, employer, educational institution, Third-Party Service Provider or any other authorised recipient in accordance with this Policy or Applicable Law, the Company shall not be responsible for the manner in which such recipient subsequently stores, processes, retains, transfers or otherwise handles such Personal Data.

The Company shall not be liable for any act, omission, negligence, default, data breach or misuse committed by any independent third party after the lawful disclosure of Personal Data, except to the extent that such liability arises directly from the Company's own wilful misconduct or gross negligence under Applicable Law.

14.14 Restriction on Unauthorised Disclosure

Except as expressly provided in this Policy, the Agreement or Applicable Law, the Company shall not knowingly sell, lease, commercially exploit, publish or otherwise disclose Personal Data to any unauthorised person for marketing, advertising or any unrelated commercial purpose without the lawful authority or consent required under Applicable Law.

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:33:44 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

14.15 Disclosure in Good Faith

Every disclosure of Personal Data undertaken by the Company shall be made in good faith, for a lawful purpose and only to the extent reasonably necessary for achieving the purpose for which the disclosure is made. The Company shall endeavour to implement reasonable safeguards to protect the confidentiality and integrity of Personal Data during the process of disclosure and transmission.

15. CROSS-BORDER TRANSFER OF PERSONAL DATA

15.1 General

The Company acknowledges that the nature of the Consultancy Services provided by it frequently requires the transfer, transmission, disclosure or other lawful processing of Personal Data outside the territorial boundaries of India. Such transfers are an integral part of immigration consultancy, visa consultancy, work permit applications, residence permit applications, permanent residence applications, citizenship applications and other international mobility services provided by the Company.

Accordingly, the Data Principal acknowledges and understands that Personal Data may be transferred to foreign jurisdictions where such transfer is reasonably necessary for the provision of the Consultancy Services, compliance with Applicable Law, fulfilment of contractual obligations or compliance with the documentary requirements prescribed by the relevant foreign Government Authority, Embassy, Consulate, Visa Application Centre or other competent authority.

15.2 Circumstances in which Cross-Border Transfers may be undertaken

The Company may transfer Personal Data outside India where such transfer is reasonably necessary for preparing, submitting, supporting, monitoring or administering immigration, visa, work permit, residence permit, citizenship or any other immigration-related application. Such transfers may also be undertaken where required for document verification, educational credential assessments, employer verification, professional licensing procedures, compliance with foreign immigration requirements, responding to lawful governmental requests or any other lawful purpose directly connected with the Consultancy Services.

15.3 Persons and Organisations to whom Personal Data may be transferred

Subject to Applicable Law, Personal Data may be transferred to Government Authorities, immigration departments, Embassies, High Commissions, Consulates, Visa Application Centres, employers, prospective employers, educational institutions, licensing bodies, credential assessment organisations, medical examination centres, language testing organisations, professional advisers, Third-Party Service Providers, cloud service providers, document verification agencies or any other person or organisation reasonably involved in the immigration process or the provision of the Consultancy Services.

15.4 Compliance with Applicable Law

The Company shall endeavour to ensure that every cross-border transfer of Personal Data undertaken by it complies with Applicable Data Protection Laws, the Digital Personal Data Protection Act, 2023, applicable governmental notifications and every other legal requirement governing international transfers of Personal Data.

Where Applicable Law imposes restrictions upon the transfer of Personal Data to any particular jurisdiction, the Company shall endeavour to comply with such restrictions to the extent applicable to the relevant processing activity.

15.5 Acknowledgement by the Data Principal

The Data Principal expressly acknowledges that immigration consultancy services cannot ordinarily be provided without transmitting Personal Data to authorities and organisations situated outside India. By engaging the Company and requesting the Consultancy Services, the Data Principal acknowledges that such international transfers constitute an essential component of the Engagement and may involve the transmission of passports, visa records, educational documents, employment records, financial information, declarations, supporting documents and other Personal Data reasonably necessary for the relevant immigration process.

15.6 Security Measures During Cross-Border Transfer

The Company shall endeavour to implement reasonable technical, organisational and administrative safeguards designed to protect Personal Data during international transmission. Such safeguards may include secure electronic communication channels, encrypted file transmission, password-protected documents, secure cloud storage solutions, controlled access mechanisms, confidentiality obligations applicable to personnel and such other security measures as the Company may consider appropriate having regard to the nature of the Personal Data being transferred.

The Company does not, however, warrant that electronic transmission of information over international communication networks shall be completely secure or free from interception, cyber threats or technological failures.

15.7 Foreign Laws and Regulatory Requirements

The Data Principal acknowledges that once Personal Data is lawfully transferred to a foreign jurisdiction, such Personal Data may become subject to the laws, regulations, governmental powers, judicial processes and administrative procedures of that jurisdiction. The Company shall not be responsible for any lawful disclosure, processing, retention or use of such Personal Data by a foreign Government Authority or any other competent authority acting in accordance with the laws of the relevant jurisdiction.

15.8 Processing by Foreign Third Parties

Where Personal Data is lawfully transferred to any foreign employer, educational institution, Embassy, Consulate, Government Authority, Visa Application Centre, professional adviser or other independent third party, the Company shall not be responsible for the subsequent collection, storage, processing, disclosure, retention, transfer or destruction of such Personal Data by such recipient after the lawful transfer has been completed.

15.9 Client's Responsibility

The Client acknowledges that the successful processing of immigration and visa applications frequently depends upon the timely transfer of Personal Data to foreign authorities and other authorised organisations. The Client shall cooperate with the Company by providing complete, accurate and updated information and shall promptly execute every consent, declaration, authorisation or other document reasonably required for facilitating such international transfer.

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:34:53 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

Any delay, refusal or failure by the Client to provide the information or authorisations reasonably required for cross-border transfer may adversely affect the Company's ability to provide the Consultancy Services, and the Company shall not be liable for any delay, rejection, suspension or adverse consequence arising therefrom.

15.10 Restriction on Unauthorised Cross-Border Transfers

The Company shall not knowingly transfer Personal Data outside India for purposes unrelated to the Consultancy Services or in a manner prohibited by Applicable Law. Every international transfer undertaken by the Company shall be limited to the extent reasonably necessary for the lawful purpose for which such transfer is made and shall be carried out in good faith and in accordance with this Policy.

15.11 Reservation of Rights

Nothing contained in this Clause shall require the Company to undertake any cross-border transfer of Personal Data where such transfer is prohibited under Applicable Law, restricted by governmental directions, technically impracticable, inconsistent with the Company's professional obligations or otherwise considered inappropriate by the Company acting reasonably and in good faith.

16. DATA SECURITY MEASURES

16.1 General

The Company recognises that the security of Personal Data is an essential component of responsible corporate governance and the provision of professional Consultancy Services. Accordingly, the Company shall endeavour to implement and maintain appropriate technical, organisational, physical, contractual and administrative safeguards designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised access, unauthorised disclosure, misuse, theft, corruption or any other form of unlawful or unauthorised processing.

The Company shall periodically review its information security practices and, where considered appropriate, update its security measures having regard to technological developments, operational requirements, recognised industry practices, cybersecurity risks and Applicable Law.

16.2 Security Governance

The Company shall establish and maintain internal procedures governing the secure collection, storage, use, transmission, retention and disposal of Personal Data processed in connection with the Consultancy Services. Such procedures may include documented operational practices, access control mechanisms, document handling procedures, employee responsibilities, internal approvals, audit mechanisms and such other governance measures as the Company considers reasonably necessary for protecting Personal Data.

16.3 Access Controls

Access to Personal Data shall be restricted to directors, officers, employees, consultants, interns, authorised representatives and Third-Party Service Providers who require such access for the lawful performance of their duties in connection with the Consultancy Services.

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:35:26 +05'30'

Office No 102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company shall endeavour to implement role-based access controls and other reasonable measures to minimise unauthorised access to Personal Data and to ensure that access is granted only on a legitimate business need basis.

16.4 Physical Security Measures

Where Personal Data is maintained in physical form, the Company shall endeavour to store such records in secure premises using appropriate physical safeguards including controlled access, secure filing systems, restricted storage areas, visitor management procedures and such other reasonable measures as the Company considers appropriate having regard to the sensitivity of the information concerned.

The Company shall also endeavour to ensure that physical documents containing Personal Data are protected against theft, accidental loss, unauthorised copying, tampering or destruction.

16.5 Electronic Security Measures

Where Personal Data is maintained electronically, the Company shall endeavour to implement reasonable safeguards including secure servers, password protection, authentication mechanisms, user access controls, system monitoring, firewall protection, anti-malware software, secure backups, audit logs and other information security measures appropriate to the nature of the systems used by the Company.

The Company may periodically upgrade, replace or modify its technological safeguards in order to improve the security of its information systems.

16.6 Secure Storage of Client Documents

The Company shall endeavour to maintain Personal Data and supporting documents submitted by Clients in a secure manner throughout the duration of the Engagement and for such additional period as may be required under this Policy, the Agreement or Applicable Law.

Original documents, certified copies, electronic records and scanned documents shall be handled with reasonable care and stored in accordance with the Company's operational procedures and document management practices.

16.7 Internal Monitoring and Review

The Company may periodically review its security practices, document management procedures, access controls, technological safeguards and operational processes with a view to identifying vulnerabilities, strengthening internal controls and improving the overall protection of Personal Data.

Nothing contained herein shall oblige the Company to conduct any particular audit or review at any specified interval unless required by Applicable Law.

16.8 Employee Awareness and Confidentiality

The Company shall endeavour to ensure that directors, officers, employees, consultants, interns and other authorised personnel handling Personal Data are made aware of their confidentiality obligations and are expected to comply with the Company's privacy, information security and confidentiality requirements while performing their respective responsibilities.

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:35:58
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company may provide internal guidance, operational procedures, instructions or training relating to the secure handling of Personal Data whenever considered appropriate.

16.9 Security of Electronic Communications

Where Personal Data is transmitted through electronic mail, secure client portals, cloud-based platforms, messaging applications or other electronic communication channels, the Company shall endeavour to adopt reasonable safeguards appropriate to the nature of the communication.

The Client acknowledges that no method of electronic communication or internet transmission can be guaranteed to be completely secure and that electronic communications may be exposed to risks beyond the reasonable control of the Company.

16.10 Business Continuity and Data Recovery

The Company may maintain appropriate backup procedures, disaster recovery arrangements, document recovery processes and business continuity measures designed to minimise disruption to its operations and to facilitate the recovery of Personal Data following accidental loss, system failure, cyber incidents, natural disasters or other unforeseen events.

The existence of such measures shall not constitute a guarantee that every item of Personal Data can always be fully restored following a security incident.

16.11 Security Incident Response

Where the Company becomes aware of any actual or reasonably suspected compromise affecting the confidentiality, integrity or availability of Personal Data, the Company shall endeavour to investigate the matter promptly, implement reasonable containment measures, assess the nature and extent of the incident and take such further steps as may be considered appropriate under Applicable Law, including notifications where legally required.

The Company's response to any security incident shall depend upon the facts and circumstances of the particular incident, the nature of the Personal Data involved and the requirements of Applicable Law.

16.12 No Absolute Guarantee of Security

While the Company shall endeavour to implement reasonable and appropriate safeguards for protecting Personal Data, the Company does not represent or warrant that its systems, networks, servers, electronic communications, cloud infrastructure or information technology environment are completely immune from cyberattacks, hacking, malware, ransomware, phishing, unauthorised access, technological failures, force majeure events or other security incidents beyond the reasonable control of the Company.

Accordingly, except to the extent prohibited by Applicable Law or resulting directly from the Company's wilful misconduct or gross negligence, the Company shall not be liable for any loss, corruption, unauthorised disclosure, alteration, destruction or compromise of Personal Data arising from events beyond its reasonable control despite the implementation of reasonable security measures.

16.13 Continuous Improvement

**Rohit
Kaul**
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:36:30
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company acknowledges that information security is an evolving process requiring continuous monitoring and improvement. Accordingly, the Company reserves the right to modify, strengthen, replace or update its technical, organisational, contractual and administrative security measures from time to time in response to changes in technology, cybersecurity risks, operational requirements, recognised industry practices or Applicable Law, without the necessity of obtaining any separate consent from the Client or the Data Principal, provided that such modifications remain consistent with Applicable Law.

