Zigma Global Environ Solutions Private Limited

Personal Data Protection Policy

Confidential

Personal Data Protection Policy

Introduction

India's Digital Personal Data Protection Act, 2023 (the "DPDP Act"), together with other applicable data protection laws including the Singapore Personal Data Protection Act 2012, the United Kingdom General Data Protection Regulation (UK GDPR), the Malaysia Personal Data Protection Act 2010, and the New Zealand Privacy Act 2020 (collectively, the "Relevant Data Protection Laws"), protect the personal data of individuals, namely natural persons.

Zigma Global Environ Solutions Private Limited (the "Company", "we", "our" or "us") is responsible for the personal data of all individuals that is in its possession or under its control. Every current, former, and prospective client, employee, director, officer, business partner (including agents and third-party service providers), and any other individual who has dealings with the Company has legally recognized rights in relation to the protection of their personal data.

We respect and uphold these rights when collecting, using, processing, transferring, storing, accessing, correcting, or otherwise handling personal data. It is the Company's policy to comply primarily with the requirements of India's Digital Personal Data Protection Act, 2023. In doing so, we ensure adherence to applicable industry standards relating to the security, confidentiality, and integrity of personal data. In cases of doubt, the Company shall consider what a reasonable person would deem appropriate under the circumstances. A robust personal data protection framework enhances stakeholder confidence in the discretion of our services and strengthens the Company's reputation and public trust.

This Policy expressly affirms compliance with India's Digital Personal Data Protection Act, 2023 as the baseline and governing data protection law. In addition, the Company endeavours to comply with the applicable provisions of the Singapore Personal Data Protection Act 2012, the United Kingdom General Data Protection Regulation, the Malaysia Personal Data Protection Act 2010, and the New Zealand Privacy Act 2020, to the extent such laws apply to the Company's operations, websites, or processing activities.

Consistent with the above legislative frameworks, all personal data collected through websites, domains, digital platforms, or during business operations conducted by or on behalf of the Company within India shall be governed by and processed in accordance with the DPDP Act and this Policy. Personal data collected or processed in other jurisdictions such as Singapore, Malaysia, the United Kingdom, or New Zealand may also be subject to the data protection laws of the respective jurisdiction, and the Company shall ensure that such collection and processing is carried out in accordance with applicable local laws, in addition to the principles set out under this Policy.

Where personal data is collected outside India and subsequently transferred into India, the provisions of the DPDP Act shall apply in respect of all processing activities carried out within India. Compliance with foreign data protection laws may be taken into account for regulatory or contractual purposes but shall not dilute the Company's obligations under the DPDP Act.

The DPDP Act is intended to operate as the baseline data protection law governing the Company's personal data processing activities under Indian law. It does not override other applicable Indian statutes but shall operate in conjunction with them and applicable principles of law. The DPDP Act also operates alongside other Relevant Data Protection Laws, and wherever references are made in this Policy to provisions of foreign data protection laws, such references shall be construed, where applicable, to mean the corresponding or analogous provisions under the DPDP Act.

To the extent that any provision of this Policy or the DPDP Act relating to the collection, processing, use, disclosure, or protection of personal data is inconsistent with any other applicable written law, the provisions of such other applicable law shall prevail.

This Policy sets out how the Company manages personal data.

Personal Data

Personal data refers to data, whether true or not, about a natural person who can be identified from that data, or from that data and other information to which we have or are likely to have access. The data may be in electronic or non-electronic form.

Examples (non-exhaustive) of such personal data include:

- Name;
- NRIC, FIN, passport or other identification numbers;
- Mobile, residential or other contact numbers;
- Residential address;
- Email address;
- Age/Date of birth;
- Education background;
- Employment history;
- Profession/occupation;
- Photos and videos;
- Cookies/IP addresses;
- Performance indicators.

In the case of individuals who have passed away within 10 years from the date of contemplation, only provisions relating to disclosure and protection of his/her personal

data shall still apply.[1] The deceased individual's rights under these provisions may be exercised by his/her personal representative or nearest relative.[2] Once more than 10 years have passed since the death of the individual, no data protection provisions apply anymore.[3]

Business contact information is not subject to the rules on data protection, collection, use and disclosure.[4] Business contact information means an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his/her personal purposes.[5]

Information and Consent

General Requirement for Informed Consent

We shall not collect, use or disclose an individual's personal data beyond what is reasonable to provide our service(s) or product(s) to him/her[6] or to work with him/her.[7]

We shall inform the individual of the purpose(s) for collecting, using and disclosing of his/her personal data and obtain consent for the collecting, using and disclosing of the personal data before any of his/her personal data is collected, used or disclosed for such purpose. Specifically:

1. We must inform the individual of the purposes for which we collect, use and/or disclose his/her personal data before the individual gives his/her consent for such collection, use and/or disclosure. The information we provide concerning the purposes shall be, as far as is reasonably practicable, true, accurate and complete[8];
2. For queries related to data protection and to exercise data subject rights under PDPA and the relevant data protections laws, individuals can contact our Data Protection Officer; and
3. The individual must give consent for the purposes for which we collect, use and/or disclose his/her personal data prior to such collection, use and/or disclosure, preferably in writing.[9]

[1] See Sec. 4(4)(b) PDPA.
[2] See Reg.11 PDP Regulations 2014.
[3] See Sec. 4(4)(b) PDPA.
[4] See Sec. 4(5) PDPA.
[5] See Sec. 2(1) PDPA.
[6] See Sec. 14(2)(a) PDPA.
[7] See sec. 11(1) PDPA.
[8] See Sec. 14(2)(b) PDPA.
[9] See Sec. 14(1) PDPA.

We shall inform the individual and obtain his/her consent for any other purpose of the use or disclosure of his/her personal data of which he/she has not yet been informed and agreed to, prior to such use or disclosure.[10]

As best practice, we shall use our best endeavours to obtain written consents. In situations where we receive verbal consent, we shall use our best endeavours to document such verbal consent internally for records purposes.

An individual is deemed to consent to the collection, use or disclosure of personal data about him/her by us for a purpose not specifically informed to him/her, if:

(a) the individual, without actually giving consent, voluntarily provides the personal data to us for that purpose; and
(b) it is reasonable that the individual would voluntarily provide the data.

Unless this Policy indicates that deemed consent is present, the Data Protection Officer[11] must confirm the presence of deemed consent.[12]

There are certain exemptions from the consent requirement. These are set out below in Exemptions from the Consent Requirement.

In relation to Clients & Prospective Clients

Deemed Consent from Prospective Clients

In the case where, during prospecting and preliminary discussions, the prospective client voluntarily provides his/her personal data with a view to engaging our Company's services, he/she is deemed to consent to the Company collecting, using and disclosing this personal data for presenting our services to him/her.[13] The designated Account Manager shall also inform the prospective client about the structure of our group companies and the manner in which we may co-operate and share information amongst group companies.

Provision of Consent by Clients

In the process of initiating services with a client, the designated Account Manager must ensure that the service agreement signed by the client includes a specific annex titled 'Consent to Our Processing of Your Personal Data' (the "PDP Annex"). This annex is crucial as it outlines our commitment to data protection in compliance with the PDPA.

Upon signing the service agreement, the client consents to our collection, use, and disclosure of their personal data. This is solely for the purposes specified in the PDP Annex, which, in the context of our specialized services, is to utilize the personal data to effectively coordinate and facilitate arrangement to carry out the Company's

[10] See Sec. 14(1), 20(1)(b) PDPA.
[11] Please refer to the section Officer in Charge of Personal Data Protection below.
[12] See Sec. 13(a) PDPA.
[13] See Sec. 15(1) PDPA.

services as per the client's requirements. Our processing activities are based on lawful grounds as outlined in the PDPA or its corresponding provisions provided in the relevant data protection laws, including obtaining consent, legitimate interests, or any other applicable legal basis.

Representation of Third-Party Consents

In the course of providing our services, there are instances where we require personal data not only of our direct clients but also of certain third-party individuals connected to them. This may include, but is not limited to, family members, business associates, or other individuals who are integral to the client's property or the situation necessitating our services.

We are held to ensure that personal data on such persons has been collected and is disclosed lawfully by the client. Consequently, the PDP Annex contains a representation and warranty by the client that such thirdparty individuals have provided consent to the client's provision of their personal data to us.

In relation to Current, Prospective or Former Employees

Exemptions to Consent Requirement due to Employment-Related Purposes

A number of exemptions apply to the general consent requirement in the context of the employer-employee relationship. These are described below in Exemptions from the Consent Requirement.

Deemed Consent from Prospective Employees

In the case where, during the course of applying for a position with the Company, a prospective employee voluntarily provides personal data to us, he/she is deemed to consent to the Company collecting, using and disclosing this personal data for making our hiring and/or staff management decisions with respect to him/her.[14] The personnel handling the hiring process shall also inform the prospective employee about the structure of our group companies and the manner in which we may co-operate and share information amongst group companies.

Provision of Consent by Employees

All employees are required to provide explicit consent for the Company's collection, utilization, and disclosure of their personal data as outlined in the employment agreement/service agreement/appointment letter. This consent shall be formally expressed through the act of signing the said employment agreement/service agreement/appointment letter. In relation to Third Parties with No Direct Dealings with Us

Introducers and Referrers: Deemed Consent of Prospective Clients

We occasionally collaborate with individuals and entities (referred to as "Introducers") who play a pivotal role in connecting us with prospective clients. These Introducers

[14] See Sec. 15(1) PDPA.

help expand our reach to those who may benefit from our specialized services and related solutions.