17. ENCRYPTION AND CYBERSECURITY MEASURES

17.1 General

The Company recognises that the increasing use of digital platforms, electronic communication systems, cloud computing technologies and online document management systems exposes Personal Data to evolving cybersecurity risks. Accordingly, the Company shall endeavour to implement reasonable technological safeguards designed to preserve the confidentiality, integrity, availability and resilience of the information systems used for processing Personal Data.

The cybersecurity measures adopted by the Company shall be proportionate to the nature of its business operations, the sensitivity of the Personal Data processed, the volume of information handled, the reasonably foreseeable cybersecurity risks and the technological resources available to the Company.

17.2 Encryption of Personal Data

Where considered reasonably appropriate having regard to the sensitivity of the Personal Data and the technological infrastructure of the Company, the Company may utilise encryption technologies or other equivalent security mechanisms for protecting Personal Data during electronic storage, electronic transmission or other forms of digital processing.

The Company reserves the right to determine the nature, extent and method of encryption appropriate for its operations and may modify such measures from time to time in accordance with technological developments and recognised industry practices.

17.3 Secure Electronic Transmission

Where Personal Data is transmitted electronically to Clients, Government Authorities, Embassies, Consulates, Visa Application Centres, Third-Party Service Providers or other authorised recipients, the Company shall endeavour to use secure communication channels, password-protected documents, encrypted file-sharing mechanisms, secure client portals or other reasonable methods designed to reduce the risk of unauthorised interception or disclosure during transmission.

The Company does not, however, guarantee that electronic transmission over the internet or other communication networks is completely secure or immune from interception, cyberattacks or technological failures beyond its reasonable control.

17.4 Cybersecurity Controls

The Company may implement appropriate cybersecurity controls including authentication procedures, password management systems, access control mechanisms, firewall protection,

**Rohit
Kaul**
Digitally signed
by Rohit Kaul
Date: 2026.07.17
17:37:04 +05'30'

Your Personal Consultancy | Trade Advisor
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

anti-virus and anti-malware software, endpoint security measures, system monitoring tools, intrusion detection mechanisms, vulnerability management practices, secure backup solutions and other technological safeguards considered appropriate for protecting the Company's information systems.

The specific cybersecurity controls implemented by the Company may vary from time to time depending upon technological developments, operational requirements and recognised industry practices.

17.5 User Authentication

The Company shall endeavour to restrict access to electronic systems containing Personal Data through appropriate authentication mechanisms, including user credentials, passwords, multi-factor authentication, role-based permissions or other security measures considered appropriate by the Company.

Every authorised user accessing the Company's systems shall be responsible for maintaining the confidentiality of login credentials assigned to such user and shall not knowingly disclose such credentials to any unauthorised person.

17.6 System Monitoring

The Company may monitor, log and review access to its information technology systems, electronic communication platforms, document management systems and other technological resources for the purposes of maintaining system security, detecting unauthorised access, investigating security incidents, maintaining audit trails, preventing fraud and ensuring compliance with internal security requirements.

Such monitoring shall be undertaken solely for lawful business purposes and in accordance with Applicable Law.

17.7 Remote Access and Electronic Devices

Where directors, employees, consultants or authorised personnel access Personal Data through laptops, mobile devices, tablets, remote desktop solutions, cloud-based applications or other electronic devices, the Company may prescribe reasonable security requirements relating to authentication, password protection, software updates, secure internet connectivity and access controls to minimise cybersecurity risks.

Authorised personnel shall exercise reasonable care to prevent unauthorised access to Company devices, electronic records and Personal Data while working remotely or outside the Company's premises.

17.8 Cybersecurity Incident Management

Where the Company becomes aware of any actual or reasonably suspected cyber incident affecting the confidentiality, integrity or availability of Personal Data or the Company's information systems, the Company shall endeavour to promptly assess the nature and scope of the incident, implement appropriate containment measures, preserve relevant evidence where appropriate, initiate remedial actions and comply with any notification obligations imposed under Applicable Law.

Nothing contained herein shall require the Company to disclose information relating to its internal cybersecurity architecture, security controls or incident response procedures where such disclosure may itself compromise the security of the Company's systems or expose the Company to additional cybersecurity risks.

17.9 Security Updates and Technological Improvements

The Company reserves the right to implement software updates, security patches, system upgrades, infrastructure improvements, hardware replacements, cybersecurity enhancements and other technological modifications considered reasonably necessary for improving the security of its information systems and protecting Personal Data against evolving cyber threats.

Such updates may be implemented without prior notice where the Company considers immediate action necessary for maintaining system security or complying with Applicable Law.

17.10 Responsibility of Clients

The Client shall also exercise reasonable care while transmitting Personal Data to the Company and shall use secure communication methods wherever reasonably practicable. The Client shall be responsible for maintaining the confidentiality of passwords, login credentials, authentication codes and other security information provided for accessing the Company's website, client portal or other electronic platforms.

The Company shall not be responsible for any unauthorised disclosure of Personal Data resulting directly from the Client's failure to maintain appropriate security over the Client's own devices, communication systems or login credentials.

17.11 Third-Party Technology Providers

The Company may utilise third-party software platforms, cloud infrastructure providers, communication platforms, document management systems, cybersecurity service providers or other technology vendors for supporting its business operations and the provision of the Consultancy Services.

The Company shall endeavour to engage reputable service providers and to implement appropriate contractual safeguards wherever reasonably practicable. However, the Company shall not warrant that the independent information technology systems operated by such third parties are entirely free from vulnerabilities, service interruptions or cybersecurity incidents beyond the Company's reasonable control.

17.12 No Absolute Cybersecurity Guarantee

The Company acknowledges that cybersecurity threats continue to evolve and that no technological system, software application, cloud platform, communication network or electronic infrastructure can be guaranteed to be completely secure. Accordingly, while the Company shall endeavour to implement reasonable cybersecurity safeguards consistent with recognised industry practices, the Company does not guarantee absolute protection against hacking, malware, ransomware, phishing attacks, denial-of-service attacks, unauthorised access, data corruption, technological failures, force majeure events or other cybersecurity incidents beyond its reasonable control.

Except to the extent prohibited by Applicable Law or arising directly from the Company's wilful misconduct or gross negligence, the Company shall not be liable for losses arising solely from such events despite the implementation of reasonable cybersecurity measures.

18. CONFIDENTIALITY OBLIGATIONS OF EMPLOYEES, CONSULTANTS AND AUTHORISED PERSONNEL

18.1 General

The Company recognises that every director, officer, employee, consultant, intern, contractual personnel, authorised representative, advisor and every other person engaged by or acting on behalf of the Company may, during the course of their duties, obtain access to Personal Data and Confidential Information entrusted to the Company by Clients, Data Principals, Government Authorities, Embassies, Consulates, Visa Application Centres, employers, educational institutions and other authorised persons. The Company accordingly requires every such individual to maintain the highest standards of confidentiality, integrity, professionalism and due care while handling Personal Data and to ensure that such information is used solely for lawful purposes connected with the performance of their assigned duties.

18.2 Confidentiality Obligations

Every person authorised to access Personal Data shall maintain strict confidentiality with respect to such information and shall not disclose, communicate, reproduce, copy, transmit, publish, distribute or otherwise make available any Personal Data to any unauthorised person except where such disclosure is expressly authorised by the Company, required for the performance of official duties or otherwise permitted under Applicable Law.

The obligation of confidentiality shall extend to every form of Personal Data, irrespective of whether such information exists in physical form, electronic records, cloud-based systems, emails, instant messaging platforms, scanned documents, photographs, audio recordings, video recordings or any other medium.

18.3 Need-to-Know Principle

Access to Personal Data shall be granted strictly on a "need-to-know" basis. No employee, consultant, intern, authorised representative or other personnel shall access, retrieve, review or process Personal Data unless such access is reasonably necessary for the discharge of his or her official responsibilities or for providing the Consultancy Services.

The Company reserves the right to determine the extent of access that may be granted to any individual having regard to the nature of his or her duties, operational requirements, security considerations and the sensitivity of the Personal Data concerned.

18.4 Use of Personal Data

Personal Data accessed by authorised personnel shall be used solely for lawful business purposes directly connected with the provision of the Consultancy Services, compliance with Applicable Law, performance of contractual obligations or other purposes authorised by the Company.

**Rohit
Kaul**
Digitally
signed by
Rohit Kaul
Date:
2026.07.17
17:38:46
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

No person acting on behalf of the Company shall use Personal Data for personal benefit, commercial gain, private business, unauthorised research, personal curiosity or any purpose unrelated to the official responsibilities assigned by the Company.

18.5 Handling of Client Documents

Every employee and authorised person shall exercise reasonable care while handling passports, visas, educational certificates, financial records, police clearance certificates, medical reports, immigration documents, declarations, affidavits and every other document entrusted to the Company.

Such documents shall not be removed from authorised storage locations, copied, photographed, scanned, forwarded or otherwise reproduced except where reasonably necessary for the provision of the Consultancy Services or expressly authorised by the Company.

18.6 Electronic Information

Authorised personnel accessing Personal Data through computers, laptops, mobile devices, cloud-based platforms, document management systems or electronic communication platforms shall exercise reasonable care to prevent unauthorised access, accidental disclosure, loss or corruption of such information.

Employees shall not knowingly store Company records containing Personal Data on personal devices, personal cloud storage accounts, unauthorised external storage media or any system not approved by the Company except with prior written authorisation.

18.7 Passwords and Access Credentials

Every authorised user shall maintain the confidentiality of passwords, authentication credentials, security tokens and other access mechanisms issued by the Company.

No employee or authorised person shall intentionally disclose login credentials to any other individual or permit unauthorised access to the Company's information systems.

18.8 Reporting of Security Concerns

Every employee, consultant or authorised representative shall promptly report to the Company any actual or suspected unauthorised access, accidental disclosure, cyber incident, loss of documents, theft of electronic devices, suspected fraud or any other incident that may compromise the confidentiality, integrity or availability of Personal Data.

No employee shall intentionally conceal any security incident involving Personal Data.

18.9 Return of Company Property

Upon resignation, retirement, termination of employment, completion of consultancy services or cessation of engagement for any reason whatsoever, every employee, consultant, intern, contractor or authorised representative shall immediately return to the Company every file, document, electronic record, storage device, access credential, identity card, laptop, mobile device, password, client record and every other item belonging to or containing information relating to the Company or its Clients.

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:39:26 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The departing individual shall not retain copies of Personal Data except where expressly authorised in writing or required under Applicable Law.

18.10 Continuing Confidentiality

The obligation to maintain confidentiality shall survive the resignation, retirement, termination, completion or cessation of employment, consultancy, internship or any other engagement with the Company.

No former employee or consultant shall disclose or use Personal Data obtained during the course of his or her engagement except where such disclosure is required under Applicable Law or expressly authorised in writing by the Company.

18.11 Disciplinary Action

Any unauthorised access, misuse, disclosure, copying, retention, destruction or other improper handling of Personal Data by any employee, consultant, intern, contractor or authorised representative may result in disciplinary action, suspension, termination of employment or engagement, recovery of losses, legal proceedings or any other action available to the Company under the Agreement or Applicable Law.

18.12 Company's Rights

Nothing contained in this Clause shall restrict the Company's right to monitor access to its information systems, investigate suspected breaches of confidentiality, suspend access privileges, recover Company property or take such other action as may be considered reasonably necessary for protecting Personal Data and safeguarding the legitimate interests of the Company and its Clients.

19. THIRD-PARTY SERVICE PROVIDERS AND DATA PROCESSORS

19.1 General

The Company may, in the ordinary course of its business, engage Third-Party Service Providers, professional advisers and Data Processors for assisting in the provision of the Consultancy Services or supporting the Company's business operations. Such engagements may include information technology support, cloud computing services, document management services, payment processing, courier services, translation services, notarisation, apostille assistance, document verification, cybersecurity services, accounting services, legal advisory services and other professional or administrative functions.

19.2 Engagement of Third Parties

The Company shall exercise reasonable care while selecting Third-Party Service Providers and shall endeavour to engage persons or organisations possessing appropriate expertise, professional competence and operational capability for the services to be provided.