It is the responsibility of the Introducers to obtain the consent (whether explicit or deemed) of these prospective clients for sharing their personal data with us. This consent is crucial for facilitating the introduction to our services and products, and for evaluating the potential establishment of a business relationship.[15]

When an Introducer shares a prospective client's personal data with us, it is understood that the prospective client has given their consent to this sharing. This means the prospective client is deemed to have agreed to our collection and use of their personal data, as received from the Introducers, for the specific purposes of introducing our services and evaluating potential business engagements.[16]

Third Party Personal Data and Deemed Consent

During communications with clients or preliminary discussions with prospective clients about their engaging our services, it may be the case that, in order for us to carry out our work effectively and in accordance with applicable laws, the client or prospective client has to disclose to us personal data of third party individuals we do not deal directly with. For example, he/she may have to disclose to us personal data about his/her family members he/she provides for or personal data about his/her business partners.

It is the responsibility of the client or prospective client (as applicable) to ensure that his/her disclosure of such third party personal data for the purpose(s) of possibly establishing a business relationship with us and/or engaging our services and/or purchasing our services/products is consented to by such third parties, in accordance with applicable laws. Generally, however, we should also ensure that the client or prospective client has obtained the consent from the third party individuals to use and disclose their personal data for our intended purposes, before we collect, use or disclose such personal data.[17]

If the client or prospective client has consent from the third parties to use and/or disclose their personal data for the purpose of engaging in preliminary discussions with us and/or engaging our services and/or purchasing our services/products, such third parties are also deemed to consent to our collection and use of their personal data for the same purposes.[18] Notably, the third party may be deemed to consent to the disclosure of his/her personal data by the client or prospective client (as applicable) for the purposes of the client or the prospective client engaging our services, if the third party voluntarily gave his/her personal data to the client or prospective client for

[15] See Sec. 15(2) PDPA.
[16] See Sec. 15(2) PDPA
[17] See Sec.12.34 Advisory Guidelines On Key Concepts In The PDPA, Qn. 4 PDP Checklist for Organizations.
[18] See Sec. 15(2) PDPA.

this purpose and it is reasonable that such third party would voluntarily provide this data.[19]

Exemptions from the Consent Requirement for Data Collection, Use & Disclosure

Subject to applicable laws, notable exemptions from the consent requirement for collection, use and/or disclosure of personal data include the following[20]:

- when the personal data is publicly available[21];
- when the use and/or disclosure is necessary for any purpose which is clearly in the interests of the individual, if consent for its use or disclosure cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;
- when such data collection, use and/or disclosure is necessary for evaluative purposes[22];
- when such data collection, use and/or disclosure is necessary for any investigation or proceedings, if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data;
- when the disclosure is to a public agency and such disclosure is necessary in the public interest; or
- specifically in relation to current or prospective employees:
    - when the personal data is included in a document produced in the course, and for the purposes, of the individual's employment, business or profession; and collected for purposes consistent with the purposes for which the document was produced; or
    - when the personal data is collected by us and the collection is reasonable for the purpose of managing or terminating our employment relationship with the individual.

Confidentiality

We are committed to implementing strict physical, electronic, administrative and procedural safeguards to protect personal data in our possession or under our control

[19] See Sec. 15(1) PDPA.
[20] Please refer to Sec. 17 PDPA and Schedules 2, 3 & 4 to the PDPA for the full list of exemptions.
[21] "publicly available" means personal data generally available to the public and includes personal data which can be observed by reasonably expected means at a location or an event at which the individual appears and that is open to the public.
[22] "evaluative purpose" means (a) for the purpose of determining the suitability, eligibility or qualifications of the individual to whom the data relates (i) for employment or appointment to office; (ii) for promotion in employment or office or for continuance in employment or office; (iii) for removal from employment or office; or (iv) for the awarding of contracts, awards or other similar benefits; or (b) for the purpose of determining whether any contract, award or other similar benefit should be continued, modified or cancelled.

against loss, misuse, damage and unauthorized access, modifications or disclosures, at each stage of data collection, processing[23], retention and disclosure including (without limitation):

- requiring all employees to be bound by confidentiality obligations in their employment agreements;
- implementing robust staff policies and procedures (with disciplinary consequences for breaches) regarding confidentiality obligations;
- storing confidential documents in locked file cabinet systems;
- restricting employee access to confidential data on a need-to-know basis;
- restricting access to our physical premises only to authorized personnel;
- implementing sophisticated information technology software to ensure that:
    - our information systems are password-protected;
    - sensitive data is segregated and access limited to authorized users only; and/or
    - transmissions of sensitive data are securely encrypted.