Nothing contained herein shall be construed as imposing upon the Company any obligation to guarantee the performance, financial stability or continued operation of any independent Third-Party Service Provider.

19.3 Disclosure of Personal Data

**Rohit
Kaul**
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:40:08 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company may disclose Personal Data to Third-Party Service Providers only to the extent reasonably necessary for the performance of the specific services for which such provider has been engaged.

The Company shall endeavour to limit such disclosure to the minimum amount of Personal Data reasonably required for the relevant purpose.

19.4 Confidentiality Obligations

Where reasonably practicable, the Company shall endeavour to ensure that Third-Party Service Providers receiving Personal Data are subject to appropriate contractual, statutory or professional obligations requiring them to maintain the confidentiality of such information and to process Personal Data only for authorised purposes.

19.5 Processing Instructions

Third-Party Service Providers shall ordinarily process Personal Data only in accordance with the lawful instructions issued by the Company, the applicable contractual arrangements and Applicable Law.

The Company may periodically review its relationships with Third-Party Service Providers and may modify, suspend or terminate such engagements whenever considered appropriate.

19.6 Independent Third Parties

The Client acknowledges that certain organisations involved in the immigration process, including Government Authorities, Embassies, Consulates, Visa Application Centres, educational institutions, employers, licensing bodies and foreign governmental agencies, operate independently of the Company.

The Company shall not be responsible for the internal privacy practices, security procedures or data processing activities adopted by such independent organisations after Personal Data has been lawfully disclosed to them.

19.7 Cross-Border Service Providers

Certain Third-Party Service Providers engaged by the Company may be situated outside India or may process Personal Data using information technology infrastructure located outside India.

Where reasonably necessary for the provision of the Consultancy Services, the Company may permit such processing in accordance with this Policy and Applicable Law.

19.8 Responsibility of Third-Party Service Providers

Every Third-Party Service Provider engaged by the Company shall remain independently responsible for complying with the legal and contractual obligations applicable to its own business operations.

Nothing contained in this Policy shall be construed as creating an employer-employee relationship, agency relationship or partnership between the Company and any independent Third-Party Service Provider unless expressly agreed in writing.

19.9 Suspension or Replacement

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2025.07.17
17:40:40

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company reserves the right, at its sole discretion, to appoint, replace, remove, suspend or discontinue any Third-Party Service Provider whenever considered necessary for operational, commercial, legal, security or regulatory reasons without obtaining separate approval from the Client, provided that such action does not materially prejudice the lawful provision of the Consultancy Services.

19.10 Limitation of Liability

While the Company shall endeavour to engage competent and reliable Third-Party Service Providers, it does not warrant or guarantee that every independent service provider shall at all times remain free from operational failures, technological disruptions, cybersecurity incidents, human error or other events beyond the Company's reasonable control.

Accordingly, except to the extent arising directly from the Company's own wilful misconduct or gross negligence or where otherwise prohibited by Applicable Law, the Company shall not be liable for any act, omission, negligence, default or data security incident attributable solely to an independent Third-Party Service Provider after Personal Data has been lawfully disclosed in accordance with this Policy.

19.11 Survival

The engagement, replacement or cessation of any Third-Party Service Provider shall not affect the continued applicability of this Policy, the confidentiality obligations contained herein or any statutory obligation relating to the protection of Personal Data.

20. RECORD RETENTION

20.1 General

The Company recognises that the retention of Personal Data constitutes an essential component of the efficient administration of its business, the provision of Consultancy Services, compliance with Applicable Law, protection of legal rights and maintenance of professional records. Accordingly, the Company shall retain Personal Data only for such period as is reasonably necessary for the lawful purposes for which such Personal Data was collected, processed or otherwise received and shall thereafter securely archive, anonymise, erase or destroy such Personal Data in accordance with this Policy and Applicable Law.

The Company shall endeavour to ensure that the retention of Personal Data remains proportionate to the nature of the Consultancy Services, the contractual relationship between the Parties, statutory obligations, regulatory requirements and the legitimate operational needs of the Company.

20.2 Purpose of Retention

The Company may retain Personal Data for one or more of the following purposes, namely, the continued provision of Consultancy Services, completion of immigration or visa applications, compliance with Applicable Law, maintenance of professional records, responding to communications received from Government Authorities, defending legal proceedings, exercising contractual rights, resolving disputes, conducting audits, complying with taxation requirements, maintaining accounting records, preventing fraud, complying with regulatory inspections and such other lawful purposes as may reasonably justify continued retention.

20.3 Categories of Records

Without limiting the generality of this Clause, the Company may retain passports, visa documents, immigration applications, educational records, employment records, financial information, taxation documents, declarations, affidavits, correspondence, electronic communications, invoices, receipts, payment records, consultation notes, internal file notes, compliance records, document verification reports, appointment confirmations, client instructions and every other record generated or received during the course of the Engagement.

20.4 Retention Period

The period for which Personal Data is retained shall depend upon the nature of the Personal Data, the Consultancy Services provided, the applicable statutory limitation periods, regulatory requirements, contractual obligations, pending proceedings and the legitimate business interests of the Company.

The Company reserves the right to determine appropriate retention periods for different categories of records and may revise such periods from time to time having regard to Applicable Law, operational requirements and recognised industry practices.

20.5 Ongoing Engagements

Where the Engagement remains active or where any immigration, visa, residence permit, work permit, permanent residence or citizenship application continues to remain pending before any Government Authority, Embassy, Consulate, Visa Application Centre or other competent authority, the Company may continue to retain and process Personal Data until the relevant Engagement has been completed or otherwise closed.

20.6 Legal and Regulatory Requirements

The Company may continue to retain Personal Data beyond the completion of the Consultancy Services where such retention is reasonably necessary for complying with Applicable Law, judicial directions, Government notifications, taxation requirements, regulatory obligations, statutory audits, investigations, inspections or any lawful request issued by a competent authority.

20.7 Pending Disputes

Where any legal proceeding, arbitration, mediation, regulatory investigation, complaint, disciplinary proceeding, insurance claim or contractual dispute is pending or reasonably anticipated, the Company may retain relevant Personal Data until the final conclusion of such proceedings and the expiry of any applicable limitation period.

20.8 Archived Records

The Company may archive Personal Data that is no longer required for day-to-day business operations but which continues to require retention for legal, regulatory, historical, evidentiary or operational purposes.

Archived records shall remain subject to appropriate access controls and confidentiality safeguards.

20.9 Periodic Review

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
17:42:18 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company may periodically review the Personal Data retained in its records with a view to determining whether continued retention remains reasonably necessary having regard to Applicable Law, contractual obligations and operational requirements.

Where the Company determines that continued retention is no longer justified, the Company may securely erase, anonymise or destroy the relevant Personal Data in accordance with this Policy.

20.10 No Obligation to Retain Indefinitely

Nothing contained in this Policy shall require the Company to retain Personal Data indefinitely.

Subject to Applicable Law, the Company reserves the right to securely archive, anonymise, erase or destroy Personal Data after the expiry of the applicable retention period without issuing any separate notice to the Client or the Data Principal.

20.11 Company's Discretion

The Company shall retain the sole discretion to determine the appropriate method, duration and manner of retention of Personal Data, provided that such discretion is exercised reasonably, in good faith and consistently with Applicable Law.

21. DATA ARCHIVAL, ERASURE AND SECURE DESTRUCTION

21.1 General

The Company recognises that responsible management of Personal Data extends beyond its collection and use and includes the lawful archival, anonymisation, erasure and secure destruction of Personal Data once such information is no longer required for the purposes specified in this Policy or under Applicable Law.

Accordingly, the Company shall endeavour to implement reasonable procedures governing the secure disposal of Personal Data while maintaining due regard to legal obligations, contractual commitments, regulatory requirements and recognised information security practices.

21.2 Archival of Records

Where Personal Data is no longer required for active business operations but must continue to be retained for legal, regulatory, contractual or historical purposes, the Company may archive such information in secure physical or electronic repositories.

Archived records shall remain subject to appropriate access restrictions and shall ordinarily be accessible only to authorised personnel having a legitimate business requirement.

21.3 Erasure of Personal Data

Where the lawful basis for retaining Personal Data has ceased to exist and no statutory, contractual or regulatory obligation requires continued retention, the Company may erase such Personal Data from its active records and information systems.

Erasure may be carried out manually, electronically or through such other lawful methods as the Company considers appropriate.

21.4 Anonymisation

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

Rohit
Digitally signed
by Rohit Kaul
Date: 2026.07.17
17:43:00 +05'30'

Kaul

Where considered appropriate, the Company may anonymise Personal Data so that the information can no longer reasonably identify any individual.

Once Personal Data has been effectively anonymised, the resulting information may continue to be retained and used by the Company for lawful business purposes, statistical analysis, operational improvement, internal research or compliance activities, subject to Applicable Law.

21.5 Secure Destruction of Physical Records

Physical documents containing Personal Data may be securely destroyed by shredding, pulping, incineration or such other secure destruction methods as the Company considers reasonably appropriate having regard to the nature of the records and recognised industry practices.

The Company shall endeavour to ensure that destroyed documents cannot reasonably be reconstructed or retrieved.

21.6 Secure Destruction of Electronic Records

Electronic records containing Personal Data may be securely deleted, overwritten, destroyed, anonymised or otherwise rendered inaccessible through technological methods considered reasonably appropriate by the Company.

The Company does not guarantee that every residual copy stored within backup systems, disaster recovery environments or historical archives can be immediately eliminated where retention remains necessary for legitimate operational or legal reasons.

21.7 Destruction by Third-Party Service Providers

Where Personal Data is stored or processed by Third-Party Service Providers on behalf of the Company, the Company may require such service providers to securely return, erase or destroy the Personal Data upon completion of the relevant services, subject to Applicable Law and the applicable contractual arrangements.

21.8 Exceptions

Nothing contained in this Clause shall require the Company to erase or destroy Personal Data where continued retention is reasonably necessary for complying with Applicable Law, defending legal proceedings, exercising contractual rights, responding to Government Authorities, maintaining accounting records, complying with taxation requirements or protecting the legitimate interests of the Company.

21.9 Requests by Data Principals

Any request by a Data Principal seeking erasure or deletion of Personal Data shall be considered by the Company in accordance with Applicable Data Protection Laws, the Agreement and the Company's legal obligations.

The Company reserves the right to refuse or defer such request where continued retention of the Personal Data is authorised or required under Applicable Law or reasonably necessary for the purposes specified in this Policy.

21.10 Destruction Schedule

The Company may establish and periodically revise internal schedules governing the archival, anonymisation, erasure and secure destruction of different categories of records having regard to the nature of the Personal Data, applicable retention periods, legal obligations and recognised industry practices.

22. COOKIES AND SIMILAR TECHNOLOGIES

22.1 General

The Company may utilise cookies, web beacons, pixels, software development kits (SDKs), session identifiers, local storage technologies, log files and other similar technologies (collectively referred to in this Clause as "Cookies") in connection with the operation of its Website, client portal, mobile applications and other digital platforms. Such technologies are intended to improve the functionality, security, efficiency and user experience of the Company's electronic platforms and to facilitate the lawful provision of the Consultancy Services.

The Company shall endeavour to ensure that the use of Cookies is consistent with Applicable Law and this Policy.

22.2 Purpose of Cookies

The Company may use Cookies for one or more lawful purposes, including—

- 22.2.1** identifying returning visitors and maintaining user sessions;
- 22.2.2** authenticating users accessing secured portions of the Company's Website or client portal;
- 22.2.3** improving the performance, functionality and reliability of the Company's electronic platforms;
- 22.2.4** analysing Website usage patterns and user behaviour for internal business purposes;
- 22.2.5** maintaining system security and detecting unauthorised access or suspicious activities;
- 22.2.6** preventing fraud and protecting the integrity of the Company's electronic systems;
- 22.2.7** remembering user preferences, language selections and other Website settings;
- 22.2.8** generating statistical reports relating to Website performance;
- 22.2.9** improving the quality of the Consultancy Services and the Company's digital platforms; and
- 22.2.10** every other lawful purpose reasonably connected with the administration, maintenance or improvement of the Company's electronic services.