Involvement of Third Parties

Data Intermediaries

In the course of our business operations, personal data in our possession or under our control may be collected, processed and disclosed[24], pursuant to written contracts, on our behalf by third parties such as the following:

- other group companies;
- third party agents, contractors or service providers who provide operational services; and
- professional advisers such as auditors and lawyers.

Such parties are our data intermediaries.[25]

The Data Protection Officer shall ensure, via our contracts with such third parties, that the data intermediaries handle the personal data in accordance with this Policy[26], particularly in relation to the protection and retention of personal data.

Introducers

In the course of our business dealings with Introducers, where we seek to collect and use personal data about prospective clients from them, we shall provide the

[23] Sec. 2(1) PDPA sets out the definition of "processing". "Processing", in relation to personal data, means the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following: (*a*) recording; (*b*) holding; (*c*) organisation, adaptation or alteration; (*d*) retrieval; (*e*) combination; (*f*) transmission; (*g*) erasure or destruction.
[24] See Note 20 for the definition of "processing".
[25] Sec. 2(1) PDPA defines "data intermediary" as 'an organization which processes personal data on behalf of another organization but does not include an employee of that other organization".
[26] See Sec. 4(3) PDPA.

Introducers with sufficient information concerning the purposes for which we seek the personal data, to allow the Introducers to determine whether their disclosure of the personal data of prospective clients to us would be in accordance with applicable laws.[27]

Processing of Personal Data for Other Organisations

Where we handle personal data on behalf of any other organisation, including but not limited to other group entities, this Policy shall apply to our handling of such personal data, too.

Transfer to Other Jurisdictions

As a matter of practise we do not transfer personal data in our possession or under our control outside of India or the respective jurisdiction.

In the event such a transfer is approved by management to proceed, prior to such transfer, the Data Protection Officer shall take reasonable steps to verify that the overseas receiving party(s) have in place, a standard of protection for the transferred data equal to or higher than that set out in this Policy, in adherence with applicable laws and cross-border data protection policies.[28]

When personal data is transferred overseas, the Data Protection Officer or Account Manager shall inform the affected individuals of the extent to which their personal data will be protected in the foreign jurisdiction(s) to which the data will be transferred and seek their consent. In case of such international data transfers, we ensure compliance with the PDPA (to the extent applicable), the other relevant data protection laws including UK GDPR, by employing mechanisms such as Standard Contractual Clauses for secure data transfers.

Collection

We shall not collect any personal data on any prospective client, client, prospective employee, employee, business partner or any other individual without having obtained the individual's consent and only for purposes the individual has been informed about,[29] unless an exemption provided by statutory regulations, in particular in the PDPA, as indicated in this Policy applies.

[27] See Sec. 20(2) PDPA.
[28] See Sec. 26(1) PDPA, Reg. 9 PDP Regulations 2014.
[29] See Information and Consent for details.

Children's Data

The collection, use and disclosure of children's personal data by us would be limited to exceptional contracts, contracts executed on behalf of children by their parent or legal guardian, or non-contractual situations (that is, where the relationship between organisation and child is governed by statute). Where the child is below the age of 18 years, such data processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Automated Monitoring

In our operations we may monitor and record physical and communicative interaction concerning or involving the Company, including in the following manners:

- monitoring and/or recording of voice calls with clients and banks for employee training and performance evaluation, identity verification and, most of all, control purposes;
- monitoring and/or recording of internet use; and
- carrying out closed circuit television cameras ("CCTVs") surveillance and conducting security clearances to manage the safety and security of our premises and services.

Generally, we shall inform all concerned individuals that we are carrying out the monitoring of and recording of information, be it data, video or voice.

The PDP Annex, the EPDP Annex and written updates from the Company to all concerned individuals shall include information on all types of monitoring and recording of information carried out by us, and the purposes behind our surveillance.

In relation to CCTVs, we shall place notifications of CCTV deployment in prominent locations within our office in order to enable individuals to have sufficient awareness of the CCTVs and to inform such individuals of the purpose for which we deploy CCTVs. The placement or content of the notifications need not reveal the exact location of the CCTVs.

For incoming voice calls, every individual who calls the Company shall be notified via an automated message, prior to the telephone conversation taking place, that his/her call may be recorded and what the purpose for recording is.

Duty to determine Accuracy and Completeness

We shall, as far as reasonably practicable, ensure that personal data collected by or on behalf of us is accurate and complete, particularly in the case where:

(a) an individual's personal data is likely to be used by us to decide a matter that affects him/her, e.g. on-boarding a new client, or making a hiring decision; or

(b) we are likely to disclose such personal data to another organization, e.g. sharing client information with insurance companies to assist in claims process or during collaborative works with subcontractors or partners for certain specialized services.[30]

We may presume personal data provided directly to us by concerned individuals is accurate in most circumstances.[31] As best practice, our on-boarding and employment documentation process shall include a representation and warranty by all clients and employees, that the personal data provided by them is accurate and complete, as well as research where appropriate or legally required.