22.3 Types of Cookies

Depending upon the functionality of the Company's electronic platforms, the Company may use essential cookies, functional cookies, session cookies, persistent cookies, security cookies, performance cookies, analytics cookies or other similar technologies considered reasonably necessary for the operation of the Website and the provision of the Consultancy Services.

The Company reserves the right to modify, update, replace or discontinue its Cookie practices at any time having regard to technological developments, operational requirements, recognised industry practices or changes in Applicable Law.

23. WEBSITE PRIVACY

23.1 General

This Clause governs the collection, use, processing and protection of Personal Data through the Company's official Website, client portal, online enquiry forms, appointment booking systems, electronic communication platforms and every other digital platform owned, operated or controlled by the Company.

The use of the Company's Website shall constitute acceptance of this Policy to the extent applicable to the processing of Personal Data through such electronic platforms.

23.2 Information Submitted Through the Website

Visitors may voluntarily submit Personal Data through contact forms, enquiry forms, consultation requests, appointment booking facilities, document upload portals, client registration forms, newsletter subscriptions, feedback forms, electronic communications or any other interactive feature available on the Company's Website.

The Company shall process such information only for the lawful purposes connected with responding to enquiries, providing Consultancy Services, communicating with prospective Clients, administering appointments or otherwise conducting its legitimate business operations.

23.3 Website Security

The Company shall endeavour to implement reasonable technical and organisational safeguards for protecting Personal Data collected through the Website against unauthorised access, accidental disclosure, alteration, misuse, corruption or destruction.

Notwithstanding the foregoing, the Company does not represent or warrant that the Website, internet communications or electronic transmissions are completely secure or immune from cyberattacks, hacking, malware, phishing, denial-of-service attacks, technological failures or other events beyond the Company's reasonable control.

23.4 Online Communications

Electronic communications transmitted through the Company's Website, online contact forms or email systems may not always be encrypted during transmission over public communication networks. Accordingly, users should exercise reasonable caution while transmitting highly sensitive information electronically and should follow any secure communication procedures prescribed by the Company.

23.5 User Responsibilities

Every visitor using the Company's Website shall—

23.5.1 provide accurate, complete and truthful information;

23.5.2 refrain from uploading false, misleading, unlawful, defamatory or malicious content;

23.5.3 not knowingly introduce viruses, malware, ransomware or any other harmful software into the Company's electronic systems;

23.5.4 not attempt to obtain unauthorised access to the Company's servers, databases, client portals or information systems;

23.5.5 comply with Applicable Law while accessing or using the Website; and

23.5.6 use the Website solely for lawful purposes.

23.6 External Links

The Company's Website may contain hyperlinks to websites, applications or digital platforms operated by independent third parties solely for the convenience of users.

The Company neither controls nor assumes responsibility for the privacy practices, security standards, accuracy, availability or content of such external websites. Users accessing third-party websites shall do so entirely at their own discretion and shall remain subject to the terms and privacy policies applicable to such websites.

23.7 Third-Party Services

The Company may integrate its Website with third-party payment gateways, communication platforms, scheduling systems, cloud infrastructure, mapping services, analytics providers or other technological services for facilitating the Consultancy Services.

The Company shall endeavour to engage reputable service providers; however, the Company shall not be responsible for the independent acts, omissions, security practices or privacy policies of such third-party providers.

23.8 Website Availability

The Company does not warrant that its Website shall remain continuously available or free from interruptions, technical failures, maintenance downtime, software defects or communication errors.

The Company reserves the right to suspend, modify, restrict or discontinue any portion of its Website without prior notice where reasonably necessary for maintenance, security, technological upgrades, legal compliance or operational requirements.

23.9 Intellectual Property

Nothing contained in this Policy shall be construed as granting any right, title or interest in the intellectual property forming part of the Company's Website. All trademarks, logos, trade names, software, graphics, layouts, text, documents, images and other materials appearing on the Website shall remain the exclusive property of the Company or the respective lawful owner thereof and shall not be copied, reproduced, modified, distributed or otherwise exploited without prior written authorisation.

23.10 Limitation of Liability

Except to the extent prohibited by Applicable Law or arising directly from the Company's wilful misconduct or gross negligence, the Company shall not be liable for any direct, indirect, incidental, consequential or special loss arising out of or in connection with the use of the

Website, interruption of electronic services, unauthorised access by third parties, transmission failures, internet disruptions, cyber incidents or any event beyond the reasonable control of the Company.

23.11 Reservation of Rights

The Company reserves the right to modify, redesign, suspend, replace or permanently discontinue the Website or any feature thereof and to amend the privacy practices applicable to the Website at any time in accordance with Applicable Law.

24. RIGHTS OF DATA PRINCIPALS

24.1 General

The Company recognises that every Data Principal is entitled to certain statutory rights in relation to his or her Personal Data under the Digital Personal Data Protection Act, 2023 and other Applicable Laws. The Company shall endeavour to respect, facilitate and respond to the lawful exercise of such rights in accordance with Applicable Law, this Policy and the legitimate operational requirements of the Company.

The rights recognised under this Clause shall be exercised subject to the conditions, limitations, exceptions and procedural requirements prescribed under Applicable Law and nothing contained in this Policy shall be construed as enlarging, restricting or otherwise modifying any statutory right available to a Data Principal.

24.2 Right to Information

Every Data Principal shall have the right, subject to Applicable Law, to obtain information regarding the processing of his or her Personal Data by the Company.

Without limiting the generality of the foregoing, the Data Principal may request information relating to—

- 24.2.1 the categories of Personal Data processed by the Company;
- 24.2.2 the purposes for which such Personal Data is being processed;
- 24.2.3 the lawful basis upon which such processing is undertaken;
- 24.2.4 the categories of recipients to whom Personal Data has been disclosed;
- 24.2.5 the manner in which the Personal Data has been collected;
- 24.2.6 the period for which such Personal Data is proposed to be retained; and
- 24.2.7 such other information as the Company is required to provide under Applicable Law.

24.3 Right to Access Personal Data

Subject to Applicable Law, a Data Principal may request confirmation as to whether the Company is processing his or her Personal Data and may seek access to such Personal Data in accordance with the procedures prescribed by the Company.

Rohit
Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:14:59 +05'30'

Kaul

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company reserves the right to verify the identity of the requesting individual before providing access to any Personal Data and may refuse or defer any request where identity cannot reasonably be established or where disclosure would be contrary to Applicable Law.

24.4 Right to Correction and Completion

Every Data Principal shall have the right to request correction of inaccurate Personal Data, completion of incomplete Personal Data and updating of Personal Data that has become outdated, subject to verification by the Company and the requirements of Applicable Law.

The Company may require the Data Principal to produce documentary evidence supporting the requested correction before modifying its records.

24.5 Right to Erasure

Subject to Applicable Law, a Data Principal may request the erasure of Personal Data where such information is no longer required for the purpose for which it was collected or where continued processing is otherwise no longer authorised under Applicable Law.

Nothing contained in this Clause shall require the Company to erase Personal Data where continued retention is necessary for complying with Applicable Law, defending legal proceedings, fulfilling contractual obligations, responding to Government Authorities, maintaining professional records or protecting the legitimate interests of the Company.

24.6 Right to Withdraw Consent

Where Personal Data is processed on the basis of consent, the Data Principal shall have the right to withdraw such consent in accordance with Applicable Law and Clause 25 of this Policy.

The withdrawal of consent shall operate prospectively and shall not affect the lawfulness of any processing undertaken prior to the receipt of such withdrawal by the Company.

24.7 Right to Grievance Redressal

Every Data Principal shall have the right to submit complaints, representations or grievances relating to the processing of Personal Data by the Company.

Such grievances shall be addressed through the grievance redressal mechanism established under this Policy and shall ordinarily be examined by the Grievance Officer designated by the Company.

24.8 Right to Nominate

Where recognised under Applicable Law, a Data Principal shall have the right to nominate another individual to exercise such rights as may lawfully survive or become exercisable upon the death or incapacity of the Data Principal.

The Company may require reasonable documentary proof establishing the validity of such nomination before recognising or acting upon any request made by the nominee.

24.9 Right to Fair Processing

**Rohit
Kaul**
Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:15:44
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

Every Data Principal shall be entitled to expect that Personal Data entrusted to the Company shall be processed in a lawful, fair, transparent and responsible manner consistent with the principles set out in this Policy and Applicable Law.

The Company shall endeavour to ensure that Personal Data is processed only for legitimate purposes and only to the extent reasonably necessary for the provision of the Consultancy Services.

24.10 Verification of Requests

Before acting upon any request made under this Clause, the Company may verify the identity of the Data Principal, the authority of any representative acting on behalf of the Data Principal and the authenticity of the request.

The Company may decline to act upon any request which appears fraudulent, vexatious, manifestly unfounded, repetitive, unauthorised or otherwise inconsistent with Applicable Law.

24.11 Circumstances Where Rights May Be Limited

The rights contained in this Clause shall be subject to every exemption, restriction and limitation recognised under Applicable Law.

Without limiting the generality of the foregoing, the Company may refuse, defer or restrict the exercise of any right where—

24.11.1 Applicable Law requires continued processing or retention;

24.11.2 disclosure would adversely affect the rights of another individual;

24.11.3 the Personal Data forms part of ongoing judicial, regulatory or governmental proceedings;

24.11.4 the request would compromise fraud prevention, cybersecurity, information security or regulatory compliance;

24.11.5 identity of the requesting person cannot reasonably be verified;

24.11.6 the request is manifestly excessive, repetitive or abusive;

24.11.7 compliance would prejudice the establishment, exercise or defence of legal rights; or

24.11.8 the Company is otherwise authorised or required under Applicable Law to decline such request.

24.12 Procedure for Exercising Rights

A Data Principal seeking to exercise any right under this Clause shall submit a written request to the Company through such communication channels as may be notified by the Company from time to time.

The Company may prescribe reasonable procedures, documentary requirements, identity verification measures and response mechanisms for dealing with such requests, provided that such procedures remain consistent with Applicable Law.

24.13 No Waiver of Statutory Rights

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:16:21
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

Nothing contained in this Policy shall be interpreted as limiting, excluding or waiving any statutory right available to a Data Principal under the Digital Personal Data Protection Act, 2023 or any other Applicable Law.

Similarly, nothing contained herein shall prevent the Company from relying upon any exemption, defence or statutory protection available to it under Applicable Law.

24.14 Exercise of Rights in Good Faith

The rights recognised under this Clause shall be exercised reasonably and in good faith.

Nothing contained in this Policy shall require the Company to act upon any request that is fraudulent, unlawful, intended to harass the Company, inconsistent with judicial orders or otherwise contrary to Applicable Law.

25. WITHDRAWAL OF CONSENT

25.1 General

Where the processing of Personal Data is based upon the consent of the Data Principal, the Data Principal shall have the right to withdraw such consent at any time in accordance with the provisions of the Digital Personal Data Protection Act, 2023, Applicable Law and this Policy. The Company acknowledges that the withdrawal of consent constitutes a statutory right of the Data Principal and shall endeavour to facilitate the exercise of such right in accordance with Applicable Law.

The withdrawal of consent shall not, however, affect the lawfulness of any collection, use, processing, disclosure, transfer, storage or other processing activity undertaken by the Company prior to the effective receipt of such withdrawal.

25.2 Procedure for Withdrawal

A Data Principal seeking to withdraw consent shall submit a written request to the Company through such communication channels as may be prescribed by the Company from time to time, including electronic mail, the Company's client portal, written correspondence or any other lawful communication mechanism notified by the Company.

The Company may require reasonable information for verifying the identity of the Data Principal before acting upon any request for withdrawal of consent.

25.3 Verification of Identity

Before processing any request for withdrawal of consent, the Company may require the Data Principal or any authorised representative to furnish documentary evidence establishing identity, authority or any other information reasonably necessary for preventing fraud, unauthorised requests or identity theft.

The Company reserves the right to refuse or defer any request where the identity or authority of the requesting individual cannot reasonably be established.

25.4 Effective Date of Withdrawal

Unless otherwise required under Applicable Law, withdrawal of consent shall become effective only upon receipt, verification and acceptance of the request by the Company.

The Company shall be entitled to take such reasonable time as may be necessary for verifying the request, updating its records, communicating with relevant personnel, informing Third-Party Service Providers where appropriate and implementing the withdrawal across its operational systems.

25.5 Consequences of Withdrawal

The Data Principal acknowledges that the provision of immigration consultancy services necessarily requires the processing of Personal Data. Accordingly, withdrawal of consent may materially affect or completely prevent the Company's ability to continue providing the Consultancy Services.

Without limiting the generality of the foregoing, withdrawal of consent may result in-

25.5.1 suspension of the Consultancy Services;

25.5.2 inability to prepare or submit immigration or visa applications;

25.5.3 inability to communicate with Government Authorities, Embassies, Consulates, Visa Application Centres or other competent authorities;

25.5.4 closure of the Client's file;

25.5.5 termination of the Engagement in accordance with the Agreement;

25.5.6 delay in the immigration process; or

25.5.7 such other consequences as may naturally arise from the Company's inability to lawfully process the Personal Data required for the Consultancy Services.

25.6 Processing Permitted After Withdrawal

Notwithstanding the withdrawal of consent, the Company may continue to retain or process Personal Data where such processing is authorised or required under Applicable Law, judicial orders, regulatory requirements, contractual obligations, statutory record retention requirements, protection of legal rights, defence of legal proceedings or any other lawful purpose recognised under Applicable Law.

25.7 No Retrospective Effect

Withdrawal of consent shall operate prospectively only.

No withdrawal shall invalidate, reverse or otherwise affect any lawful processing, disclosure, communication, transfer, submission or use of Personal Data undertaken prior to the effective date of withdrawal.

25.8 Financial Obligations

Withdrawal of consent shall not discharge the Client from any obligation to pay Professional Fees, Government Charges, Third-Party Charges, administrative expenses, contractual liabilities or any other amount lawfully payable to the Company in respect of Consultancy Services already rendered prior to the withdrawal of consent.

25.9 Company's Rights

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:17:36 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company reserves the right to suspend, discontinue or terminate the Consultancy Services where continued processing of Personal Data becomes impossible or commercially impracticable due to the withdrawal of consent by the Data Principal.

The exercise of such right shall not constitute a breach of the Agreement or this Policy.

26. CORRECTION, COMPLETION AND UPDATING OF PERSONAL DATA

26.1 General

The Company recognises that accurate, complete and up-to-date Personal Data is essential for the efficient provision of the Consultancy Services, compliance with Applicable Law and the proper administration of immigration and visa applications. Accordingly, every Data Principal shall have the right, subject to Applicable Law, to request the correction of inaccurate Personal Data, the completion of incomplete Personal Data and the updating of Personal Data that has become inaccurate or outdated.

26.2 Responsibility of the Data Principal

The Data Principal and the Client shall remain responsible for ensuring that every document, declaration, certificate, statement, application, passport, financial record, educational record, employment record and every other information supplied to the Company remains true, complete, accurate and current throughout the duration of the Engagement.

The Company shall ordinarily be entitled to rely upon the accuracy of the information supplied by the Client and shall not be under any obligation to independently verify every statement or document unless expressly agreed in writing or required under Applicable Law.

26.3 Submission of Correction Requests

Any request seeking correction, completion or updating of Personal Data shall be submitted to the Company in writing together with such documentary evidence as may reasonably be required for verifying the proposed correction.

The Company may prescribe reasonable procedures for receiving, verifying and implementing such requests.

26.4 Verification

The Company reserves the right to verify the authenticity, accuracy and completeness of every request for correction before modifying its records.

Where the Company reasonably considers additional information or documentary evidence necessary, the Company may defer implementation of the requested correction until such information has been received and verified.

26.5 Corrections During Ongoing Applications

Where an immigration, visa, work permit, residence permit, permanent residence or citizenship application has already been submitted to any Government Authority, Embassy, Consulate or Visa Application Centre, the Company shall endeavour to communicate corrected information to the relevant authority where reasonably practicable and where such communication is permitted under Applicable Law and the procedures prescribed by the relevant authority.

**Rohit
Kaul**
Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:18:20
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company shall not, however, guarantee that any Government Authority or foreign institution will accept or act upon the corrected information.

26.6 Documents Previously Submitted

The correction or updating of Personal Data shall not automatically invalidate documents, declarations or applications previously submitted by the Company on the basis of information supplied by the Client at the relevant time.

The Client acknowledges that any consequences arising from inaccurate or incomplete information originally supplied shall remain the responsibility of the Client unless such inaccuracy is directly attributable to the Company's own error.

26.7 Time for Processing Requests

The Company shall endeavour to process requests for correction, completion or updating of Personal Data within a reasonable period after receipt of the request together with all supporting documents reasonably required for verification.

The period required for implementation may vary depending upon the complexity of the request, the volume of records involved, pending applications and the requirements of Applicable Law.

26.8 Circumstances Where Correction May Be Refused

The Company may refuse, postpone or limit any request for correction where—

26.8.1 the request is unsupported by adequate documentary evidence;

26.8.2 the identity or authority of the requesting person cannot reasonably be established;

26.8.3 the requested correction appears fraudulent, misleading or inconsistent with official records;

26.8.4 Applicable Law prohibits modification of the relevant records;

26.8.5 the relevant records have already been lawfully submitted to Government Authorities and cannot be altered by the Company; or

26.8.6 the Company is otherwise authorised under Applicable Law to decline such request.

26.9 Continuing Obligation

The Client shall promptly notify the Company of every material change relating to passport particulars, nationality, residential address, contact details, educational qualifications, employment status, financial information, immigration status, marital status or any other Personal Data which may reasonably affect the Consultancy Services.

Failure to promptly communicate such changes may adversely affect the Company's ability to provide the Consultancy Services, and the Company shall not be liable for any delay, rejection, adverse decision or other consequence resulting directly from the Client's failure to provide updated information.

27. ERASURE AND RESTRICTION OF PROCESSING

**Rohit
Kaul**
Digitally
signed by
Rohit Kaul
Date:
2026.07.17
18:18:56
+05:30

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

27.1 General

Subject to the provisions of the Digital Personal Data Protection Act, 2023, Applicable Law and this Policy, a Data Principal may request the erasure of Personal Data or the restriction of its processing where such Personal Data is no longer required for the purposes for which it was collected, where consent has been lawfully withdrawn, where the processing is otherwise no longer authorised under Applicable Law or where the Data Principal is otherwise entitled to seek such relief under Applicable Law.

The Company shall consider every such request in good faith, having regard to the rights of the Data Principal, the legitimate interests of the Company, the contractual relationship between the Parties and every applicable statutory or regulatory obligation.

27.2 Submission of Requests

Any request seeking erasure, deletion or restriction of processing shall be submitted in writing through such communication channels as may be notified by the Company from time to time.

The Company may require the Data Principal to provide documentary proof of identity, authority and such additional information as may reasonably be necessary for verifying the request before taking any action under this Clause.

27.3 Verification

Before erasing or restricting the processing of any Personal Data, the Company may verify—

- 27.3.1** the identity of the requesting individual;
- 27.3.2** the authority of any representative acting on behalf of the Data Principal;
- 27.3.3** the nature and extent of the Personal Data concerned;
- 27.3.4** whether the Company continues to possess a lawful basis for retaining or processing such Personal Data; and
- 27.3.5** whether any statutory, contractual or regulatory obligation requires continued retention or processing.

27.4 Circumstances in which Erasure may be Refused

The Company may refuse, postpone or limit any request for erasure where continued retention or processing of Personal Data is reasonably necessary for—

- 27.4.1** compliance with Applicable Law;
- 27.4.2** compliance with judicial orders or directions issued by Government Authorities;
- 27.4.3** compliance with taxation, accounting or regulatory requirements;
- 27.4.4** defending or enforcing legal or contractual rights;
- 27.4.5** pending or reasonably anticipated judicial, arbitral, regulatory or administrative proceedings;
- 27.4.6** maintaining professional records relating to the Consultancy Services;

27.4.7 pending immigration, visa, work permit, residence permit, permanent residence or citizenship applications;

27.4.8 fraud prevention, cybersecurity, document verification or internal compliance investigations; or

27.4.9 any other lawful purpose recognised under Applicable Law.

27.5 Restriction of Processing

Where immediate erasure is not legally permissible but continued unrestricted processing is unnecessary, the Company may restrict the processing of the relevant Personal Data to the minimum extent reasonably necessary for complying with Applicable Law, protecting legal rights, completing pending proceedings or satisfying other lawful obligations.

Restricted Personal Data shall ordinarily remain accessible only to those persons whose official responsibilities require such access.

27.6 Effect upon Consultancy Services

The Data Principal acknowledges that immigration consultancy services depend upon the continued availability of Personal Data throughout the duration of the Engagement.

Accordingly, any request for erasure or restriction of processing may materially affect the Company's ability to continue providing the Consultancy Services and may result in suspension, delay or termination of the Engagement where continued processing is reasonably necessary for performing the Agreement.

The Company shall not be responsible for any adverse consequence directly arising from the lawful implementation of such request or from the Company's inability to continue providing the Consultancy Services following the erasure or restriction of Personal Data.

27.7 Records Already Submitted

Where Personal Data has already been lawfully submitted to Government Authorities, Embassies, Consulates, Visa Application Centres, employers, educational institutions or other independent organisations, the Company shall not be responsible for procuring the deletion or restriction of processing of such Personal Data by those independent recipients.

The Data Principal acknowledges that the processing of such Personal Data by independent organisations shall remain subject to their respective legal obligations and internal privacy practices.

27.8 Partial Erasure

Where only a portion of the Personal Data may lawfully be erased, the Company may erase such portion while retaining the balance of the Personal Data that continues to be required under Applicable Law or this Policy.

27.9 No Immediate Destruction

The Company shall not be required to immediately destroy every copy of Personal Data upon receipt of an erasure request where such information continues to exist within secure backup

**Rohit
Kaul**
Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:20:43 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

systems, disaster recovery environments, archived records or other systems maintained for lawful operational purposes.

Such information shall continue to remain subject to appropriate confidentiality and security safeguards.

28. GRIEVANCE REDRESSAL MECHANISM AND GRIEVANCE OFFICER

28.1 General

The Company is committed to addressing concerns relating to the collection, use, processing, disclosure, retention and protection of Personal Data in a fair, transparent and timely manner. Accordingly, the Company shall establish an internal grievance redressal mechanism for receiving, examining, investigating and resolving complaints submitted by Data Principals in accordance with Applicable Law.

The objective of the grievance redressal mechanism shall be to facilitate the prompt and effective resolution of privacy-related concerns while ensuring compliance with the Digital Personal Data Protection Act, 2023 and this Policy.

28.2 Appointment of Grievance Officer

The Company shall designate a Grievance Officer or such other authorised officer as may be required under Applicable Law for the purpose of administering the grievance redressal mechanism established under this Policy.

The Company reserves the right to appoint, replace or redesignate the Grievance Officer from time to time in accordance with its organisational requirements and Applicable Law.

28.3 Scope of Grievances

Without limiting the generality of this Clause, grievances may relate to—

- 28.3.1 collection of Personal Data;
- 28.3.2 use or processing of Personal Data;
- 28.3.3 unauthorised disclosure of Personal Data;
- 28.3.4 requests for correction, updating or completion of Personal Data;
- 28.3.5 requests for erasure or restriction of processing;
- 28.3.6 withdrawal of consent;
- 28.3.7 alleged Personal Data Breaches;
- 28.3.8 refusal of statutory requests;
- 28.3.9 alleged violations of this Policy; or
- 28.3.10 every other matter relating to the processing of Personal Data by the Company.

28.4 Submission of Grievances

**Rohit
Kaul**
Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:21:21
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

Any grievance shall ordinarily be submitted in writing together with sufficient particulars describing the nature of the complaint, the Personal Data concerned, the relief sought and every other information reasonably necessary for enabling the Company to examine the grievance.

The Company may prescribe standard complaint formats or electronic submission procedures from time to time.

28.5 Verification

The Company may verify the identity of the complainant before investigating or responding to any grievance involving Personal Data.

Where a grievance is submitted through an authorised representative, the Company may require documentary evidence establishing the representative's authority.