At the start of each financial year, the Data Protection Officer shall review all data and take steps to verify that the personal data in our possession and under our control remains up to date and, if necessary, update the relevant data.

Retention of Personal Data

We shall not store any personal data on any prospective client, client, prospective employee, employee, business partner or any other person without having obtained the individual's consent and only for purposes that the individual has been informed about,[32] unless an exemption provided by statutory regulations, in particular in the PDPA, as indicated in this Policy applies.

We shall retain personal data for as long as it is reasonable to assume the need for retention, to fulfil the purposes for which such data was collected, our business purposes, or as is otherwise required under any applicable laws. This Policy is subject to our rights and obligations under applicable laws to ensure retention of records which may contain personal data as well as the Company's archiving and records retention policies.[33]

Notably:

(a) under the Companies Act, we are required to retain accounting records which may contain personal data of individuals for at least 5 years from the end of the financial year in which the relevant transactions or operations are completed[34]; and

[30] See Sec. 23 PDPA.
[31] See Sec. 16.6 Advisory Guidelines On Key Concepts In The PDPA.
[32] See Information and Consent for details.
[33] See. Sec.25 PDPA.
[34] See Sec.199 of the Companies Act (Cap.50, 2006 Rev.Ed.).

(b) under the Income Tax Act and the Goods and Services Tax Act, we are required to keep our business records for a period of at least 5 years.[35]

As soon as the expiry of (i) validity of the purposes for which personal data was collected; and (ii) all records retention obligations under applicable laws and our business needs, may be reasonably assumed, on approval by management and the Data Protection Officer, we shall erase or destroy our documents and other media containing personal data, or remove the means by which the personal data can be associated with particular individuals.

Within 2 months of the end of each financial year, the Data Protection Officer shall review all data in our possession or under our control for the purpose of identifying personal data that should no longer be retained. All data that contains personal data which should no longer be retained shall either be destroyed or any personal data therein erased.

In the event of extenuating circumstances which require us to retain certain personal data beyond its usual retention timeframe, e.g. if the Company is engaged in an legal dispute, we shall preserve such data as long as is reasonably necessary, such as until the legal dispute is settled. In such cases, the Data Protection Officer shall maintain a list of the data to be preserved and notify management of the extended retention.

In the case of a contemplated business asset transaction[36], should personal data of the employees, clients, directors, officers or shareholders of the prospective counterparty have been collected, and such business asset transaction did not proceed or complete, we shall destroy, or return to the prospective counterparty, all such personal data collected.[37]

Use

We shall not use any personal data on any prospective client, client, prospective employee, employee, business partner or any other person without having obtained the individual's consent and only for purposes that the individual has been informed about,[38] unless an exemption provided by statutory regulations, in particular in the PDPA, as indicated in this Policy applies.

[35] See Sec.67 Income Tax Act (Cap.134, 2014 Rev.Ed.), Sec.46(2) Goods and Services Tax Act (Cap.117A, 2005 Rev.Ed.).
[36] "business asset transaction" means the purchase, sale, lease, merger or amalgamation or any other acquisition, disposal or financing of the Company or any part thereof or of any of our business or assets other than the personal data to be disclosed.
[37] See Para. 3(4) of the Second Schedule to the PDPA.
[38] See Information and Consent for details.

Prohibition Against Cold Calling or Any Other Similar Marketing Technique

We do not engage in the cold calling strategy for lead generation or to make unsolicited offers, in any other similar manner or via any other similar medium including text messaging, of our services or any of our products (if applicable).

Disclosure

Generally, we shall not disclose any personal data on any prospective client, client, prospective employee, employee, business partner or any other person without having obtained the individual's consent and only for purposes that the individual has been informed about[39], unless an exemption provided by statutory regulations, in particular in the PDPA, as indicated in this Policy applies.

We shall, as far as reasonably practicable, verify that the transmission of the personal data is secure and that the receiving party employs the necessary security measures.

For disclosure of data to parties outside of India, please refer to Transfer to Other Jurisdictions.

Who We May Disclose Clients' Personal Data to

Generally, we shall protect and keep confidential personal data of our clients and prospective clients. However, subject to applicable laws, we may disclose such personal data for the purposes set out in the PDP Annex[40] to parties such as those set out below:

- our group companies;
- companies providing services relating to insurance and/or reinsurance to us, and associations of insurance companies,
- agents, contractors or third party service providers who provide services to us
- our professional advisers such as our auditors and lawyers; and
- regulators and authorities.