28.6 Investigation

Upon receipt of a grievance, the Company shall endeavour to examine the facts, review the relevant records, consult appropriate personnel, conduct such internal enquiries as may reasonably be necessary and determine the appropriate course of action consistent with Applicable Law and this Policy.

The Company may request additional documents or clarifications from the complainant where reasonably necessary for completing the investigation.

28.7 Resolution

Following completion of the investigation, the Company shall endeavour to communicate its decision, proposed corrective measures or other appropriate response to the complainant within such period as may be prescribed under Applicable Law or, where no period is prescribed, within a reasonable time having regard to the complexity of the grievance.

28.8 Corrective Measures

Where the Company determines that corrective action is warranted, it may implement such measures as it considers reasonably appropriate, including correction of records, enhancement of security measures, modification of operational procedures, employee guidance, additional training, restricted processing, implementation of technical safeguards or such other lawful remedial action as may be appropriate in the circumstances.

28.9 Record of Grievances

The Company may maintain appropriate records of complaints, investigations, correspondence, findings and corrective measures undertaken under this Clause for compliance, audit, legal and operational purposes.

Such records shall be retained in accordance with the Company's record retention policy and Applicable Law.

28.10 Escalation

Where a Data Principal remains dissatisfied after completion of the Company's internal grievance process, the Data Principal may exercise such statutory remedies as may be available under the Digital Personal Data Protection Act, 2023 or any other Applicable Law.

Nothing contained in this Policy shall restrict the Data Principal from exercising any statutory remedy available under Applicable Law.

28.12 No Frivolous or Vexatious Complaints

The Company reserves the right to decline, discontinue or limit the processing of complaints that are manifestly frivolous, vexatious, repetitive, abusive, fraudulent or otherwise submitted in bad faith, without prejudice to any statutory rights available to the complainant under Applicable Law.

29. PERSONAL DATA BREACH MANAGEMENT

29.1 General

The Company recognises that, notwithstanding the implementation of reasonable technical, organisational, contractual and administrative safeguards, incidents affecting the confidentiality, integrity or availability of Personal Data may occur. Accordingly, the Company shall maintain appropriate procedures for identifying, reporting, investigating, containing, mitigating and responding to any actual or reasonably suspected Personal Data Breach in accordance with the Digital Personal Data Protection Act, 2023, Applicable Law and recognised information security practices.

The Company shall endeavour to respond to every Personal Data Breach in a timely, proportionate and responsible manner, having due regard to the nature of the incident, the categories of Personal Data involved, the number of affected Data Principals, the potential impact of the incident and the legal obligations applicable to the Company.

29.2 Meaning of Personal Data Breach

For the purposes of this Policy, a Personal Data Breach shall include any accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, access to, acquisition of or misuse of Personal Data, whether arising from cyber incidents, human error, system failures, physical loss of records, malicious activities, technological failures or any other cause affecting the security of Personal Data.

29.3 Detection and Reporting

Every director, officer, employee, consultant, intern, contractor, authorised representative or Third-Party Service Provider who becomes aware of any actual or suspected Personal Data Breach shall promptly report the same to the appropriate personnel designated by the Company.

No person acting on behalf of the Company shall knowingly conceal, suppress or intentionally delay the reporting of any Personal Data Breach.

29.4 Initial Assessment

Upon becoming aware of a Personal Data Breach, the Company shall endeavour to conduct an initial assessment for determining—

29.4.1 the nature and cause of the incident;

29.4.2 the categories and volume of Personal Data affected;

29.4.3 the number of affected Data Principals, where reasonably ascertainable;

29.4.4 whether the breach remains ongoing;

29.4.5 the actual or reasonably foreseeable consequences of the incident; and

29.4.6 the immediate measures required for containing the incident.

29.5 Containment Measures

Where reasonably practicable, the Company shall implement appropriate containment measures designed to minimise the impact of the Personal Data Breach. Such measures may include restricting system access, isolating affected systems, recovering compromised records, suspending user credentials, enhancing security controls, changing authentication credentials, restoring backup data or implementing other appropriate remedial actions.

29.6 Investigation

The Company may conduct such internal investigation as it considers reasonably necessary for determining the circumstances surrounding the Personal Data Breach, identifying the systems or records affected, evaluating compliance with internal procedures, determining whether misconduct has occurred and identifying measures necessary for preventing recurrence.

The Company may engage information technology experts, cybersecurity consultants, forensic specialists, legal advisers or other professional advisers where considered appropriate.

29.7 Notification

Where notification of a Personal Data Breach is required under Applicable Law, the Company shall endeavour to provide such notification to the appropriate regulatory authority, Government Authority or affected Data Principal within the period and in the manner prescribed under Applicable Law.

Nothing contained in this Clause shall require the Company to issue any notification where such notification is not required by Applicable Law.

29.8 Cooperation with Authorities

The Company shall cooperate with competent Government Authorities, regulatory bodies, law enforcement agencies and other authorities to the extent required under Applicable Law in connection with any investigation relating to a Personal Data Breach.

Such cooperation shall not require the Company to disclose information protected by legal privilege, contractual confidentiality obligations or any other protection recognised under Applicable Law except where disclosure is lawfully required.

29.9 Documentation

The Company may maintain records relating to every Personal Data Breach, including details of the incident, investigative findings, corrective actions, communications, notifications, remedial measures and lessons learned for compliance, audit and operational purposes.

29.10 Corrective Measures

Following completion of the investigation, the Company may implement such corrective, preventive and organisational measures as it considers reasonably appropriate for reducing the

likelihood of recurrence, improving information security, strengthening operational controls and enhancing compliance with Applicable Law.

29.11 No Admission of Liability

The occurrence of a Personal Data Breach or the implementation of any remedial measure shall not, by itself, constitute an admission of negligence, fault or liability on the part of the Company.

The liability of the Company, if any, shall be determined solely in accordance with Applicable Law and the Agreement governing the relationship between the Parties.

30. COMPLIANCE MONITORING, AUDIT AND POLICY REVIEW

30.1 General

The Company acknowledges that effective privacy governance requires continuous monitoring, periodic evaluation and regular improvement of its policies, operational procedures and information security practices. Accordingly, the Company shall endeavour to establish and maintain an appropriate compliance framework designed to ensure continuing adherence to this Policy, the Digital Personal Data Protection Act, 2023 and every other Applicable Law governing the processing of Personal Data.

30.2 Compliance Monitoring

The Company may periodically monitor its internal operations, document management practices, information technology systems, employee compliance, Third-Party Service Provider relationships and operational procedures for the purpose of evaluating compliance with this Policy and identifying opportunities for improvement.

Such monitoring may be conducted through manual reviews, electronic monitoring systems, internal reporting mechanisms, management supervision or such other lawful means as the Company considers appropriate.

30.3 Internal Audits

The Company may conduct periodic internal privacy audits, compliance reviews, information security assessments, operational evaluations or other internal examinations for assessing compliance with this Policy, Applicable Law, contractual obligations and recognised industry practices.

The frequency, scope and methodology of such audits shall be determined by the Company having regard to the nature of its business operations, technological environment, operational risks and legal requirements.

30.4 External Assessments

Where considered appropriate, the Company may engage independent auditors, legal advisers, cybersecurity consultants, information security professionals or other qualified experts for reviewing its privacy governance framework, information security controls, operational procedures or compliance practices.

**Rohit
Kaul**
Digitally
signed by
Rohit Kaul
Date:
2026.07.17
18:24:09
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

Nothing contained herein shall require the Company to conduct any external audit unless required under Applicable Law or voluntarily determined by the Company.

30.5 Employee Compliance

The Company may periodically evaluate whether directors, officers, employees, consultants, interns, contractors and other authorised personnel are complying with their obligations under this Policy, internal operating procedures, confidentiality requirements and Applicable Law.

Where deficiencies are identified, the Company may implement appropriate corrective measures, additional supervision, employee guidance, supplementary training or disciplinary action as may be considered appropriate.

30.6 Review of Third-Party Service Providers

The Company may periodically review the performance, security practices and compliance standards of Third-Party Service Providers engaged for processing Personal Data or supporting the Company's business operations.

The Company reserves the right to modify, suspend or terminate any engagement where continued association may expose the Company or its Clients to unreasonable operational, legal or cybersecurity risks.

30.7 Policy Review

This Policy may be reviewed periodically by the Company to ensure that it remains accurate, effective and consistent with Applicable Law, technological developments, operational requirements, judicial pronouncements, regulatory guidance and recognised industry practices.

The Company reserves the right to amend, supplement or replace any provision of this Policy following such review.

30.8 Regulatory Developments

The Company may modify its operational procedures, document management practices, information security controls, internal governance framework and privacy practices in response to amendments in Applicable Law, governmental notifications, judicial decisions, regulatory directions or changes in recognised industry standards.

30.9 Corrective and Preventive Measures

Where any weakness, non-compliance, operational deficiency or information security vulnerability is identified through audits, monitoring activities, regulatory inspections, employee reporting or any other lawful means, the Company may implement such corrective and preventive measures as it considers reasonably necessary for strengthening its privacy governance framework.

30.10 Continuous Improvement

The Company recognises that privacy governance and cybersecurity are evolving disciplines requiring continuous improvement.

Accordingly, the Company shall endeavour to enhance its policies, operational procedures, employee awareness, information security controls, technological safeguards and

**Rohit
Kaul**

Digitally signed
by Rohit Kaul
Date: 2026.07.17
18:24:52 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

organisational practices from time to time in order to promote responsible processing of Personal Data and compliance with Applicable Law.

31. REGULATORY COOPERATION AND GOVERNMENT REQUESTS

31.1 General

The Company acknowledges its obligation to cooperate with Government Authorities, regulatory bodies, statutory authorities, judicial forums, law enforcement agencies and every other competent authority having lawful jurisdiction over the Company or the processing of Personal Data. Accordingly, the Company shall respond to lawful requests, notices, summons, directions, investigations, inspections, audits and other communications received from such authorities in accordance with Applicable Law, while endeavouring to protect the confidentiality of Personal Data and the legitimate interests of its Clients and Data Principals.

Nothing contained in this Policy shall prevent the Company from complying with any lawful direction issued by a competent authority where such compliance is mandatory under Applicable Law.

31.2 Government Requests

The Company may collect, use, retain, disclose or otherwise process Personal Data where such processing is reasonably necessary for complying with judicial orders, statutory notices, summons issued by courts, tribunals or regulatory authorities, lawful directions issued by Government Authorities, investigations conducted by competent authorities, statutory inspections or audits, immigration or border control requirements, taxation requirements, anti-money laundering obligations, national security requirements or every other lawful governmental or regulatory requirement applicable to the Company.

31.3 Verification of Requests

Before disclosing Personal Data pursuant to any governmental or regulatory request, the Company may, where reasonably practicable and not prohibited by Applicable Law, verify the identity of the requesting authority, the legal authority under which the request has been issued, the scope of the information requested, whether the request appears proportionate to its stated purpose and whether any limitation or confidentiality requirement applies to the requested disclosure.

Nothing contained herein shall require the Company to delay compliance where immediate disclosure is mandated by Applicable Law.

31.4 Scope of Disclosure

The Company shall endeavour to disclose only such Personal Data as is reasonably necessary for complying with the applicable governmental or regulatory requirement.

Where reasonably practicable, the Company may limit the disclosure to the categories of Personal Data specifically requested or otherwise lawfully required to be disclosed.

31.5 Confidentiality

Where the Company receives Personal Data pursuant to confidential governmental proceedings or where Applicable Law restricts disclosure of the existence or contents of any governmental

request, the Company shall comply with such confidentiality obligations to the extent required by Applicable Law.

31.6 Cooperation During Investigations

The Company may cooperate with Government Authorities, law enforcement agencies, regulatory bodies, courts and tribunals during investigations relating to fraud, cybercrime, document forgery, immigration offences, identity theft, financial crimes or other unlawful activities where such cooperation is authorised or required under Applicable Law.

Such cooperation may include the production of records, provision of information, preservation of evidence, attendance before competent authorities or such other lawful assistance as may reasonably be required.

31.7 International Regulatory Cooperation

Where the Consultancy Services involve foreign jurisdictions, the Company may cooperate with foreign Government Authorities, Embassies, Consulates, immigration departments or other competent authorities where such cooperation is reasonably necessary for the provision of the Consultancy Services or otherwise required under Applicable Law.

Such cooperation shall remain subject to the restrictions applicable under Indian law and any other relevant legal requirements governing cross-border disclosures.

31.8 Preservation of Records

Where the Company becomes aware of any governmental investigation, judicial proceeding or regulatory enquiry relating to Personal Data, the Company may preserve relevant records notwithstanding any provision relating to erasure or destruction contained elsewhere in this Policy until such proceedings have been finally concluded or until Applicable Law otherwise permits disposal of such records.

31.9 No Liability

The Company shall not be liable for any disclosure of Personal Data made in good faith pursuant to a lawful governmental request, judicial order, statutory direction or regulatory requirement.

32. ARTIFICIAL INTELLIGENCE AND AUTOMATED PROCESSING

32.1 General

The Company recognises that technological developments, including artificial intelligence, machine learning, automation software, intelligent document management systems and other digital technologies, may assist in improving the efficiency, accuracy and consistency of the Consultancy Services. Accordingly, the Company may utilise such technologies for supporting its lawful business operations in accordance with Applicable Law and this Policy.

The Company shall endeavour to ensure that the use of artificial intelligence or automated processing remains responsible, proportionate and subject to appropriate human oversight.

32.2 Permitted Uses

**Rohit
Kaul**

Digitally
signed by
Rohit Kaul
Date:
2026.07.17
18:26:25
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

Artificial intelligence and automated technologies may be utilised for one or more of the following lawful purposes—

32.2.1 document classification;

32.2.2 document indexing;

32.2.3 document organisation;

32.2.4 workflow management;

32.2.5 appointment scheduling;

32.2.6 client communication support;

32.2.7 document comparison;

32.2.8 language translation assistance;

32.2.9 identification of incomplete documentation;

32.2.10 operational reporting;

32.2.11 cybersecurity monitoring;

32.2.12 fraud detection;

32.2.13 quality assurance; and

32.2.14 every other lawful operational purpose reasonably connected with the provision of the Consultancy Services.

32.3 Human Oversight

The Company shall endeavour to ensure that material decisions affecting the rights, obligations or interests of Clients are not based solely upon automated processing where human review is reasonably necessary.

Professional advice relating to immigration strategy, visa eligibility, legal interpretation, assessment of documentation or recommendations to Clients shall ordinarily remain subject to appropriate human review and professional judgment.

32.4 No Automated Decision Guarantee

The Company does not represent that artificial intelligence systems, automated software or digital tools are free from errors, inaccuracies or technological limitations.

Every automated output generated by such systems may require human verification before being relied upon for professional purposes.

32.5 Third-Party Artificial Intelligence Platforms

The Company may utilise artificial intelligence platforms, cloud-based software, workflow automation systems or document management technologies provided by independent Third-Party Service Providers.

Rohit
Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:27:07 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company shall endeavour to engage reputable service providers and implement reasonable safeguards; however, the Company shall not warrant the uninterrupted availability, absolute accuracy or complete security of independent third-party artificial intelligence systems.

32.6 Protection of Personal Data

Where Personal Data is processed using artificial intelligence or automated systems, the Company shall endeavour to implement reasonable technical and organisational safeguards designed to protect such Personal Data against unauthorised access, misuse, accidental disclosure or unlawful processing.

The use of artificial intelligence shall not diminish the Company's confidentiality obligations under this Policy.

32.7 Continuous Evaluation

The Company may periodically evaluate the performance, reliability, security and legal compliance of artificial intelligence systems utilised in its operations and may modify, replace, suspend or discontinue such technologies where considered appropriate.

32.8 Regulatory Compliance

The Company shall endeavour to ensure that its use of artificial intelligence and automated processing remains consistent with Applicable Law, recognised industry practices and evolving regulatory guidance concerning privacy, cybersecurity and responsible use of emerging technologies.

32.9 Reservation of Rights

The Company reserves the right to introduce, modify, expand, restrict or discontinue the use of artificial intelligence, automation technologies or digital processing systems at any time having regard to technological developments, operational requirements, cybersecurity considerations, regulatory changes or business needs.

33. BUSINESS CONTINUITY AND DISASTER RECOVERY

33.1 General

The Company recognises that uninterrupted access to information systems, client records and Personal Data is essential for the efficient provision of the Consultancy Services. Accordingly, the Company shall endeavour to establish and maintain reasonable business continuity and disaster recovery measures designed to minimise disruption to its operations arising from natural disasters, cyber incidents, technological failures, power outages, communication failures, fire, flood, pandemics, civil disturbances, force majeure events or any other unforeseen circumstances that may adversely affect its business operations.

The Company shall periodically review its operational resilience measures and may revise or strengthen such measures having regard to technological developments, operational requirements, recognised industry practices and Applicable Law.

33.2 Business Continuity Measures

**Rohit
Kaul**

Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:27:46
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company may establish appropriate business continuity procedures for maintaining critical business operations during emergencies. Such measures may include—

33.2.1 alternative communication channels;

33.2.2 secure backup of electronic records;

33.2.3 remote working arrangements;

33.2.4 alternative information technology infrastructure;

33.2.5 emergency operational procedures;

33.2.6 continuity of client communications;

33.2.7 protection of physical records; and

33.2.8 such other measures as the Company considers reasonably appropriate for ensuring operational continuity.

33.3 Disaster Recovery

The Company may maintain disaster recovery procedures designed to facilitate the restoration of information systems, electronic records, communication platforms, document repositories and other critical business resources following a disruptive event.

Such procedures may include secure backup systems, restoration protocols, system redundancy, alternative storage arrangements and other technological safeguards considered appropriate by the Company.

33.4 Backup of Personal Data

Where reasonably practicable, the Company may maintain backup copies of Personal Data, client files, operational records and other business information for the purpose of facilitating recovery following accidental deletion, technological failure, cyber incidents or other unforeseen events.

Backup records shall remain subject to the confidentiality, security and access control requirements prescribed under this Policy.

33.5 Prioritisation of Critical Services

During any business interruption, the Company may prioritise the restoration of critical operational functions, including access to client records, communication with Government Authorities, immigration application management, document repositories, cybersecurity controls and such other functions considered necessary for the continued provision of the Consultancy Services.

33.6 Third-Party Dependencies

The Company acknowledges that certain aspects of its business operations depend upon the services of independent third parties, including internet service providers, cloud infrastructure providers, payment service providers, communication platforms, software vendors, courier agencies and Government Authorities.

Rohit
Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:28:27 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company shall not be responsible for delays, interruptions or failures attributable solely to such independent third parties beyond the Company's reasonable control.

33.7 Testing and Review

The Company may periodically review, test or update its business continuity and disaster recovery procedures to improve operational resilience and to ensure that such procedures remain appropriate in light of technological developments, cybersecurity risks and changing business requirements.

Nothing contained herein shall require the Company to conduct any particular test or review at specified intervals unless otherwise required under Applicable Law.

33.8 Force Majeure

Where the Company's ability to provide the Consultancy Services is affected by any force majeure event, including natural disasters, war, terrorism, riots, strikes, epidemics, pandemics, governmental restrictions, cyber warfare, widespread technological failures or other events beyond the Company's reasonable control, the Company shall not be liable for any delay, interruption or inability to perform its obligations to the extent directly attributable to such event.

The Company shall, however, endeavour to resume normal operations as soon as reasonably practicable.

33.9 No Guarantee of Continuous Operations

While the Company shall endeavour to maintain appropriate business continuity arrangements, the Company does not represent or warrant that its business operations, information systems, communication infrastructure or electronic services shall remain continuously available or free from interruption under all circumstances.

34. LIMITATION OF LIABILITY

34.1 General

To the maximum extent permitted under Applicable Law, the Company shall not be liable for any indirect, incidental, special, consequential, exemplary or punitive damages arising out of or in connection with the collection, use, processing, disclosure, transfer, retention, storage or protection of Personal Data, except where such liability arises directly from the Company's wilful misconduct or gross negligence.

Nothing contained in this Clause shall exclude any liability that cannot lawfully be excluded or restricted under Applicable Law.

34.2 Government Decisions

The Company shall not be liable for any decision, action or omission of any Government Authority, Embassy, Consulate, High Commission, Visa Application Centre, immigration department, foreign governmental authority, educational institution, employer or other independent authority affecting the Client or the processing of Personal Data.

**Rohit
Kaul**

Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:29:10
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

Without limitation, the Company shall not be responsible for the refusal, rejection, delay, suspension, cancellation or withdrawal of any visa, permit, immigration benefit, citizenship application or other governmental approval.

34.3 Accuracy of Information Supplied by the Client

The Company shall be entitled to rely upon the information and documents supplied by the Client.

The Company shall not be liable for any loss, rejection, delay, investigation, penalty or adverse consequence arising from inaccurate, incomplete, forged, misleading or outdated information or documents supplied by the Client or any third party acting on the Client's behalf.

34.4 Independent Third Parties

The Company shall not be liable for the acts, omissions, negligence, defaults, cyber incidents, operational failures, privacy practices or information security measures of independent Government Authorities, Embassies, Consulates, Visa Application Centres, Third-Party Service Providers, cloud service providers, payment gateways, employers, educational institutions or other independent organisations after Personal Data has been lawfully disclosed to them in accordance with this Policy or Applicable Law.

34.5 Cybersecurity Incidents

While the Company shall endeavour to implement reasonable technical and organisational safeguards, the Company shall not be liable for losses arising solely from hacking, malware, ransomware, phishing attacks, denial-of-service attacks, internet failures, telecommunications failures, cyber warfare, technological failures or other cybersecurity incidents beyond the Company's reasonable control, provided that the Company has acted in accordance with its obligations under Applicable Law.

34.6 Force Majeure

The Company shall not be liable for any delay, interruption, inability to perform or other loss arising directly or indirectly from force majeure events, including natural disasters, floods, earthquakes, fire, epidemics, pandemics, war, terrorism, civil unrest, governmental actions, labour disputes, power failures or any other event beyond the Company's reasonable control.

34.7 Website and Electronic Communications

The Company does not warrant that its Website, client portal, electronic communication systems, cloud infrastructure or digital platforms shall remain continuously available, uninterrupted, secure or error-free.

Accordingly, the Company shall not be liable for losses arising from temporary service interruptions, technological failures, communication delays, internet disruptions or other events affecting electronic communications beyond the Company's reasonable control.

34.8 No Professional Guarantee

Nothing contained in this Policy or the Consultancy Services shall be construed as guaranteeing the approval of any visa, work permit, residence permit, permanent residence application, citizenship application or any other immigration-related benefit.

**Rohit
Kaul**
Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:29:55
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Company's responsibility shall be limited to providing professional consultancy services with reasonable skill and care and in accordance with the Agreement and Applicable Law.

34.9 Mitigation of Loss

Every Client and Data Principal shall take reasonable steps to mitigate any loss arising from any incident relating to Personal Data and shall promptly notify the Company upon becoming aware of any circumstance likely to affect the confidentiality, integrity or availability of such Personal Data.

Failure to mitigate avoidable loss may be taken into consideration in determining the extent of any liability, where permitted under Applicable Law.

34.10 Aggregate Limitation

To the maximum extent permitted under Applicable Law and without prejudice to any limitation contained in the Agreement, the aggregate liability of the Company arising under this Policy shall not exceed the total Professional Fees actually received by the Company from the Client in respect of the specific Engagement giving rise to the claim, unless a higher liability is expressly imposed by Applicable Law.

34.11 Survival

The limitations, exclusions and protections contained in this Clause shall survive the completion, termination, suspension or expiration of the Consultancy Services, the Agreement and this Policy.

35. INDEMNITY

35.1 General

The Client and, where applicable, the Data Principal, shall jointly and severally indemnify, defend and hold harmless the Company, its directors, shareholders, officers, employees, consultants, authorised representatives, interns, agents, successors and assigns (collectively referred to in this Clause as the "Indemnified Persons") from and against every claim, demand, action, proceeding, liability, loss, damage, penalty, fine, cost, expense or other obligation whatsoever, including reasonable legal and professional expenses, arising directly or indirectly from any act, omission, negligence, misrepresentation or breach attributable to the Client or the Data Principal.