Who We May Disclose Current, Prospective or Former Employees' Personal Data to

Without limitation, parties to whom current, former or prospective employees' personal data may be disclosed include:

- other group companies;

[39] See Information and Consent for details.
[40] See Sec. 15(2) PDPA.

- vendors, landlords, agents and representatives;
- regulators, authorities, professional bodies;
- other financial institutions; and
- employees' representatives.

Access to Personal Data, Correction of Personal Data and Withdrawal of Consent

Request for Access to Personal Data and/or Correction of Personal Data

Any individual may request us in writing to grant him/her access to his/her personal data and/or to correct an error or omission in his/her personal data.[41]

The Data Protection Officer shall first identify the person making the request and ensure that this person is authorised to access the personal data, in particular personal data regarding clients and prospective clients.[42]

Access to Personal Data

The Data Protection Officer shall collect the personal data to which access is requested. He/She shall submit the collected data to senior management for consent before disclosing it to the applicant.

Generally, we shall, as soon as reasonably practicable and as accurately and completely as reasonably possible:

- provide the applicant with his/her personal data in our possession or controlled by us; and
- inform him/her about how we have or may have used or disclosed such data within 1 year of the date of such request.[43]

Generally, we shall provide to the applicant the requested personal data and information on its use and disclosure within 30 days after receiving the request. If our response will take longer, the Data Protection Officer shall inform the applicant in writing of the time by which we will respond to the request.

However, there are certain circumstances under which we may be prohibited from providing access or we may in our discretion, deny access requests.

For example, we are prohibited from providing an individual access if the provision of the data could reasonably be expected to[44]:

[41] See Reg. 3(1) PDP Regulations.
[42] See Reg. 3(1) PDP Regulations.
[43] See Rec. 21(1) PDPA, Reg. 4(2) PDP Regulations 2014.
[44] For the full list of prohibitions see sec. 21(3) PDPA.

- threaten the safety or physical or mental health of another individual;
- reveal personal data about another individual;
- reveal the identity of another individual who has provided the personal data, and the individual has not consented to the disclosure of his or her identity; or
- be contrary to national interest.[45]

We may also at our discretion deny access requests to personal data if[46]:

- it is opinion data kept solely for an evaluative purposes. For example, we need not provide access to records of the Company's opinions formed about a potential employee in the course of interviewing him/her to determine suitability and eligibility for the position;
- the disclosure of the information would reveal confidential commercial information that could harm our competitive position; or
- it is related to an on-going prosecution or on-going investigation, in which case we may, if necessary, refuse to confirm or deny the existence of such personal data.[47]

Where the individual is not to be granted access to portions of the personal data, we shall omit such data while still providing the individual access to the other personal data.[48]

Correction

The Data Protection Officer shall make efforts to verify if the requested amendments are true, accurate and complete. He/she shall submit his/her findings to senior management for consent.

If no good reason to the contrary is detected, the Data Protection Officer shall correct the personal data as soon as practicable to do so and send the corrected data to every organization to which we have, within a year of the date of such correction, disclosed the relevant data for legal or business purposes.[49]

If other organizations notify us of corrections to be made to personal data in our possession or under our control, we shall make the necessary corrections as soon as practicable to do so, unless we have good reason to believe such correction should not be made.[50]

[45] See Sec. 21(2),(3) and (4) PDPA.
[46] For the full list see 5th Schedule to the PDPA.
[47] See Reg. 6 PDP Regulations.
[48] See Sec. 21(5) PDPA.
[49] See Sec. 22 PDPA.
[50] See Sec. 22(4) PDPA.

In the case where we have good reason to reject making the requested amendments, we shall annotate the relevant personal data to reflect the amendments requested but not made.[51]

We need not correct personal data on request if the request is in respect of opinion data kept solely for an evaluative purpose or data related to an ongoing prosecution.[52]

Withdrawal of Consent

At any time, by giving us prior written notice, an individual may withdraw any actual or deemed consent in respect of our collection, use or disclosure of his/her personal data.[53]

On receipt of such notice of withdrawal we shall first highlight the consequences of withdrawal to the individual concerned even if those consequences have been set out somewhere else.[54] Thereafter, should the individual still wish to proceed, we shall, as soon as is reasonably practicable, cease the collection, use or disclosure of such personal data. Concerned data intermediaries and third party service providers must also be informed of the withdrawal and we shall ensure that they cease collecting, using or disclosing such personal data for our purposes.[55]

Despite withdrawal, we are not required to delete or destroy the personal data upon request and may continue to retain such data in accordance with this Policy.[56] In particular, we shall retain personal data where we have a legal obligation to maintain records.[57]

Likely Consequences of Withdrawal of Consent by Prospective Clients

In the event of notification by a prospective client of withdrawal of his/her consent, the designated Account Manager shall advise such prospective client that we will discontinue the on-boarding process.[58]

Likely Consequences of Withdrawal of Consent by Clients

In the event of notification by a client of withdrawal of his/her consent, the Account Manager shall advise such client of the likely consequences of such withdrawal, including the probable limitation or cessation of the provision of services we are able to provide to him/her.[59]

[51] See Sec. 22(5) PDPA.
[52] See 6th Schedule to the PDPA.
[53] See Sec. 16(1) PDPA.
[54] See Sec 12.46 Advisory Guidelines On Key Concepts In The PDPA.
[55] See Sec. 12.47 Advisory Guidelines On Key Concepts In The PDPA.
[56] See Sec. 12.49 Advisory Guidelines On Key Concepts In The PDPA.
[57] See Retention of Personal Data.
[58] Pursuant to Sec. 16(2) PDPA.
[59] Pursuant to Sec. 16(2) PDPA.

Likely Consequences of Withdrawal of Consent by Prospective Employees

In the event of notification by a prospective employee of withdrawal of his/her consent, we shall advise him/her that we will discontinue the hiring process.[60]

Likely Consequences of Withdrawal of Consent by Current Employees

Current employees are advised that in the event of such withdrawal of consent, we reserve the right to terminate the employment relationship, reassign such employees' current responsibilities and/or transfer such employees to a different role.[61] Moreover, salary payments and benefits may be delayed or may not be provided anymore.

Specific Rights under of Data Subjects under the UK GDPR

Individuals domiciled in the UK shall have additional specific rights under the UK GDPR, including the right to access, rectify, and erase their personal data. For details on exercising these rights, individuals may contact our Data Protection Officer. Individuals have rights1 in relation to the way we handle their personal data. These include:

• Right to be informed about the collection and use of personal data.

• Right to access and receive a copy of written or recorded (audio and video)

personal data, and other supplementary information.

• Right to rectification to have inaccurate personal data rectified, or completed if it is incomplete

• Right to erasure of personal information in certain circumstances

• Right to restrict processing of personal data in certain circumstances

• Right to object to processing of personal data in certain circumstances

• Rights related to automated decision-making including profiling. Individuals have

the right not to be subject to a decision based solely on automated processing,

including profiling

• Right to complain

Dispute

[60] Pursuant to Sec. 16(2) PDPA.
[61] Pursuant to Sec. 16(2) PDPA.

In the event an individual submits a complaint in connection with our handling of his/her personal data, the Data Protection Officer shall acknowledge in writing the receipt of such complaint within 2 business days.

Within 10 business days, the Data Protection Officer shall contact the individual to inform him/her that the Data Protection Officer will conduct an investigation into the complaint. The Data Protection Officer shall also provide the individual with an estimation of the reasonable timeframe for our investigations and resolution of the complaint. If the complaint requires more time beyond such estimation to resolve due to its complexity, the Data Protection Officer shall inform the individual accordingly on or before the expiry of the original estimated timeframe.

The Data Protection Officer shall then investigate the complaint and submit his/her findings to senior management for consent. The results shall subsequently be presented to the individual by the Data Protection Officer, Account Manager and/or management, as deemed appropriate.

In the event that the Data Protection Officer's investigations conclude with a solution that is dissatisfactory to the individual, the individual shall be directed to contact our management. The Chief Executive Officer shall acknowledge his/her complaint within 2 business days of such contact, review the complaint and original resolution and strive to provide a satisfactory closure to the individual within 10 business days.

In the unlikely event that the Company is unable to reach an agreement with the individual, we shall send him/her a final response and inform him/her of their right to refer the complaint to the Personal Data Protection Commission. Alternatively, mediation shall be suggested as a method of alternative dispute resolution.[62]

Execution

Disclosure of Policy and Procedures

We shall provide to all concerned individuals information on our personal data protection policies and practices in the following manners:

(a) incorporating information on our personal data protection policies and practices in our legal documentation, such as the PDP Annex, the EPDP Annex[63];
(b) sending of letter updates to the concerned individuals informing of legal or policy updates to our personal data protection policies and practices;
(c) making available on our website dedicated information on our personal data protection policies and practices for any matter concerning the

[62] See Part VII PDPA.
[63] Please refer to the explanations of "Consent" and "Employee Consent" set out in Transition.

personal data of individuals, in particular our consent withdrawal procedures and our complaints procedure; and

(d) making the business contact information of our Data Protection Officer publicly available information, via our website and our Company documentation, in order that concerned individuals may contact him/her to request for further information on our personal data protection policies and practices, resolve queries in this regard and/or submit a complaint in this regard.[64] Such business contact information should be readily accessible from India, operational during India business hours and in the case of telephone numbers, be India telephone numbers.[65]

Officer in Charge of Personal Data Protection

Our Data Protection Officer is our designated responsible person in charge of ensuring that the Company complies with this Policy and the PDPA at all times.[66] He/She is also the point of contact for all matters related to personal data protection. Should any employee who is not the Data Protection Officer receive requests from individuals concerning personal data protection, they are to forward these requests to the Data Protection Officer immediately.