The indemnity contained in this Clause shall survive the completion, suspension, termination or expiration of the Engagement and this Policy.

35.2 False or Inaccurate Information

The Client shall indemnify the Company against every loss arising from false, inaccurate or misleading Personal Data, forged, fabricated or altered documents, suppression of material facts, inaccurate declarations, incorrect translations supplied by the Client, outdated information which the Client failed to update or any other inaccurate information supplied to the Company by or on behalf of the Client.

35.3 Unauthorised Disclosure

**Rohit
Kaul**
Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:30:52
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

The Client shall indemnify the Company against every loss arising from the unauthorised disclosure, publication, circulation or misuse of Personal Data by the Client, the Data Principal or any person acting under their authority or instructions.

35.4 Breach of Applicable Law

The Client shall indemnify the Company against every liability arising from the Client's violation of Applicable Law, immigration laws, visa regulations, data protection laws, anti-money laundering requirements, governmental directions or any other legal obligation applicable to the Client.

35.5 Breach of this Policy

The Client shall indemnify the Company against every loss arising from any breach of this Policy, the Agreement or any other contractual document executed between the Parties, including any failure to comply with obligations relating to confidentiality, data protection, cooperation, record accuracy or lawful use of the Consultancy Services.

35.6 Third-Party Claims

Where any Government Authority, Embassy, Consulate, Visa Application Centre, employer, educational institution, regulatory authority or any other third party initiates any claim, proceeding, investigation or demand against the Company arising from the acts or omissions of the Client or the Data Principal, the Client shall indemnify the Company against every resulting liability, cost, penalty, expense and legal proceeding.

35.7 Investigation Costs

The indemnity contained herein shall include the reasonable costs incurred by the Company in investigating complaints, responding to Government Authorities, participating in regulatory proceedings, preserving records, engaging professional advisers, conducting internal investigations or defending judicial, arbitral or administrative proceedings arising from the acts or omissions of the Client.

35.8 Duty to Cooperate

Where any claim arises which may give rise to an indemnity under this Clause, the Client shall promptly provide every reasonable assistance, document, explanation, clarification and cooperation requested by the Company for defending such claim or mitigating the resulting loss.

35.9 No Limitation

The indemnity contained in this Clause shall be in addition to, and not in substitution for, every other right, remedy or protection available to the Company under the Agreement, this Policy, Applicable Law or the general law.

36. AMENDMENT OF THIS POLICY

36.1 General

The Company recognises that privacy laws, information security practices, technological developments and regulatory requirements continue to evolve. Accordingly, the Company

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
16:31:39 +05:30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

reserves the right to amend, modify, supplement, replace, revise or update this Policy from time to time for the purpose of ensuring continued compliance with Applicable Law, improving operational practices, strengthening information security or responding to changes affecting the Company's business operations.

36.2 Circumstances for Amendment

Without limiting the generality of the foregoing, the Company may amend this Policy where such amendment becomes necessary on account of amendments to Applicable Law, judicial decisions, governmental notifications or regulatory directions, technological developments, cybersecurity risks, operational changes within the Company, introduction of new Consultancy Services, changes in information technology infrastructure, recognised industry practices or any other circumstance reasonably requiring revision of this Policy.

36.3 Publication of Amendments

The Company may publish the revised version of this Policy through its Website, client portal, electronic communication, written notice or such other communication mechanism as the Company considers reasonably appropriate.

The Company may also maintain previous versions of this Policy for internal compliance, audit or legal purposes where considered appropriate.

36.4 Effective Date

Unless otherwise specified, every amendment to this Policy shall become effective from the date specified in the revised Policy or, where no date is specified, from the date on which such amendment is published or otherwise communicated by the Company.

36.5 Continued Use

Subject to Applicable Law, the continued engagement of the Company by the Client or the continued use of the Consultancy Services after the effective date of any amendment may constitute acceptance of the revised Policy to the extent permitted by Applicable Law.

Nothing contained herein shall prejudice any statutory rights requiring fresh consent where such consent is mandatory under Applicable Law.

36.6 No Obligation to Provide Individual Notice

Except where individual notice is expressly required under Applicable Law, the Company shall not be under any obligation to separately notify every Client or Data Principal of each amendment made to this Policy.

The Client shall remain responsible for periodically reviewing the current version of the Policy where it is made available by the Company.

36.7 Transitional Arrangements

Where the Company considers it reasonably necessary, any amendment to this Policy may include transitional provisions governing the implementation of revised operational procedures, updated technological safeguards, modified record retention practices or other compliance measures.

36.8 Severability of Amendments

If any amendment or revised provision of this Policy is declared invalid, unenforceable or inconsistent with Applicable Law by a competent court or authority, such determination shall not affect the validity or enforceability of the remaining provisions of this Policy.

36.9 Preservation of Rights

No amendment made under this Clause shall prejudice the Company's right to rely upon any provision of this Policy that was in force at the time of any act, omission, transaction or event giving rise to a legal claim, investigation or regulatory proceeding, unless otherwise required under Applicable Law.

37. MISCELLANEOUS

37.1 Entire Policy

This Policy constitutes the complete statement of the Company's privacy and Personal Data protection practices and shall be read together with the Agreement, the General Terms and Conditions, the Company's Website Terms of Use, Cookies Policy and every other policy or document expressly incorporated by reference. In the event of any inconsistency between this Policy and any other Company policy relating specifically to the protection of Personal Data, the provisions of this Policy shall prevail to the extent of such inconsistency unless otherwise required under Applicable Law.

37.2 Relationship with the Agreement

Nothing contained in this Policy shall be construed as modifying, superseding or limiting any provision contained in the Agreement executed between the Company and the Client except to the extent expressly stated herein. This Policy supplements the contractual obligations contained in the Agreement and shall be interpreted harmoniously with the General Terms and Conditions governing the Consultancy Services.

37.3 Severability

If any provision of this Policy or any part thereof is held by any court, tribunal or competent authority to be illegal, invalid, unenforceable or contrary to Applicable Law, such provision shall, to the extent of such illegality, invalidity or unenforceability, be deemed severed from this Policy without affecting the legality, validity or enforceability of the remaining provisions, which shall continue in full force and effect.

The Parties shall endeavour to replace any invalid provision with a valid provision that most closely reflects the commercial intent of the original provision.

37.4 Waiver

No failure, delay or omission by the Company in exercising any right, power or remedy available under this Policy, the Agreement or Applicable Law shall constitute a waiver thereof.

No waiver shall be valid unless expressly made in writing by an authorised representative of the Company, and any waiver granted in respect of one breach shall not constitute a waiver of any subsequent or continuing breach.

Rohit Kaul
Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:33:33 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

37.5 Survival

The provisions of this Policy which by their nature are intended to survive the completion, suspension, termination or expiration of the Consultancy Services shall continue to remain binding upon the Parties notwithstanding such completion, suspension, termination or expiration.

Without limitation, provisions relating to confidentiality, disclosure, cross-border transfers, record retention, data archival, limitation of liability, indemnity, governing law, dispute resolution and every other continuing obligation shall survive to the fullest extent permitted under Applicable Law.

37.6 Assignment

The Company may assign, transfer, novate or otherwise deal with its rights or obligations under this Policy in connection with any merger, amalgamation, demerger, restructuring, sale of business, business transfer or other lawful corporate reorganisation, subject to Applicable Law.

The Client shall not assign or transfer any right or obligation arising under this Policy without the prior written consent of the Company.

37.7 Notices

Any notice, communication, request, consent or other correspondence relating to this Policy shall be given in writing through electronic mail, courier, registered post, hand delivery, the Company's client portal or any other communication method recognised by the Company and Applicable Law.

A notice shall be deemed to have been duly received in accordance with the communication procedure prescribed in the Agreement or, in the absence thereof, within a reasonable period after dispatch by the relevant communication method.

37.8 Electronic Records

The Parties acknowledge that electronic records, electronic communications, electronic signatures, scanned documents, digital records and electronically stored information may constitute valid records to the extent recognised under Applicable Law.

The Company may maintain records in physical or electronic form and may rely upon electronic records maintained in the ordinary course of its business operations.

37.9 No Partnership or Agency

Nothing contained in this Policy shall be construed as creating any partnership, joint venture, agency, employment relationship or fiduciary relationship between the Company and the Client except to the limited extent expressly provided in the Agreement or required under Applicable Law.

37.10 Headings

The headings, titles and numbering used in this Policy are inserted solely for convenience of reference and shall not affect the interpretation, construction or meaning of any provision contained herein.

**Rohit
Kaul**
Digitally signed
by Rohit Kaul
Date: 2026.07.17
18:34:33 +05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

37.11 Interpretation

Unless the context otherwise requires, words importing the singular shall include the plural and vice versa, words importing one gender shall include every gender, references to persons shall include natural persons, companies, firms, partnerships, Government Authorities and every other legal entity, and references to Applicable Law shall include every amendment, modification, re-enactment or replacement thereof.

38. GOVERNING LAW AND JURISDICTION

38.1 Governing Law

This Policy shall be governed by and construed in accordance with the laws of the Republic of India, including, without limitation, the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000 (to the extent applicable), the rules, regulations, notifications and guidelines issued thereunder, and every other Applicable Law governing the processing, protection and management of Personal Data.

38.2 Compliance with Applicable Law

The Company and the Client acknowledge that every activity involving the collection, use, processing, disclosure, storage, transfer, retention and protection of Personal Data shall remain subject to Applicable Law.

Where any provision of this Policy becomes inconsistent with any mandatory requirement of Applicable Law, such mandatory requirement shall prevail to the extent of the inconsistency, and the remaining provisions of this Policy shall continue to remain valid and enforceable.

38.3 Jurisdiction

Subject to Clause 38.4 below and the dispute resolution provisions contained in the Agreement, the courts having competent jurisdiction at New Delhi, India, shall have exclusive jurisdiction over every dispute, claim, proceeding or matter arising out of or in connection with this Policy, the processing of Personal Data or the rights and obligations of the Parties hereunder.

38.4 Relationship with Dispute Resolution Clause

Where the Agreement executed between the Company and the Client contains an arbitration agreement or any other agreed dispute resolution mechanism, such arbitration agreement or dispute resolution mechanism shall apply to disputes arising under this Policy to the extent permitted by Applicable Law.

Nothing contained in this Clause shall prejudice the right of the Company or the Data Principal to approach any court, tribunal, regulatory authority or statutory forum having jurisdiction under Applicable Law where such right cannot lawfully be excluded.

38.5 Regulatory Proceedings

Nothing contained in this Policy shall prevent any Government Authority, regulatory body, court, tribunal or other competent authority from exercising such powers, jurisdiction or authority as may be conferred upon it under Applicable Law.

**Rohit
Kaul**
Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:36:05
+05'30'

Your Personal Consultancy Private Limited
Office No 102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India

Similarly, nothing contained herein shall prevent the Company from complying with any lawful direction, order, notice or regulatory requirement issued by any competent authority.

38.6 Interpretation Consistent with Applicable Law

Every provision of this Policy shall be interpreted, to the maximum extent reasonably possible, in a manner consistent with the Digital Personal Data Protection Act, 2023 and every other Applicable Law governing Personal Data.

Where two interpretations are reasonably possible, the interpretation that better promotes lawful processing, protection of Personal Data and compliance with Applicable Law shall ordinarily be preferred.

38.7 Continuing Effect

The completion, suspension, termination or expiration of the Consultancy Services or the Agreement shall not affect the continued operation of those provisions of this Policy which, by their nature or express wording, are intended to survive, including provisions relating to confidentiality, record retention, limitation of liability, indemnity, dispute resolution, governing law and every other continuing obligation.

38.8 Final Declaration

This Policy represents the Company's commitment to maintaining the privacy, confidentiality, integrity and security of Personal Data entrusted to it in connection with the provision of immigration, visa, international mobility and related consultancy services. The Company shall endeavour to administer this Policy fairly, transparently and in good faith while continuously strengthening its privacy governance framework, information security practices and compliance with Applicable Law.

**Rohit
Kaul**
Digitally signed
by Rohit Kaul
Date:
2026.07.17
18:36:50
+05'30'

Your Personal Consultancy Private Limited
Office No.102, 52A, First Floor,
Vijay Block, East Delhi,
Delhi-110095, India