On request by any person, the Company shall provide him/her with the business contact information the Data Protection Officer.[67]

Personal Data Inventory Map

To facilitate the proper implementation of this Policy, the Data Protection Officer shall, in conjunction with management, keep an up-to-date personal data inventory map which tracks in general terms what personal data is collected by the Company, the purposes for such collection, the channels of collection, the methods of collection, the location of storage of data, and who such data is disclosed to.[68]

Remedial Plan

In the event the Data Protection Officer becomes aware of a breach of this Policy, he/she shall immediately notify the management of such breach and, in consultation with the management, take all appropriate actions to remedy and/or mitigate the consequences of such breach to the extent possible.

Within 3 business days of such breach, the Data Protection Officer shall commence an investigation into the circumstances of the breach and, if necessary, take disciplinary action against any employees who are culpable for the breach in accordance with this Policy and applicable laws. In the event of a proven data

[64] See Sec. 11(5), sec. 12(d) PDPA.
[65] See Sec.20.6 Advisory Guidelines On Key Concepts In The PDPA.
[66] See Sec. 11(3) PDPA.
[67] See Sec. 20(1)(c) PDPA.
[68] See Qn. 2 PDP Checklist for Organizations.

breach arising from the UK, we shall adhere to the UK GDPR requirements for prompt notification to the Information Commissioner's Office (ICO) and affected individuals.

Annual Review

At the end of each financial year, a review of personal data in our possession and under our control, this Policy and our execution thereof shall be conducted[69] to:

(a) affirm that the collection, use and disclosure of the data is limited only to purposes that we have obtained consent for;
(b) affirm the classification of the personal data held by us to ensure that our employees, third party service providers and business partners are accessing such data only on a need-to-know basis[70];
(c) enhance our data security policies and security measures to ensure a consistently high level of security;
(d) affirm that contractual provisions are in place to ensure proper safeguards in respect of personal data disclosed to our third party data intermediaries; and
(e) affirm the work carried out by the Data Protection Officer, in particular the proper removal of personal data which are no longer subject to any retention requirements.

Such review may be carried out either by management or by internal or external auditors. We may also conduct Privacy Impact Assessments if required, particularly for high-risk data processing activities. A Privacy Impact Assessment is a systematic evaluation process used to assess the potential impact of a specific project, initiative, or system on the privacy of individuals. It involves identifying and mitigating privacy risks associated with the processing of personal data.

Training

Management views the protection of personal data with utmost importance.

As employees of this Company, each member of our staff has the duty to familiarize themselves with this Policy and our personal data protection practices, and to carry out their duties in strict adherence with such policy and practices.[71]

To facilitate this, the Data Protection Officer shall, in consultation with management, carry out regular training sessions once every two years to train our employees on best practices for handling and protecting personal data in accordance with this Policy and the PDPA[72] and strengthen their awareness of threats to security of personal data.

[69] See Qn. 25 PDP Checklist for Organizations.
[70] See Qn. 21 PDP Checklist for Organizations.
[71] Pursuant to Sec. 53(2) PDPA.
[72] See Sec. 12(c) PDPA.

Transition

The Company may continue using personal data about an individual collected before 1 July 2014 for the purposes for which the personal data was collected unless:

(a) consent for such use is withdrawn; or
(b) the individual, whether before, on or after 1 July 2014, has otherwise indicated to the Company that he/she does not consent to the use of the personal data.[73]

All existing clients and employees of the Company as of 2 July 2014 shall be required to indicate their consent to the Company's collection, use and disclosure of their personal data for purposes described (i) in case of clients, in the letter entitled "Personal Data Protection Notification & Consent" (the "Consent"), or (ii) in case of employees, in the statement entitled "Consent to Our Processing of Your Personal Data" (the "Employee Consent"), by signing the letter or statement (as applicable). Our processing activities are based on lawful grounds as outlined in the PDPA or its corresponding provisions provided in the relevant data protection laws, including obtaining consent, legitimate interests, or any other applicable legal basis.

The Data Protection Officer shall review the Company's current terms of engagement with the following:

- other group companies;
- other financial institutions; and
- all third party service providers involved in our business operations, such as agents, partners or data intermediaries;

to determine whether under the present terms of engagement, the Company remains in adherence with this Policy and the PDPA. Where amendments need be made, the Data Protection Officer shall submit the proposed changes for management review and approval as soon as possible and reach out to the relevant counterparties to implement the necessary amendments.

[73] See Sec. 19 PDPA.